DICCIONARIO de Protección de Datos Personales

Conceptos fundamentales

Isabel Davara F. de Marcos
COORDINADORA

inai

DICCIONARIO de Protección de Datos Personales

Conceptos fundamentales

inai

DIRECTORIO

Pleno del INAI

Francisco Javier Acuña Llamas
Comisionado Presidente

Oscar Mauricio Guerra Ford
Comisionado

Blanca Lilia Ibarra Cadena
Comisionada

María Patricia Kurczyn Villalobos
Comisionada

Rosendoevgueni Monterrey Chepov
Comisionado

Josefina Román Vergara
Comisionada

Joel Salas Suárez
Comisionado

Comité Editorial

Blanca Lilia Ibarra Cadena, Presidenta

Rosendoevgueni Monterrey Chepov
Josefina Román Vergara
Guillermo Miguel Cejudo Ramírez
Isabel Davara Fernández de Marcos
Pilar Ferreira García
Lilia María Vélez Iglesias

Cristóbal Robles López
Secretario Técnico del Comité Editorial

Las opiniones expresadas en esta publicación son responsabilidad exclusiva de los autores y no reflejan necesariamente las del INAI.

Derechos Reservados D.R.
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Ciudad de México, C.P. 04530.
Diseño y formación: Martha Rosalba Pérez Cravioto.

Primera edición, noviembre de 2019.
Tiraje: 3,000 ejemplares.
ISBN: 978-607-98648-3-5

Impreso en México, *Printed in Mexico*.
Ejemplar de distribución gratuita.

ÍNDICE

Lista de siglas y acrónimos 13
Lista de autores 19
Presentación 23
Semblanzas de autores 25

A

Acceso a la información pública 41
Acciones para la seguridad de los datos personales 45
Acta de verificación 48
Activo 51
Actualizaciones de las medidas de seguridad 55
Acuerdo de determinación 57
Acuerdo de Inicio de Procedimiento de Imposición de Sanciones 59
Acuerdo de Inicio del Procedimiento de Verificación 61
Afectación significativa 66
Ámbito de aplicación 66
Amenaza 68
Análisis de brecha 68
Análisis de riesgo 69
Anonimización 70
Aprendizaje de máquinas 74
Archivo electrónico 74
Auditoría 77
Autenticación 79
Autodeterminación informativa 82

Autoridad de control 87
Autoridades coadyuvantes 90
Autorregulación 93
Aviso de privacidad 96

B

Bases de datos 105
Big data 109
Bloqueo de los datos personales 114

C

Ciclo de vida de datos personales....121
Ciclo de vida de la acreditación....125
Ciclo de vida de la autorización....127
Ciclo de vida del certificado 128
Comisionado 130
Comité de transparencia 133
Cómputo en la nube....135
Comunicaciones privadas....143
Conciliación dentro del Procedimiento de Protección de Derechos 146
Confidencialidad de la información....152
Consejero consultivo del INAI 153
Consejo Consultivo de los organismos garantes de las entidades federativas....158
Consejo Consultivo del INAI 162
Consejo Nacional de Transparencia, Acceso a la Información
y Protección de Datos Personales 170
Consentimiento....175
Consentimiento expreso 181
Consentimiento expreso y por escrito 185
Consentimiento otorgado por medios electrónicos 188
Consentimiento tácito....192

Conservación de los datos 195
Control de seguridad 197
Convenio 108 del Consejo de Europa 199
Cookies 204

D

Daño moral 209
Dato personal 211
Dato personal sensible 216
Datos personales biométricos 218
Datos personales genéticos 221
Datos personales relativos a la salud 226
Deber de confidencialidad 229
Deber de seguridad 232
Delegado de protección de datos 235
Delito en materia de protección de datos personales 240
Departamento de protección de datos personales 244
Derecho a la imagen 247
Derecho a la limitación del tratamiento 252
Derecho al honor 254
Derecho al olvido 269
Derechos ARCO 273
Derecho humano 296
Derechos morales 305
Derecho de portabilidad 307
Derechos patrimoniales 313
Desechamiento de la denuncia 314
Dignidad humana 317
Directrices de la OCDE sobre protección de datos y flujos transfronterizos 320
Disociación 324
Disponibilidad de la información 325
Divulgación 326
Documento de seguridad 328
Documento electrónico (mensaje de datos) 331

E

Encargado.....339
Equivalencia funcional 345
Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) 347
Esquemas de mejores prácticas en materia de protección de datos personales.....351
Estándares de seguridad 355
Ética en la protección de datos personales.....359
Evaluación de Impacto en la Protección de Datos Personales (EIPD) 360
Evaluación del Sistema de Autorregulación Vinculante 369
Exportador.....371

F

Factores para determinar las medidas de seguridad 377
Firma autógrafa 379
Firma electrónica 380
Firma electrónica avanzada 383
Fuente de acceso público.....386
Funciones de seguridad 388
Fundamentación y motivación 389

G

Geolocalización 401
Grupo de empresas.....405

I

Impacto 417
Incidente de seguridad 417
Información confidencial 418
Información pública 427
Información reservada.....431
Infracción 432
Infractor 438
Instituto Nacional de Transparencia, Acceso a la Información
y Protección de Datos Personales.....441
Integridad de la información 443
Inteligencia artificial.....444
Interés legítimo 446
Interés público 450
Internet de las cosas 453
Intervención de las comunicaciones.....456
Intimidad.....459
Inviolabilidad de las comunicaciones 465

J

Juicio contencioso administrativo (juicio de nulidad) 471
Juicio de resolución exclusiva de fondo 477
Juicio por la vía sumaria.....484
Juicio de amparo.....490
Juicio de amparo directo.....509
Juicio de amparo indirecto 513
Juicio en línea.....526

L

Listado de exclusión.....539

M

Mecanismos alternativos de solución de controversias....543
Medidas de apremio....549
Medidas compensatorias....551
Medidas correctivas en caso de vulneraciones de seguridad....554
Medidas de seguridad....555
Medidas de seguridad administrativas....559
Medidas de seguridad físicas....562
Medidas de seguridad técnicas....565
Medios de impugnación en el amparo....569
Modalidades del aviso de privacidad....584
Monetización de datos personales....588
Monitoreo de datos personales....590
Multa....592

N

Neutralidad tecnológica....599
Nivel adecuado de protección de datos personales....601
Notificación de vulneración de seguridad....610

O

Organismos garantes....619

P

Persona física identificable....625
Plataforma Nacional de Transparencia....627
Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales....634

Prestador de servicios de certificación 640
Presunto infractor 644
Principio de calidad 648
Principio de consentimiento 652
Principio de finalidad 656
Principio de lealtad 659
Principio de licitud 661
Principio de proporcionalidad 663
Principio de responsabilidad 665
Principios de autorregulación vinculante 670
Privacidad 672
Procedimientos en materia de protección de datos personales
para el sector público 680
Protección de datos personales 687
Protección de datos por defecto 694
Protección de datos personales por diseño 696
Procedimiento de Imposición de Sanciones (Pisan) 700
Procedimiento de investigación (PI) 704
Procedimiento de protección de derechos 712
Procedimiento de Verificación (PV) 719
Programa Nacional de Protección de Datos Personales 731
Prueba electrónica 737
Prueba de daño 742
Puesta a disposición del aviso de privacidad 744

R

Recomendaciones de Seguridad 749
Reconducción de la denuncia 751
Registro de los esquemas de autorregulación vinculante 752
Reglamento General de Protección de Datos 753
Reglamento interior del IFAI (actualmente INAI) 758
Reincidencia 764
Relación jurídica 767
Remisión de datos personales 768

Requerimiento de información 770
Resolución de Madrid de Estándares Internacionales de Privacidad 773
Resolución del Pleno del INAI 775
Responsable del tratamiento.....782
Revisión del Sistema de Autorregulación Vinculante 785
Revocación del consentimiento 787
Riesgo.....789
Riesgo de seguridad 789

S

Seguridad de la información 793
Seudonimización 796
Sistema de certificación en materia de protección de datos personales.....799
Sistema de gestión de seguridad de datos personales 801
Sistema de justicia en línea 805
Sistema de privacidad APEC 808
Sistema Electrónico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (IFAI-Prodatos). 814
Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (SNT) 817
Sistema de privacidad y protección de datos personales en Estados Unidos de América (modelo estadounidense) 824
Situación de emergencia.....827
Sobreseimiento del procedimiento.....830
Solicitud de protección de datos dentro del procedimiento de protección de derechos 834
Soporte electrónico 837
Soporte físico 838
Subcontratación.....838
Subencargado 841
Supresión de datos personales 842

T

Tercero 849
Titular de los datos personales 850
Toma de decisiones sin intervención humana valorativa.....853
Transferencia 855
Tratamiento 860
Tratamiento intensivo de datos personales.....864

U

Unidad de transparencia 871

V

Vida privada 875
Videovigilancia 885
Visitas de verificación 888
Vulnerabilidad.....894
Vulneración de datos personales.....894

W

Web beacons 897

LISTA DE SIGLAS Y ACRÓNIMOS

AEPD	Agencia Española de Protección de Datos
APDP	Autoridad de Protección de Datos Personales
APEC	Foro de Cooperación Económica Asia-Pacífico
BCR	Binding Corporate Rules o Normas Corporativas Viculantes
CADH	Convención Americana sobre Derechos Humanos
CBPR	Cross Border Privacy Rules o Reglas de Privacidad Transfronterizas
CCF	Código Civil Federal
CDFUE	Carta de Derechos Fundamentales de la Unión Europea
CDN	Convención sobre Derechos del Niño
CE	Comisión Europea
CFPC	Código Federal de Procedimientos Civiles
Convenio 108	Convenio nº 108 del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal
CIDH	Corte Interamericana de Derechos Humanos
CPEUM	Constitución Política de los Estados Unidos Mexicanos
CT	Comité de Transparencia

Derechos ARCO	Derechos de acceso, rectificación, cancelación y oposición
DGIV	Dirección General de Investigación y Verificación para el Sector Privado
DGIVSP	Dirección General de Investigación y Verificación para el Sector Público
DGPDS	Dirección General de Protección de Derechos y Sanción
Directiva 95/46/CE	Directiva 95/46/CE, sobre protección de personas físicas en lo que respecta al tratamiento de datos personales
Disposiciones sobre EIPD	Disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales
DOF	Diario Oficial de la Federación
DPD	Delegado de Protección de Datos
DRAE	Diccionario de la Real Academia de la Lengua Española
DUDH	Declaración Universal de los Derechos Humanos
Estándares Iberoamericanos	Estándares de Protección de Datos Personales para los Estados Iberoamericanos
Estatuto Orgánico del INAI	Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
GISGSDP	Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales
GTA29	Grupo de Trabajo del Artículo 29 en materia de protección de datos personales
IA	Inteligencia Artificial
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos Personales
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos Personales
IoT	Internet de las cosas o internet de los objetos

LA	Ley de Amparo Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos
LFPA	Ley Federal de Procedimiento Administrativo
LFPCA	Ley Federal de Procedimiento Contencioso Administrativo
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LFTAIP	Ley Federal de Transparencia y Acceso a la Información Pública
LFTAIPG	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
LGPDPPSO	Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados
LGTAIP	Ley General de Transparencia y Acceso a la Información Pública
Lineamientos de Portabilidad	Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales
Lineamientos del Aviso de Privacidad	Lineamientos para la elaboración de los avisos de privacidad
Lineamientos del PNPDP	Lineamientos para la elaboración, ejecución y evaluación del Programa Nacional de Protección de Datos Personales
Lineamientos Generales	Lineamientos Generales de Protección de Datos Personales para el Sector Público
OCA	Órganos constitucionalmente autónomos
OCDE	Organización para la Cooperación y el Desarrollo Económico
Parámetros de autorregulación	Parámetros para el correcto desarrollo de los Esquemas de Autorregulación Vinculante
PI	Procediimiento de investigación (investigaciones previas)
Pisan	Procedimiento de Imposición de Sanciones
PNT	Plataforma Nacional de Transparencia
PPD	Procedimiento de Protección de Derechos

Pronadatos	Programa Nacional de Protección de Datos
PV	Procedimiento de Verificación
Recomendaciones de Seguridad	Recomendaciones en materia de seguridad de datos personales para el sector privado
Reforma constitucional de transparencia	Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en materia de transparencia publicado el 7 de febrero de 2014
RGPD	Reglamento General de Protección de Datos Personales Europeo
Repep	Registro Público para Evitar Publicidad
Reus	Registro Público de Usuarios que no deseen información publicitaria de productos y servicios financieros
RI	Recurso de Inconformidad
RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
RRSN	Recurso de Revisión en Materia de Seguridad Nacional
RV	Recurso de Revisión
SCJN	Suprema Corte de Justicia de la Nación
SEPD	Supervisor Europeo de Protección de Datos
SGSDP	Sistema de Gestión de Seguridad de Datos Personales
SMVDF	Salario Mínimo Vigente en el Distrito Federal
SNT	Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales
SPD	Solicitud de Protección de Datos
SPDP	Secretaría de Protección de Datos Personales
TCA	Tribunal Constitucional Alemán
TCE	Tribunal Constitucional Español

TEDH	Tribunal Europeo de Derechos Humanos
TFJA	Tribunal Federal de Justicia Administrativa
TIC	Tecnologías de la información y las comunicaciones
TJUE	Tribunal de Justicia de la Unión Europea
UMA	Unidad de Medida y Actualización
UT	Unidad de Transparencia

LISTA DE AUTORES

Autor	Institución a la que pertenece
Alday González, Alejandro	Secretaría de Relaciones Exteriores
Barco Vega, Gregorio	Instituto Tecnológico Autónomo de México
Carbonell Sánchez, Miguel	Centro de Estudios Jurídicos Carbonell
Carrera Méjan, Luis Manuel	Instituto Tecnológico Autónomo de México
Cervantes Padilla, Alexis	Instituto Tecnológico Autónomo de México
Davara F. De Marcos, Isabel	Instituto Tecnológico Autónomo de México
Esquenazi Franco, Jacobo	HP Inc.
Ferrer Mac-Gregor Poisot, Eduardo	Corte Interamericana de Derechos Humanos
Fragoso Rodríguez, Uciel	Instituto Tecnológico Autónomo de México
Franco Velázquez, Rosa María	International Association of Privacy Professionals
Garzón Galván, Jonathan Gabriel	Instituto Tecnológico Autónomo de México
Gómez Ruano, Sofía	Consejo Consultivo del Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales
González Granados, Patricio	Instituto Tecnológico Autónomo de México
González Mejía, Jesús Eulises	Instituto de Investigaciones Jurídicas (UNAM)

Guillén Lara, Denise	Consejo Consultivo del Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales
Hidalgo Ezquerra, Faustino Gerardo	Magistrado del Tribunal Federal de Justicia Administrativa
Huesca Morales, Erik	Fundación para el Conocimiento y Cultura Digital
Islas López, Jorge	Universidad Nacional Autónoma de México
López Ayllón, Sergio	Centro de Investigación y Docencia Económicas
López López, Gabriel	Instituto Tecnológico Autónomo de México
Maqueo Ramírez, María Solange	Centro de Investigaciones y Docencia Económicas Consejo Consultivo del Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales
Marván Laborde, María	Instituto de Investigaciones Jurídicas (UNAM) Comisionada Presidenta fundadora del Instituto Federal de Acceso a la Información y Protección de Datos
Mendoza Enríquez, Olivia Andrea	Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (Infotec)
Moreno González, Jimena	Centro de Investigación y Docencia Económicas
Orta Villar, Jorge Antonio	Instituto Tecnológico de Estudios Superiores de Monterrey
Paredes González, Christian	SAP México
Pérez de Acha, Luis Manuel	Comité Ciudadano del Sistema Nacional Anticorrupción
Pérez Cirera Santacruz, Daniel Antonio	Samsung México
Salazar Ugarte, Pedro	Instituto de Investigaciones Jurídicas (UNAM)
Soto Galindo, José	Periódico *El Economista*
Trinidad Zaldívar, Ángel	Consultor Comisionado del Instituto Federal de Acceso a la Información y Protección de Datos
San Martín Rebolloso, Marina	Comisionada ciudadana del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (InfoCDMX)

Tron Petit, Jean Claude	Magistrado del Cuarto Tribunal Colegiado en materia Administrativa del Primer Circuito
Tron Zuccher, Denise	Pérez de Acha Ibarra de la Rueda Abogados
Tsuru Alberu, Kiyoshi	Instituto Tecnológico Autónomo de México
Velázquez Olavarrieta, Andrés	Investigaciones Digitales de MaTTica

PRESENTACIÓN

Dra. Isabel Davara F. de Marcos

Decir que para mí es un gran honor y una enorme responsabilidad la encomienda de coordinar este diccionario por parte del Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI) se queda indudablemente muy corto.

Agradezco con todo el corazón la impresionante generosidad de los renombrados colaboradores de esta obra. El lector, sin duda, podrá reconocer con facilidad que se encuentran los más brillantes y más reputados especialistas de nuestro país en la materia.

Además, no es menor mi agradecimiento a mi equipo de colaboradores más cercanos. Es obvio que una obra de esta magnitud y calado requiere de una gran ayuda y disposición de un equipo que ha hecho que este retador proyecto sea posible. No quiero dejar pasar estas líneas sin agradecer a Gregorio Barco Vega, Alexis Cervantes Padilla, Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez su inestimable apoyo y colaboración.

Este diccionario es una obra inédita, no sólo en México, sino internacionalmente. Seleccionar los términos y el alcance de los mismos no ha sido una tarea fácil, y aunque probablemente habrá muchas cosas que se puedan mejorar, fue un proceso de extensa dedicación, procurando cubrir, a lo largo de más de 200 voces, con más de 30 autores, conceptos fundamentales relativos a la protección de datos personales y otros con una mayor interrelación con otras materias.

El derecho a la protección de datos personales fue reconocido constitucionalmente en nuestro país en junio de 2009. Desde entonces ha habido muchos otros hitos normativos de diferente relevancia, contando en la actualidad con un detallado y específico marco regulatorio, tanto a nivel público como privado. Esta obra pretende abarcar las dos esferas regulatorias, así como exponer las tendencias internacionales más relevantes que puedan, en cada concepto, ayudar a entender e interpretar mejor su alcance y contenido.

La aproximación a cada voz ha pretendido cumplir con altos estándares de calidad y objetividad en la explicación de los términos. Uno de los principios rectores al aproximarnos a cada uno de ellos ha sido recoger, en la medida de lo posible, todas aquellas fuentes legales y normativas que exponen cada voz, cuando así existen, de manera que el lector pueda encontrar un compendio de las referencias ahí establecidas y así poder contar con una visión, lo más comprehensiva posible, de cada una de las voces.

Como decíamos, seguro hay espacio para muchas mejoras en el tiempo, pero consideramos que esta obra es, con un importante nivel de detalle, un excelente punto de partida para todo aquél que requiera contar con referencias precisas sobre las principales instituciones del derecho a la protección de datos personales en México.

Reitero mi más profundo agradecimiento al INAI por el encargo de liderar esta magna tarea, espero que la obra satisfaga las más altas expectativas y cumpla el propósito de fomentar y fortalecer la cultura de la protección de datos personales en México y en la región.

Davara F. de Marcos, Isabel

Coordinadora de esta obra. Doctora en derecho y licenciada en ciencias económicas y empresariales, por la Universidad Pontificia Comillas de Madrid. Abogada practicante en México y en España. Socia fundadora del despacho DAVARA ABOGADOS, boutique legal especializada en derecho de las tecnologías de la información y las comunicaciones. Profesional certificada en privacidad en Estados Unidos, Europa y gestión de proyectos y reconocida como líder de privacidad por la International Association of Privacy Professionals (CIPP/E/US, CIPM & FIP). Profesora y coordinadora en postgrado en el ITAM y profesora invitada en diversas instituciones académicas nacionales y extranjeras. Ha participado como conferencista y panelista en más de 300 foros especializados en derecho de las TIC nacional e internacionalmente. Autora y coautora de más de 15 libros, y más de 150 artículos y ensayos en la materia a nivel nacional e internacional.

Alday González, Alejandro

Licenciado en derecho, egresado de la Universidad Iberoamericana. Cuenta con estudios especializados en derecho internacional público, en la Academia de Derecho Internacional de La Haya, el Instituto Interamericano de Derechos Humanos en San José, Costa Rica, y en sistema jurídico estadounidense, en el programa de Educación Continua de la U.N.A.M. Es miembro de carrera del Servicio Exterior Mexicano desde el año de 1998. Actualmente es el director general del Instituto Matías Romero. En representación de México, ha sido negociador en varias convenciones internacionales en el marco de la OEA, la ONU y el Consejo de Europa. Además, fue el jefe negociador para la delimitación de las fronteras marítimas de México con Cuba y Estados Unidos en el Golfo de México, en el 2016, y ha sido agente ante la Corte Interamericana de Derechos Humanos y asesor principal en la Asamblea de los Estados Parte de la Corte Penal Internacional.

Barco Vega, Gregorio

Es licenciado y maestro en derecho por la UNAM. Docente del Diplomado de Derecho de las TIC del Instituto Tecnológico Autónomo de México (ITAM). Abogado especializado en derecho de las TIC en Davara Abogados S.C. Cuenta con experiencia en materias como protección de datos personales, telecomunicaciones, firma electrónica, contratos electrónicos y *FinTech*. Autor y coautor de diversas publicaciones entre las que destacan *Repercusiones jurídicas de las TIC* (2019), *FINTECH, Análisis a detalle de las innovaciones en la industria de los servicios financieros* (2019), *Cómo garantizar la protección de los datos personales* (2017), *El Mundo del Comercio Electrónico Bajo la Ley* (2017) *y El derecho humano a la protección de datos personales en México* (2016).

Carbonell **Sánchez, Miguel**

Es licenciado en derecho (UNAM) y doctor en derecho constitucional (Universidad Complutense de Madrid). Además es investigador Nacional nivel III del Sistema Nacional de Investigadores e investigador en el IIJ-UNAM.

Carrera **Méjan, Luis Manuel**

Académico en ITAM, doctor en derecho (UNAM). Profesor normalista, maestro en educación cívica y social. Licenciado en derecho. Investigador nivel 1 del SIN (CONACYT). Por treinta años abogado de Banco Nacional de México S.A. donde fue director de asesoría jurídica y prosecretario del Banco y del grupo financiero. Presidió el Comité Jurídico de la Asociación de Banqueros de México, de junio 2000 hasta diciembre de 2009 fue director general del IFECOM y presidió la International Association of Insolvency Regulators. Miembro de la Barra Mexicana, Colegio de Abogados A. C. y varias asociaciones profesionales internacionales, representa a México en la CNUDMI y en el Grupo ad hoc del Banco Mundial.Es confereciante en eventos académicos en múltiples países. Autor de una docena de libros y múltiples artículos en revistas especializadas de México y el extranjero.

Cervantes **Padilla, Alexis**

Licenciado en derecho por el Instituto Tecnológico Autónomo de México (ITAM) y Maestro en derecho económico por la Universidad Panamericana (UP). Es especialista en derecho de las TIC y en privacidad y protección de datos personales. Parte del equipo de Davara Abogados y apoyo externo para TMI Abogados. Cuenta con preparación especializada en propiedad intelectual, argumentación jurídica, juicios orales y derecho de las TIC. Es coautor del libro *Comentarios a la Ley Federal de Protección de Datos Personales en Posesión de Particulares*. Es profesor del ITAM y del Master Internet Business en materias de privacidad, protección de datos personales, comercio electrónico y *fintech*.

Esquenazi Franco, Jacobo

Tiene 20 años de experiencia en los aspectos regulatorios e implementación de protección de datos personales y privacidad. Actualmente se desempeña como estratega global de protección de datos personales para HP Inc. Se encarga de desarrollar la estrategia e implementación del programa global de protección de datos personales de la empresa. Cuenta con diversas certificaciones en la materia, incluida la de "Fellow of Information Privacy" de la Asociación Internacional de Profesionales de Privacidad (IAPP). Ha contribuido al debate sobre regulación de la privacidad y la protección de datos en diversos países como experto invitado y participa actualmente de manera activa en los trabajos de organismos internacionales en la materia.

Ferrer Mac-Gregor Poisot, Eduardo

Es presidente de la Corte Interamericana de Derechos Humanos, investigador titular por oposición en el Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (UNAM) y profesor de la Facultad de Derecho de la misma Universidad. Investigador nivel III del Sistema Nacional de Investigadores del Conejo Nacional de Ciencia y Tecnología (CONACYT). Laboró en la Suprema Corte de Justicia de la Nación y en otros tribunales del Poder Judicial de la Federación. Ha sido profesor, investigador visitante o conferencista en universidades y centros de investigación en Estados Unidos, Latinoamérica y Europa.

Fragoso Rodríguez, Uciel

Tiene estudios de ingeniería electrónica con especialidad en sistemas digitales en la Universidad Autónoma Metropolita. Tiene una maestría en ciencias de la computación en el Colegio Imperial de Londres Inglaterra. Obtuvo el grado de doctor con especialidad en informática en el Instituto Nacional de Telecomunicaciones en Francia. Actualmente, es coordinador de redes y telecomunicaciones de la Dirección de Servicios Tecnológicos e Informáticos del ITAM. En la parte académica, ha sido profesor en las asignaturas de: Redes de Computadoras y Seguridad Informática en la licenciatura, maestría y extensión universitaria del ITAM. Ha participado como asesor técnico en Transparencia Mexicana. Las áreas de interés son: tecnologías de redes y telecomunicaciones y seguridad de la información.

Franco Velázquez, Rosa María

Directora para América Latina de la International Association of Privacy Professionals (IAPP). Es abogada por el Instituto Tecnológico Autónomo de México (ITAM), especialista en propiedad intelectual, privacidad y protección de datos; certificada por la IAPP, desde el 2012, como Certified Information Privacy Professional(CIPP/US). Cuenta con un LL.M por The George Washington University, en Washington DC. Es socia de Axkati Legal, S.C., donde encabeza la práctica de privacidad y protección de datos. Ha participado como ponente en diferentes conferencias, incluyendo IAPP Privacy Summit y el International Privacy Law Forum. Who´s who legal Mexico 2015 se refiere a ella como: "Una fantástica abogada en materia de protección y privacidad de datos personales. Sus compañeros la consideran una de las más inteligentes y profesionales expertas en el mercado".

Garzón Galván , Jonathan Gabriel

Abogado especialista en tecnología y sistema financiero. Es licenciado en derecho por la Barra Nacional de Abogados y licenciado en ciencia política y administración pública por la UNAM, ambos grados con mención honorifica. Cuenta con los grados de maestro en Derecho de la Empresa con mención honorífica, por la Universidad Panamericana y maestro en comercio electrónico por el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM). En 2107 concluyó el programa de perfeccionamiento directivo en el IPADE y en 2019 cursó el programa ejecutivo de Liderazgo en la Innovación del Instituto Tecnológico de Massachussets (MIT). Cuenta con más de 10 años de experiencia docente a nivel posgrados en diversas instituciones como: ITAM, La Salle, Universidad Iberoamericana, Universidad Panamericana e ITESM, Escuela Libre de Derecho de Sinaloa.

Gómez Ruano, Sofía

Consejera consultiva honoraria del Instituto Nacional de Transparencia, Acceso a la Información y Datos Personales (INAI), por el periodo 2017-2020. Socia fundadora del despacho Abogados Ortega y Gómez Ruano, en el que su práctica profesional se centra en las áreas de protección de datos personales, y solución alternativa de controversias actuando como mediadora, árbitro y abogada de parte en disputas nacionales e internacionales. Egresada de la Universidad Panamericana, certificada como experta en protección de datos personales por NYCE México, integrante de la Asociación Internacional de Profesionales en Privacidad (IAPP) y profesora en el Diplomado en Derecho de las TIC de la Asociación Mexicana de Derecho Informático (AMDI).

González Granados, Patricio

Abogado especializado en propiedad intelectual con amplia experiencia en litigio administrativo y constitucional. Actualmente asesora clientes en asuntos de propiedad industrial, derechos de autor, videojuegos, derecho a la propia imagen, protección de nuevas tecnologías, derechos digitales, comercio electrónico, nombres de dominio, competencia económica, derecho del entretenimiento y del deporte. Es egresado del Instituto Tecnológico Autónomo de México (ITAM) y tiene una maestría en Propiedad Intelectual y Competencia Económica por la University College London (UCL).

González Mejía, Jesús Eulises

Es licenciado en derecho por la Facultad de Derecho de la Universidad Nacional Autónoma de México (UNAM), ha cursado diplomados especializados en acceso a la información y protección de datos personales. Actualmente cursa la Maestría en Derecho también en la UNAM. Se ha desempeñado como jefe de departamento adscrito a la Secretaría de Protección de Datos Personales del Instituto Nacional de Acceso a la Información y Protección de Datos Personales y actualmente funge como enlace de Transparencia y Archivo del Instituto de Investigaciones Jurídicas (IIJ-UNAM). Aunado a las labores como enlace de IIJ, ha colaborado en la elaboración de investigaciones académicas en materia de Transparencia, Archivo y Protección de Datos Personales.

Guillén Lara, Denise

Miembro del Consejo Consultivo del INAI (2017-2019). Es vicepresidente jurídico, líder de integridad y líder de Women in Nielsen para Latinoamérica. Es miembro de la Junta Menor del INCAM, consejera fundadora de AbogadasMX, miembro del Consejo de Centro Mexicano Pro Bono. The *GC Powerlist* la reconoció como una de las abogadas de empresa más influyentes para México. The *Corporate Counsel 100* la reconoció como una de los 100 abogados de empresa que demostraron ser más influyentes e innovadores en Latinoamérica. Foro Jurídico la reconoció como una de las abogadas más influyentes en México. Se graduó con honores de la Facultad de Derecho de Universidad La Salle, estudió Manejo de Crisis en MIT, Management para Abogados en Yale y Negociación Avanzada en Harvard.

Hidalgo Ezquerra, Faustino Gerardo

Licenciado en derecho por la Universidad Popular Autónoma de Puebla. Ha participado en el transcurso de 39 años en múltiples diplomados, cursos de actualización, talleres y congresos nacionales e internacionales, en materia de derecho fiscal y administrativo, jurisdiccional de tecnología y de administración. Ha sido expositor en diversos foros nacionales e internacionales de diversos temas de derecho fiscal, administrativo y jurisdiccionales, y recientemente sobre el Proyecto de Juicio en Línea y el Sistema de Justicia en Línea del Tribunal Federal de Justicia Administrativa. Autor de diversas publicaciones en las áreas en las que desarrolla su práctica. Es miembro del Colegio Nacional de Profesores e Investigadores de Derecho Fiscal, y Finanzas Públicas, A.C., de la Academia Mexicana de Derecho Fiscal A.C. y miembro fundador de la Academia de Derecho Fiscal de Yucatán A.C.

Huesca Morales, Erik

Presidente de la Fundación para el Conocimiento y la Cultura Digital (FUNCO), dedicada al estudio e investigación de nuevas formas de conocimiento y el desarrollo de las culturas digitales. Es miembro del consejo consultivo del Instituto Federal de Telecomunicaciones. Formó parte del equipo que introdujo Internet a México, fundador del primer centro privado de investigación de inteligencia artificial. Fue presidente de la Academia Mexicana de Informática y fundador del capitulo mexicano de la Internet Society. Diseñó múltiples redes de internet para universidades, operadores y países de América Latina Recibió en 2015 y 2016 el reconocimiento por parte del Hispanic IT Executive Council (HITEC) como uno de los 50 latinos más influyentes en la industria en Latinoamérica y España.

Islas López, Jorge

Es cónsul general de México en Nueva York por la designación del presidente Andrés Manuel López Obrador y la ratificación unánime del Senado de la República, que se realizó el 20 de marzo de 2019. Tomó posesión de este cargo el 3 de mayo de 2019. Es reconocido a nivel nacional, tanto en el sector público como privado, por su experiencia en derecho constitucional y como defensor de derechos humanos. Ha trabajado para promover el derecho de los televidentes como defensor de audiencias del canal del Congreso; así como para velar por derechos ambientales. Es autor de la primera disposición legal de los derechos de la Madre Tierra en la legislación mexicana. Redactó la primera legislación federal en México referente a acciones colectivas (2008-2009) y a transparencia y acceso a la información pública (2002). Profesor de Derecho Constitucional en la UNAM y en el Instituto Tecnológico Autónomo de México (ITAM).

López Ayllón, Sergio

Es doctor en derecho por la Universidad Nacional Autónoma de México. Obtuvo su maestría en sociología del derecho y relaciones sociales en la Universidad de Paris II. Es profesor investigador del Centro de Investigación y Docencia Económica (CIDE) donde actualmente se desempeña como director general. Es miembro del Sistema Nacional de Investigadores (nivel III) y de la Academia Mexicana de Ciencias. Es autor de varios libros y ha publicado numerosos artículos y capítulos de libros tanto en México como en el extranjero en materia de derecho a la información y transparencia, regulación y sociología del derecho. En la administración pública federal ha desempeñado varios cargos, además ha sido consultor de la Suprema Corte de Justicia de la Nación, la H. Cámara de Diputados, la H. Cámara de Senadores, la Secretaría Economía, la Secretaría de la Función Pública, el Instituto Federal de Acceso a la Información, entre otras instituciones.

López López, Gabriel

Licenciado en derecho por el Centro Universitario México, División Estudios Superiores, A.C. Maestro en derecho fiscal por la Universidad Panamericana, A.C. Oficial de cumplimiento certificado por la Comisión Nacional Bancaria y de Valores. Socio de Martínez y de Labra, S.C. Abogado of Counsel de Davara Abogados, S.C. Oficial de Cumplimiento de Operadora de Servicios Mega, S.A. de C.V. SOFOM E.R. Compliance Officer para Mota-Engil México, S.A.P.I. de C.V. Profesor en el Diplomado de Tecnologías de la Información del ITAM.

Maqueo Ramírez, María Solange

Presidenta del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Obtuvo el grado de doctora en el programa Estado de Derecho y Políticas Públicas y la Cátedra Jean Monnet de la Universidad de Salamanca, España. Abogada por la Escuela Libre de Derecho con mención honorífica en el examen profesional. Actualmente es directora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). Miembro del Sistema Nacional de Investigadores, distinción que otorga el CONACYT y líder de derechos digitales del Centro de Política Digital para América Latina (Centro LATAM Digital).

Marván Laborde, María

María Marván Laborde estudió en la UNAM sociología y se graduó de maestría y doctorado en la New School for Social Research, de la ciudad de Nueva York en los EEUU. Fue comisionada del Instituto Federal de Acceso a la Información Pública del 2003 al 2011 y comisionada presidenta desde su fundación hasta el 2006. Además fue consejera del Instituto Federal Electoral del 2011 al 2014. Ha sido catedrática en diversas instituciones de educación superior como son la UNAM, el ITAM, la U de G, el ITESO y la UP. Desde septiembre de 2014 se reintegró a la vida académica como investigadora de tiempo completo en el Instituto de Investigaciones Jurídicas de la UNAM. Desde enero de 2015 es la presidenta del Consejo de Transparencia Mexicana.

Mendoza Enríquez, Olivia Andrea

Es licenciada en derecho, maestra en derecho con especialidad en Derecho Económico y doctora en derecho con distinción *Ad Honorem* por la Benemérita Universidad Autónoma de Puebla. Especialista en derechos humanos por la Universidad Castilla-La Macha (UCLM), España. Cuenta con un máster en derechos humanos por la misma institución. Profesora investigadora del Centro de Investigación y Docencia Económicas (CIDE). Miembro del Sistema Nacional de Investigadores, nivel I. Su línea de investigación es regulación y tecnología. Colaboradora en el Observatorio Iberoamericano de Datos Personales. Profesora invitada de la DEC de la Facultad de Derecho la UNAM, de la Escuela Libre de Derecho, de la Universidad Iberoamericana campus Santa Fe y de la Universidad de Salamanca USAL, España. Participante del sector académico para la conformación de la Estrategia Nacional de Ciberseguridad para México.

Moreno González, Jimena

Abogada por la UNAM. Maestra en dirección internacional por el ITAM, con diplomado en Evaluación de Políticas Públicas y Dirección Estratégica por el Centro de Investigación y Docencia Económicas (CIDE), cuenta con un curso en derecho constitucional por la Universidad de Berkeley, California. Actualmente es secretaria de vinculación del CIDE, y profesora de la materia de Derecho Internacional Público, de Privacidad y Protección de Datos Personales. Dirige el Diplomado de Privacidad, Regulaciòn y Governanaza de Datos. Ha impartido diversos cursos sobre transparencia, acceso a la información y protección de datos personales. Especialista en regulación, acceso a la información, privacidad, datos personales y derecho internacional público. Miembro del equipo de Centro Latam Digital, del CIDE. Es coautora del *Manual de Derecho Internacional Público*, y de artículos en revistas internacionales sobre arbitraje en inversiones, educación jurídica, proteccion de datos personales, cómputo en la nube, competitividad y economía del internet.

Orta Villar, Jorge Antonio

Cuenta con 24 años de experiencia como consultor juridico de empresas y abogado litigante. En su trayectoria ha incursionado tanto en el sector público como en el privado, especializándose en las ramas civil, mercantil, así como en diversas sub especialidades de derecho administrativo. Tiene 16 años colaborando con el Instituto Tecnológico y de Estudios Superiores de Monterrey, en el cual se ha desempeñado como abogado general y al mismo tiempo ha participado en diversas cátedras para dicho Instituto.

Paredes González, Christian

Es abogado egresado de la Universidad La Salle, campus Ciudad de México. Cuenta con 15 de años de trayectoria como especialista en derecho de las tecnologías de la información. Es director de Integridad y Cumplimiento de SAP México, también es el coordinador del área de Datos Personales y Privacidad de la empresa. Es coordinador de la Comisión de Derecho de Tecnologías de la Información en la Barra Mexicana Colegio de Abogados, A.C. Ha sido incluido desde el año 2017 en la publicación *GC PowerList Mexico* como uno de los abogados corporativos más innovadores de la industria.

Pérez de Acha, Luis Manuel

Abogado por la Escuela Libre de Derecho y doctor en derecho por la UNAM. Experto en derecho constitucional, fiscal y administrativo. Integrante del Comité de Participación Ciudadana del Sistema Nacional Anticorrupción de 2017 a 2019.Catedrático de la UNAM, Escuela Libre de Derecho, CIDE, ITAM, Universidad Panamericana, Universidad Anáhuac, Universidad Iberoamericana e Instituto Politécnico Nacional. Articulista en *New York Times*, *Reforma, Universal*, *Excélsior*, *El Economista*, *Animal Político*, *Forbes México*, *Expansión*, *Nexos*, *Este País y Tax Notes International*. Autor de las monografías: *Establecimiento Permanente*, *Beneficios Empresariales*, *Estudios Tributarios*, *Protección Constitucional en las Visitas Domiciliarias y Expropiación en México*.

Pérez-Cirera Santacruz, Daniel Antonio

Es director jurídico, oficial de cumplimiento y encabeza el área de relaciones con gobierno de Samsung México. El licenciado Pérez-Cirera es abogado por la Escuela Libre de Derecho donde se graduó con doble mención honorífica y Maestro en Finanzas Corporativas y Derecho por la Universidad de Northwestern donde se graduó *Cum Laude*. Perez-Cirera trabajó previamente en Ingersoll Rand Mexico como director jurídico, oficial de cumplimiento y jefe de privacidad y estuvo encargado de implementar un departamento jurídico y de cumplimiento regional. Asimismo, estuvo a cargo del departamento jurídico de Nokia en México, antes de enfocarse en el mundo corporativo trabajó en la firma Galicia Abogados en CDMX y Davis Polk en la ciudad de Nueva York, entre otras prestigiadas firmas en México y el extranjero. Es un apasionado expositor en conferencias y seminarios sobre temas de cumplimiento.

Salazar Ugarte, Pedro

Pedro Salazar Ugarte es licenciado en derecho por el Instituto Tecnológico Autónomo de México y doctor en filosofía política por la Universidad de Turín, Italia. Investigador de tiempo completo del Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México (desde 2003). Fue secretario académico de ese Instituto de 2008 a 2010 y secretario de su consejo interno durante el mismo periodo. Director del IIJ de 2014 a 2018 en un primer periodo; y de 2018 a la fecha en un segundo periodo. Es miembro del Sistema Nacional de Investigadores (Nivel III).

Soto Galindo, José

Periodista especializado en tecnologías de la información, telecomunicaciones y protección de datos personales. Es maestro en transparencia y protección de datos personales por la Universidad de Guadalajara. Desde 2010 dirige la edición digital de *El Economista*, con sede en la Ciudad de México. Ha colaborado en *Milenio Jalisco*, *Expansión*, *Magis*, *Gatopardo*, *Vice*, *Zona de Obras* y *Zócalo*. Escribe la columna *Economicón*, que se publica semanalmente en *El Economista* y en http://economicon.mx

Trinidad Zaldívar, Ángel

Licenciado en derecho y especialidad en finanzas públicas por la UNAM. Maestro en administración y gobierno con mención honorífica por la BUAP. Actualmente es miembro del Comité de Participación Ciudadana del Sistema Anticorrupción CDMX. Ha ocupado, entre otros, los siguientes cargos: sub comisionado jurídico y coordinador de delegaciones en el Instituto Nacional de Migración; consejero del consejo consultivo del canal del Congreso; titular de la Unidad de Sistemas, Información y Transparencia de la Auditoría Superior de la Federación; secretario ejecutivo y posteriormente comisionado del IFAI; secretario técnico de la Conferencia Mexicana de Acceso a la Información Pública (COMAIP); coordinador de enlace interinstitucional de la presidencia de la República. Ha publicado artículos y ensayos en libros, revistas y periódicos.

San Martín Rebolloso, Marina

Comisionada ciudadana del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. Es licenciada en derecho por la UNAM, con un máster por el Instituto Universitario de Investigación Ortega y Gasset y un máster universitario por la Universidad de Alcalá, España. Se ha especializado en temas de transparencia, acceso a la información, protección de datos personales y rendición de cuentas, desempeñando distintos cargos de dirección y coordinación en el IFAI/INAI y en la ASF. Ha sido profesora de maestría y diplomados en universidades e instituciones educativas públicas y privadas. Cuenta con publicaciones especializadas en transparencia y artículos en prensa y revistas.

Tron Petit, Jean Claude

Egresado de la UNAM. Especialidad y master en Argumentación Jurídica por la Universidad de Alicante. Catedrático en el Instituto de la Judicatura del Poder Judicial de la Federación, en el CIDE, en la UNAM, Universidad Panamericana, en la Escuela Libre de Derecho y en el ITAM. Autor de varias obras jurídicas. Magistrado integrante del cuarto tribunal colegiado en materia administrativa del primer circuito ha suscrito sentencias en el tema de Transparencia y en el tema de rendición de cuentas.

Tron Zuccher, Denise

Abogada egresada del Instituto Tecnológico Autónomo de México. Cursó el Diplomado en Análisis Político Estratégico en el Centro de Investigación y Docencia Económicas y la maestría en derecho administrativo y de la regulación en el Instituto Tecnológico Autónomo de México. Coautora del libro *Protección Constitucional en las Visitas Domiciliarias* y autora de diversos artículos. Forma parte del despacho Pérez de Acha e Ibarra de Rueda desde 2003 y es responsable del área de investigación y publicaciones.

Tsuru Alberu, Kiyoshi

Egresado de la Universidad Iberoamericana. Cuenta con una especialidad en obligaciones y contratos por la Escuela Libre de Derecho, y una maestría en propiedad intelectual en la George Washington University. Obtuvo el premio Thelma Weaver Memorial al mejor alumno extranjero. Es socio fundador y director de TMI Abogados, despacho especializado en propiedad intelectual, tecnología y ciberespacio, y también funge como director general de BSA | The Software Alliance (México) y como árbitro de la Organización Mundial de la Propiedad Intelectual (OMPI).

Velázquez, Andrés

Ingeniero en cibernética y en sistemas computacionales por la Universidad la Salle. Presidente y Fundador de MaTTica, especialista en ciberseguridad y cómputo forense. La revista de negocios *Expansión* lo nombró recientemente uno de los 30 jóvenes en los treinta para liderar el cambio en México. Es coautor del libro *Normatividad Bancaria 2017* y de la Ley General de Protección de Datos Personales en Sujetos Obligados, comentada. Cuenta con certificaciones en ciberseguridad como la CISSP (Certified Information Systems Security Professional) y la IEM (Infosec Evaluation Methodology), así como en las principales herramientas especializadas para investigaciones digitales. Es considerado líder de opinión por medios escritos y televisivos donde participa de forma constante explicando los elementos vinculados a los delitos informáticos.

Acceso a la información pública

María Marván Laborde

El derecho de acceso a la información pública gubernamental debe considerarse como parte del derecho a la información que en México está consagrado en el artículo 6 de la Constitución de los Estados Unidos Mexicanos (CPEUM). El 6 de diciembre de 1977, en el contexto de la reforma política que se considera, dio inicio el proceso de transición democrática y se introdujo en este artículo la aseveración de que "el derecho a la información será garantizado por el Estado". Entre esa fecha y 2002, hubo muchas discusiones sobre la necesidad expedir una ley reglamentaria que le diera contenidos claros a este derecho social fundamental. Muchas fueron las interpretaciones de los jueces sobre los alcances que podría tener esa pequeña frase de tan solo diez palabras. Las interpretaciones previas a 2002 no estuvieron exentas de contradicción.[1]

La libertad de expresión y la libertad de prensa se entienden en principio como libertad negativa, lo que no debe hacer el Estado para limitar la libertad de las personas. En el siglo XXI se ha ampliado en México el alcance y significado del derecho a la información al incluir una serie de acciones positivas que imponen obligaciones para favorecer un ejercicio cabal de las libertades de buscar, recibir y/o difundir informaciones y opiniones.

El derecho de acceso a la información pública gubernamental impuso una serie de obligaciones administrativas y procedimentales a todos los entes del Estado mexicano para garantizar, de manera efectiva, el ejercicio de este derecho y facilitar a cualquier persona los medios cuasijurisdiccionales para poder defenderse de decisiones que consideren afecten sus derechos.

En junio de 2002, en el marco del primer gobierno de alternancia, se expidió la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) para reglamentar el derecho de acceso a la información del gobierno federal. En una clara ampliación de la concepción de la democracia se estableció que los ciudadanos tienen derecho a conocer cualquier documento gubernamental, y que el gobierno tiene la obligación de establecer mecanismos claros, sencillos y eficientes para facilitar el ejercicio de

1 Carpizo, J. y Carbonell, M. (comps.). (2000). "Derecho a la información y derechos humanos. Estudios en homenaje al maestro Mario de la Cueva". En López Ayllon, S. *El derecho a la información como derecho fundamental*. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México. México, p. 172.

este derecho. La transformación cultural de la burocracia, con respecto al manejo de la información al interior de las dependencias y entidades, debería dar un giro radical. Es connatural a la burocracia proteger la información y preferir el secreto administrativo partiendo de la premisa de Max Weber de que la información es poder, tiende a desarrollarse en todo burócrata la costumbre de informar lo menos posible a la ciudadanía sobre las actividades gubernamentales y el ejercicio de los recursos públicos.[2]

En el ámbito local las primeras entidades que emitieron leyes de acceso a la información fueron Sinaloa y Jalisco. Estas fueron emitidas antes que la ley federal. En 2007 todas las entidades de la República mexicana, habían expedido leyes en esta materia. Sin embargo, la heterogeneidad de concepciones, procedimientos, plazos e inclusive requisitos y costos para poder ejercer este derecho, sirvió como acicate para promover la reforma del artículo 6 de la CPEUM.[3]

El 20 de julio de 2007 se le adicionó un párrafo que estableció tres principios y cinco bases que deberían convertirse en parámetros obligatorios para todas las entidades, de tal manera que la garantía de acceso a la información gubernamental tuviera una base mínima para que todos los mexicanos, sin importar la entidad en la que vivieran, pudieran ejercer, de manera similar, su derecho. En contrapartida, cualquier gobierno estatal o municipal debería ser exigido de la misma manera que los demás.

La reforma constitucional de 2007 tuvo alcances limitados, ya que no todos los congresos locales se ciñeron estrictamente a los principios y las bases establecidas en el artículo 6 de la CPEUM. El 7 de febrero de 2014 se modificó nuevamente este artículo. A través de esta reforma, el instituto garante del acceso a la información se convirtió en un organismo constitucional autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio (artículo 6 apartado A fracción VIII). El Instituto Nacional de Transparencia Acceso a la Información Pública y Protección de Datos Personales (INAI) es la institución garante del acceso a la información y la protección de los datos personales y deberá regirse por los principios de certeza, igualdad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

Lo primero que establece el artículo 6 es que "toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y solo podrá ser reservada temporalmente por razones de interés público y seguridad nacional en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información".

El derecho de acceso a la información pública gubernamental en México se reconoce como un derecho fundamental. Es parte esencial de la relación democrática entre ciudadanos y gobernantes, por ello, es especialmente significativo que la primera ley en la materia se haya expedido por el primer gobierno de alternancia. Vicente Fox fue el primer presidente emanado del Partido Acción Nacional, derrotó al Partido Revolucionario Institucional que gobernó al país desde 1929 hasta el 2000. Dentro de sus propuestas de democratización

2 Guerrero, E. (2008). *La transparencia. Colección para entender*. México. Nostra, pp. 20-21.

3 Cfr. López, S. Coord. (2006). *Democracia, transparencia y Constitución. Propuestas para un debate necesario*. México. UNAM- IFAI.

del país estuvo la de garantizar el acceso a la información gubernamental. Gracias a una venturosa coincidencia con las aspiraciones de grupos de la sociedad civil organizada, académicos de diversas universidades y algunos medios de comunicación (prensa escrita primordialmente) fue posible la aprobación de la LFTAIPG en 2002.

Esta Ley establece que cualquier persona tiene derecho a solicitar información de cualquier gobierno y que el Estado tiene la "obligación positiva" de entregarla sin necesidad de "acreditar un interés directo para su obtención o una afectación personal".[4] La reforma de 2014, que amplió los alcances de este derecho, fue especialmente cuidadosa de incluir, en esta obligación, a cualquier persona física o moral que por cualquier razón recibiese dinero público, en el entendido de que uno de los objetivos primordiales de este derecho es poder saber y buscar información que revele la forma en la que los gobernantes gastan el dinero público y hacen uso de sus facultades.

Entre las obligaciones positivas del Estado están las de establecer mecanismos de acceso a la información y procedimientos de revisión para que las personas que hayan solicitado información y estén inconformes con la respuesta recibida tengan la posibilidad de quejarse ante una autoridad autónoma. Para poder exigir de manera efectiva este fundamental derecho ciudadano, los sujetos obligados tienen el mandato expreso de la CPEUM de documentar todas y cada una de sus decisiones y actividades, especialmente en lo que se refiere al ejercicio de recursos públicos. Cualquier incumplimiento a la legislación puede ser sancionado administrativa e inclusive penalmente.

El derecho de acceso a la información pública gubernamental tiene restricciones como cualquier otro derecho fundamental. Debido a que desde la CPEUM se mandata a los jueces que han de interpretar la ley a decantarse siempre por la máxima publicidad, las restricciones tienen que estar escritas de manera expresa en ley, responder a un objetivo lícito y ser "necesarias en una sociedad democrática, lo que depende de que estén orientadas a satisfacer un interés público imperativo".

El límite legal reconocido es la información reservada, esta información es pública por su naturaleza pero que por alguna causa de interés general puede estar embargada por un tiempo determinado cuando se considere, justificadamente, que la publicidad puede causar un daño en la consecución de los objetivos últimos de determinada política pública.

Por otra parte, la información confidencial (artículo 6 apartado A, fracción II) es información que, a pesar de encontrarse en los archivos de cualquiera de los sujetos obligados, no es pública por su propia naturaleza, esta información está bajo resguardo del Estado porque le es indispensable para poder desempeñar sus funciones. La información confidencial es, por ejemplo, los secretos bancario, fiduciario, fiscal y postal, y los datos personales de los que nos ocuparemos más extensamente.

De la misma manera que garantizar a los ciudadanos acceso a cualquier documento del quehacer gubernamental es parte esencial de un gobierno que se precie de ser democrático, la protección de los datos personales es también un buen indicador de la madurez democrática de un determinado Estado. Para decirlo en palabras llanas, los ciudadanos tienen derecho a conocer todo lo que hace su gobierno y sus gobernantes, pero los gobernantes no deben entrometerse en la vida privada de los gobernados, más que el mínimo indispensable y siempre con una justificación legal y a veces, inclusive, constitucional.

4 López, S y Luna, I. (2016). *Derechos del pueblo mexicano. México a través de sus constituciones.* Volumen VI, sección tercera "Comentario al artículo 6". Cámara de Diputados-SCJN-TEPJF-CNDH-INE-Senado de la República-UNAM-IIJUNAM, p. 509.

En México, el derecho a la autodeterminación de los datos personales[5] está consagrado en el artículo 16 de la CPEUM desde el 1 de junio de 2009. En este artículo la CPEUM establece límites claros al Estado por los que no puede molestar a los ciudadanos en su ámbito privado sin una clara justificación legal y siguiendo un procedimiento expreso que garantice el respeto a los derechos humanos de los que goza toda persona.

La definición básica de datos personales dice que son información que concierne a una persona física, identificada e identificable. Esta información es confidencial y pertenece solo a esta persona, ella tiene derecho a tener control sobre esta información, ya bien sea que se encuentre en manos del Estado o en manos de particulares.

Para ello se han hecho dos ordenamientos distintos, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) expedida el 5 de julio de 2010 y la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO), expedida el 26 de enero de 2017. Esta última establece las normas que deberán seguir todos los sujetos obligados de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) cuando tengan en su poder bases de datos personales que sean indispensables para poder cumplir cabalmente con sus funciones.

El derecho humano a la información comprende el derecho de acceso a la información gubernamental y garantiza a los individuos la posibilidad de solicitar, investigar, difundir, buscar y recibir información —de manera particular la información sobre el quehacer del Estado—,[6] por ello fue necesario un ordenamiento específico que protegiera la información personal que se encuentra bajo resguardo de los sujetos obligados. El derecho de acceso a los datos personales forma parte de los derechos ARCO.[7]

Todo ente público o privado que posea, maneje y transforme bases de datos personales tiene la responsabilidad administrativa y penal que lo obliga a cuidar que nadie vulnere los derechos fundamentales de los gobernados al hacer mal uso de dichas bases, ya que cualquier descuido en el manejo de las mismas puede perjudicar a los individuos cuyos datos están contenidos en esas bases de datos. Por ello, la seguridad cibernética se convierte en un tema fundamental en esta materia.

Podemos decir entonces que el derecho de acceso a la información pública es la prerrogativa de toda persona para buscar información y acceder a bases de datos de información gubernamental de todos y cada uno de los entes del Estado mexicano. Las excepciones a este derecho deben ser mínimas y estar establecidas en la ley. Una excepción clara y tajante es el de los datos personales en posesión del Estado, a estos solo puede acceder el titular de los mismos.

5 En Europa, el derecho a la autodeterminación sobre los datos personales es considerado un derecho fundamental. En México se desarrolló a partir de las leyes de acceso a la información pública gubernamental con una fuerte influencia de la legislación española en la materia, así como de la cercanía del Instituto Federal de Acceso a la Información Pública y Protección de Datos con la Agencia Española de Protección de Datos.

6 Artículo 6 de la CPEUM.

7 Artículo 16 de la CPEUM.

Acciones para la seguridad de los datos personales

Uciel Fragoso Rodríguez

El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) en su artículo 61[8] propone un conjunto de acciones para establecer y mantener la seguridad de los datos personales. Se entiende como "acciones" al conjunto de actividades que debe realizar el responsable para salvaguardar la seguridad de los datos personales bajo su custodia.

La seguridad de los datos personales implica garantizar tres aspectos conocidos como triada de la información:

a) confidencialidad
b) integridad
c) disponibilidad

La confidencialidad de los datos personales consiste en que únicamente las entidades autorizadas tengan acceso a ellos. Garantizar la integridad implica que los datos personales solo podrán ser creados, modificados o eliminados por aquellas personas, grupos o procesos que estén debidamente autorizados. Finalmente, la disponibilidad de los datos personales consiste en que puedan utilizarse en el momento y forma requerida.

La primera acción que debe realizar el responsable, es la elaboración de un inventario de datos personales, así como de los sistemas que le dan tratamiento. El inventario de datos personales debe categorizarse de acuerdo con lo establecido en la GSGSDP,[9] el cual define tres niveles: estándar, sensible y especial. El nivel estándar corresponde a la categoría de datos personales de identificación y de contacto y que tienen un nivel de riesgo inherente bajo. Los datos personales de nivel sensible son aquellos que permiten determinar la ubicación física como, los patrimoniales, de autenticación, los jurídicos, de salud, de creencias y los de opinión pública, esta categoría tiene un nivel de riesgo inherente medio. La última categoría, identificada como nivel especial corresponde a todo dato personal que, debido al contexto puede causar un daño directo al titular en caso de un uso no autorizado del mismo. Cabe mencionar que la categorización de los datos personales definidos en la *Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP) puede cambiar según el contexto de la organización, es decir, un dato personal clasificado como nivel estándar en un contexto normal, puede representar un alto riesgo para el titular, por lo que debiera clasificarse como nivel sensible o especial.

Una vez que se ha realizado el inventario de datos personales, la siguiente acción consiste en identificar el tipo de tratamiento que las personas le dan en el flujo de información dentro de los procesos de las organizaciones. El tratamiento de datos según se enlista en la GISGSDP es: obtención, almacenamiento, uso (acceso, manejo, aprovechamiento, monitoreo, procesamiento), divulgación (remisión, transferencia), bloqueo, cancelación, supresión o destrucción. El inventario de datos personales, junto con el tipo de tratamiento, permite realizar una matriz de responsabilidades en donde se correlacionan las diferentes categorías

8 DOF. (2011, diciembre). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 61. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

9 INAI. (2015, junio). *Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales*. pp. 14-15. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

de datos personales con el tipo de tratamiento que las personas realizan en base a sus funciones y obligaciones. La matriz de responsabilidades proporciona una amplia visibilidad para identificar los posibles riesgos en el tratamiento de los datos personales.

La siguiente acción enfocada a la seguridad de los datos personales es la realización de un análisis de riesgo que permite identificar los peligros y evaluar el nivel de riesgo hacia los datos personales. Existen diversas metodologías y estándares internacionales para la realización de un análisis de riesgo. El estándar ISO/IEC 27005[10] provee una guía para implementar un proceso orientado a la administración de riesgos. La publicación especial NIST 800-30[11] es una guía elaborada por el National Institute of Standards and Technology (NIST) para la implementación de un análisis de riesgo dentro de las organizaciones federales de los Estados Unidos, sin embargo, es una metodología que puede ser utilizada por cualquier organización a nivel mundial. Las metodologías antes mencionadas permiten realizar análisis de riesgo sobre cualquier activo que se quiera proteger, en este sentido, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) elaboró la Metodología de Análisis de Riesgo BAA (beneficio, accesibilidad y anonimidad del atacante) (MARBAA)[12] enfocada específicamente a la protección de datos personales.

Las metodologías de análisis de riesgo establecen un proceso sistemático que consiste en crear escenarios de riesgo identificando y correlacionando todos los elementos que intervienen en el riesgo como los son: activo (que en el presente contexto consiste en los datos personales), amenazas, vulnerabilidades, controles existentes e impactos o consecuencias. Una vez creados los escenarios de riesgo, se procede a evaluar cualitativa o cuantitativamente el riesgo mediante el establecimiento de parámetros como la probabilidad de ocurrencia, el nivel de impacto o de beneficio para el atacante.

El resultado de la evaluación de los escenarios de riesgo es una lista evaluada y priorizada de riesgos, los cuales deben ser sometidos a diferentes tratamientos. A cada escenario de riesgo se le puede dar un tratamiento diferente dependiendo de los requerimientos, recursos disponibles y situación contextual. Los tipos de tratamiento al riesgo pueden ser clasificados como: a) aceptación, b) eliminación, c) mitigación y d) transferencia.

Aceptar el riesgo consiste en seguir la operación sin la implementación de ninguna contramedida de seguridad, este caso ocurre con aquellos escenarios de riesgo que resultaron con un nivel bajo y que no amerita la inversión de recursos. Eliminar el riesgo implica, prácticamente, modificar radicalmente o borrar el proceso de tratamiento de datos personales. La mitigación del riesgo es la acción más ejecutada y consiste en la implementación de controles de seguridad con el objetivo de reducir el nivel de riesgo. La transferencia del riesgo implica pasar la operación de los procesos que tratan datos personales a un tercero, o en su defecto, adquirir un seguro que, en caso de ocurrencia de un incidente, compense el impacto generado.

Para aquellos escenarios de riesgo en los que se ha decidido el tratamiento de mitigación, se propone la implementación de controles de seguridad. Las medidas de seguridad aplicables a los datos personales pueden ser de tres tipos: a) tecnológicos, b) administrativos y c) de procedimiento.

---

10 Online Browsing Platform (OBP). (2011). ISO/IEC 27005. *Information technology –Security techniques– Information security risk management*. Recuperado de: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en

11 Stonebumer, G. et al. (2002, julio). *Risk Management Guide for Information Technology Systems*. NIST. Recuperado de: https://www.archives.gov/files/era/recompete/sp800-30.pdf

12 INAI. (2015, junio). *Metodología de Análisis de Riesgo BAA*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

Las medidas tecnológicas consisten en componentes de *hardware* o *software* que robustecen la infraestructura tecnológica que procesa los datos personales. En este sentido, existen tecnologías que inciden directamente en la protección de datos personales como los mecanismos de autenticación biométrica que evita el robo de la identidad digital o los mecanismos de cifrado que garantizan la confidencialidad de los datos personales. Las medidas de seguridad administrativa son aquellas que modifican, de alguna manera, la estructura organizacional. Como ejemplos podemos mencionar la correcta asignación de privilegios de acceso a los datos personales en función de los roles y responsabilidades de las personas o la separación de actividades para evitar conflictos de interés. Las medidas de seguridad de procedimiento implican modificaciones en las actividades que conforman los procesos de negocio de las organizaciones y básicamente consisten en eliminar o mejorar las tareas en donde se detecten peligros en el tratamiento de datos personales.

Para seleccionar las medidas o controles de seguridad se hace uso de guías o mejores prácticas reconocidas a nivel internacional como el ISO/IEC 27002,[13] el NIST 800-53[14] o el CIS CSC.[15] Las guías de selección de controles de seguridad agrupan un conjunto de controles tecnológicos, administrativos o de procedimiento en categorías o familias funcionales que básicamente describen la operación de cada control y proporcionan una breve explicación de su implementación. En realidad ofrecen una guía sobre qué debe utilizarse para mitigar el riesgo, pero cómo debe implementarse y ponerse en operación depende de cada organización. Es importante que durante el proceso de selección de medidas de seguridad se realice un análisis de brecha que consiste en diferenciar entre los controles requeridos y los existentes para permitir una correcta selección de los mismos.

Una vez realizado el análisis de brecha, la siguiente acción para la seguridad de los datos personales es la elaboración de un plan de trabajo de las medidas de seguridad faltantes. El plan de trabajo está compuesto por programas de seguridad cuya implementación debe gestionarse mediante alguna guía de administración de proyectos. Los programas de seguridad pueden tener un enfoque totalmente tecnológico como un sistema de autenticación de doble factor basado en tecnología biométrica o ser programas de seguridad completamente administrativos como campañas y talles de concientización sobre la protección de datos personales.

La implementación de las medidas de seguridad no garantiza por sí misma la mitigación del riesgo sobre los datos personales, es necesario monitorear y revisar periódicamente la efectividad de los controles de seguridad, para ello se requiere definir métricas de desempeño conocidas como KPIs (*Key Performance Indicator*). Para cada control de seguridad se debe evaluar su desempeño y comparar con valores objetivos, de tal forma que si no se está logrando el desempeño requerido, deberán realizarse los ajustes necesarios para corregir o, en un caso extremo, hacer un cambio radical.

Debido a que día a día surgen nuevas amenazas y formas de ataque hacia los datos personales es necesario que las acciones hasta ahora descritas para la seguridad de los datos personales se sistematicen en un proceso de mejora continua denominado Sistema de Gestión de Seguridad de Datos Personales (SGSDP).

---

13 Online Browsing Platform (OBP). (2013). *ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security controls.* Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

14 Joint task force transformation initiative. (2013, abril). *Security and Privacy Controls for Federal Information Systems and Organizations*. NIST. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

15 Center for Internet Security. (2016, Agosto). *The CIS Critical Security Controls for Effective Cyber Defense*. Disponible en: https://www.tml.org/DocumentCenter/View/71/The-CIS-Critical-Security-Controls-Effective-Cyber-Defense-PDF

La guía para implementar un Sistema de Gestión de Seguridad de Datos Personales propuesta por el INAI se basa en el modelo de cuatro fases denominado Planificar-Hacer-Verificar-Actuar (PHVA) que establece, de la siguiente manera, las actividades para cada fase:

Planificar	Se identifican las políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por la organización (meta).
Hacer	Se implementan y operan las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
Verificar	Se evalúan y miden los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.
Actuar	Se adoptan medidas correctivas y preventivas en función de los resultados y de la revisión (o de otras informaciones relevantes) para lograr la mejora continua.

Para lograr la sistematización exitosa de las acciones para la seguridad de los datos personales es necesario considerar dos factores críticos de éxito. El primero consiste en diseñar y aplicar programas de capacitación sobre el tratamiento de datos personales a las personas indicadas según sus roles y responsabilidades. El segundo factor crítico de éxito implica la creación de un marco normativo sobre el cual se apoya la correcta ejecución de las acciones descritas. El marco normativo consiste en la creación de políticas internas para la gestión y tratamiento de los datos personales, una estructura de gobierno normativo y un proceso de gestión del ciclo de vida de las políticas de protección de datos personales.

Acta de verificación

Luis Manuel Pérez de Acha y
Denise Marie Tron Zuccher

Las visitas de verificación realizadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) concluyen con el levantamiento de un acta en la que se harán constar las circunstancias conocidas por los verificadores. La legislación referente a particulares y aquella relativa a sujetos obligados guarda gran similitud por lo que hace a los requisitos que deben observar las actas de verificación.

1. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

La visita de verificación concluye al momento en que se levanta el acta de verificación por parte del personal del INAI, así lo prevén los artículos 135 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares RLFPDPPP y 64 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de los Procedimientos). Tales ordenamientos señalan que en el acta de verificación debe quedar constancia de las actuaciones practicadas durante la visita de verificación.

Las actas de visita "constituyen un reflejo de los actos de ejecución de la orden de visita en la que se deben hacer constar los hechos u omisiones conocidos por los visitadores, éstos deberán circunstanciar en ellas todos aquellos actos que efectúen durante el desarrollo de la visita, así como aquellos que estando legalmente obligados a efectuar no los realicen

por existir algún impedimento para ello",[16] así lo resolvió la Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN).

Tanto para la autoridad como para el particular visitado, el acta de verificación constituye un elemento crucial. Los verificadores del INAI deberán asegurarse de que el acta cumpla con los requisitos de legalidad, a fin de que la misma pueda ser utilizada para motivar debidamente la resolución que en su momento se emita en el procedimiento de verificación.[17] Para el particular, lo asentado en el acta de visita es prueba de que se cumplió o no con las formalidades constitucionales y legales, las cuales deben ser observadas a cabalidad por los verificadores en tanto se trata de una excepción a la inviolabilidad del domicilio.[18]

Las actas que se levanten con motivo de una visita de verificación deberán asentar, en forma circunstanciada, los hechos u omisiones conocidos durante el desarrollo de la diligencia.[19] Esta obligación se desprende del artículo 16, párrafo decimoprimero de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

La Segunda Sala de la SCJN resolvió que "el requisito relativo al acta de visita circunstanciada consiste en detallar o pormenorizar las circunstancias de tiempo, modo y lugar de los hechos, omisiones e irregularidades detectadas". En esta jurisprudencia se sostiene que los visitadores deben precisar datos concretos y objetivos, así como la manera en que se cercioraron del cumplimiento o no de las obligaciones legales a cargo del particular.[20]

La obligación de los verificadores de levantar acta circunstanciada debe interpretarse a partir de los artículos 136 del RLFPDPPP y 65 de los Lineamientos de los Procedimientos, que establecen los datos e información a ser asentada en la misma:[21]

- Nombre del sujeto visitado.
- Momento en que inicia y concluye la visita (hora, día, mes y año).
- Lugar en que se practicó la verificación (datos que identifiquen plenamente el domicilio).
- Número telefónico u otra forma de comunicación con el sujeto verificado.
- Datos del oficio de comisión y de la orden de verificación (número y fecha).
- Persona con la que se entendió la verificación (nombre, cargo y datos de su documento de identificación).
- Datos de los testigos (nombre, domicilio y datos de su documento de identificación).

16 SCJN. (2014, julio). "Sentencia de la Contradicción de tesis 119/2014". *Gaceta del Semanario Judicial de la Federación*. Décima época. Libro 8. Tomo I, p. 271.

17 TFJA. (1987, marzo). "Tesis II-TASS-9763". *Revista del Tribunal Fiscal de la Federación*. Segunda época, año VIII, número 87, p. 738.

18 SCJN. (2015, noviembre). "Tesis I.1o.A.E.94 A (10a.)". *Gaceta del Semanario Judicial de la Federación.* Décima época. Libro 24. Tomo IV, p. 3567.

19 Con relación al motivo de visita, el artículo 16, párrafo decimoprimero de la Constitución Política de los Estados Unidos Mexicanos (CPEUM). Señala: "En toda orden de cateo, que solo la autoridad judicial podrá expedir, a solicitud del Ministerio Público, se expresará el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o en su ausencia o negativa, por la autoridad que practique la diligencia".

20 SCJN. (2013, septiembre). "Tesis 2a./J. 120/2013 (10a.)". *Semanario Judicial de la Federación y su Gaceta*. Décima época. Libro XXIV. Tomo 2, p. 1111.

21 TFJA. (2011, octubre). "Tesis VII-TASR-PE-6". *Revista del Tribunal Federal de Justicia Administrativa*. Séptima época. Año I, número 3, p. 249.

- Datos relativos a la actuación.
- Declaración del verificado, en su caso.
- Nombre y firma de quienes intervinieron en la visita.

Por lo que hace al requisito relativo a que el acta debe contener el nombre y firma de quienes hayan intervenido en la diligencia. En una tesis del Tribunal Federal de Justicia Administrativa (TFJA) se resolvió que es necesario que quede asentado el nombre y firma de cada uno de los verificadores que participó en la misma, de lo contrario, "la falta de firma por parte de todos los verificadores que actuaron en la diligencia, origina un contexto de inseguridad jurídica conforme al cual no resultó justificada la presencia y participación de todas las personas que se constituyeron a ejecutar la orden".[22]

También debe hacerse constar la firma de la persona con quien se atendió la visita. El artículo 135 del RLFPDPPP señala que, si el verificado se negara a firmar el acta, esto no afectará la validez de la misma y será necesario que esta situación quede asentada.

Los Lineamientos de los Procedimientos señalan que la "firma del verificado supondrá solo la recepción de la misma".[23] Este precepto tiene dos implicaciones, por una parte, es de reconocido derecho que la firma del acta por parte del verificado no supone que se encuentre conforme con las conclusiones a las que llegaron los verificadores durante el curso de la visita, sino que queda vigente el derecho de defensa del particular frente a las situaciones observadas en la verificación. Por otra parte, se ha pretendido sostener que la firma del acta supone que los verificadores le entregaron una copia de la misma al particular. Sobre este tema, el entonces Tribunal Fiscal de la Federación (TFF) resolvió que la autoridad debe acreditar el cumplimiento de este requisito señalándolo expresamente en la propia acta, sin que sea posible asumir que fue entregada una copia por el hecho de que el acta contenga la firma del sujeto visitado.[24]

Es un requisito constitucional que el acta de verificación sea levantada ante la presencia de dos testigos. La falta de cumplimiento de esta formalidad provoca la ilegalidad de la misma, ya que dichas personas son quienes corroboran los hechos u omisiones asentados por los verificadores.[25] Por esta razón, el artículo 135 del RLFPDPPP señala que en el supuesto de que la persona con quien se atienda la visita de verificación se niegue a nombrar a dos testigos, deberán ser designados por los verificadores.

Ahora bien, la obligación de levantar acta circunstanciada en presencia de dos testigos se actualiza cuando la visita efectivamente se lleva a cabo. Si el particular visitado se niega o se opone a la práctica de la verificación, el acta que se levante se limitará a hacer constar tales hechos, sin que resulte necesario el nombramiento de testigos para corroborarlo.[26]

22 TFJA. (2018, febrero). "Tesis VII-CASR-9ME-5". *Revista del Tribunal Federal de Justicia Administrativa*. Octava época. Año III, número 19, p. 256.

23 Artículo 64, Lineamientos.

24 TFJA. (1984, septiembre). "Tesis II-TASS-6608". *Revista del Tribunal Fiscal de la Federación*. Segunda época, año VI, número 57, p. 153.

25 TFJA. (2016, julio). "Tesis VII-CASR-2NCII-17". *Revista del Tribunal Federal de Justicia Administrativa*. Séptima época, año VI, número 60, p. 335.

26 TFJA. (2014, marzo). "Tesis VII-J-SS-69". *Revista del Tribunal Federal de Justicia Administrativa*. Séptima época, año III, número 23, p. 22. y TFJA. (2014, marzo). "Tesis I.10o.A.5 A (10a.)". *Gaceta del Semanario Judicial de la Federación*. Décima época. Libro 4. Tomo II, p. 1906.

El RLFPDPPP prevé la posibilidad de que el particular formule observaciones respecto a los hechos asentados en el acta, las cuales podrán efectuarse en el momento en que se levante y deberán constar en el texto de la misma, en términos del artículo 136, fracción VIII. Dichas observaciones también podrán ser formuladas mediante escrito presentado ante el INAI, dentro de los cinco días siguientes a la fecha en que se levantó el acta de verificación.

Dentro del procedimiento de verificación, el INAI podrá practicar más de una visita de verificación.[27] Si bien la legislación no lo señala expresamente, será necesario que se levante un acta por cada una de las visitas que se realicen.

2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)

Las visitas de verificación que lleve a cabo el INAI a los sujetos obligados concluirán con el levantamiento del acta de verificación. De acuerdo con los artículos 205 y 206 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), en el acta quedará constancia de las actuaciones practicadas durante la visita.

Los datos e información que deben quedar asentados en el acta son los mismos que se prevén para las visitas practicadas a particulares. Igualmente debe cumplirse con el requisito de levantarse ante la presencia de dos testigos, permitiéndose que estos sean nombrados por el personal del INAI en el supuesto de que las autoridades visitadas se nieguen a hacerlo.

Los sujetos obligados podrán realizar observaciones, ya sea en el momento en que se levanta el acta o bien dentro de los cinco días siguientes mediante escrito que deberá presentarse ante el INAI. Es necesario que el acta contenga la firma de la persona que atiende la visita, sin embargo, si la persona se niega a hacerlo, esto no afectará la validez de lo actuado, debiendo quedar asentada tal situación en la propia acta. Al igual que sucede respecto de los particulares, lo verificadores deberán levantar un acta por cada visita que practiquen dentro del procedimiento de verificación.

Finalmente, las actas levantadas por los verificadores en las visitas practicadas, tanto a particulares como a sujetos obligados, serán utilizadas por el INAI para emitir la resolución con la que concluye el procedimiento de verificación, en términos de los artículos 137 del RLFPDPPP y 149 de la LGPDPPSO, respectivamente.

Activo

Uciel Fragoso Rodríguez

En términos generales, un activo es cualquier elemento que representa un valor para la organización.

Acorde con la Real Academia Española (RAE)[28] "valor" se define como:

a) grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite y

b) cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente

De las definiciones anteriores, se establece que cuando un activo es dañado o atacado se genera una pérdida directa o indirecta a la organización que se materializa en un impacto económico, operativo, funcional, legal, de reputación o inclusive un daño de carácter humano.

27 Artículo 62, fracción II, Lineamientos de los Procedimientos.

28 Real Academia Española. (2019). *Diccionario de la Lengua Española*.

Los activos pueden ser tangibles o intangibles. Los activos tangibles son objetos físicos que proporcionan una utilidad en las actividades del día a día en las organizaciones, como la infraestructura tecnológica, el equipo de cómputo, de comunicaciones o cualquier dispositivo electrónico. En otro sentido, los activos intangibles incluyen datos, información digital, aplicaciones, transacciones, planes, propiedad intelectual, conocimiento, imagen, reputación, principios, valores, entre otros.

Un tercer tipo de activo está formado por la combinación de activos tangibles e intangibles como los servicios o procesos. Imaginemos un servicio financiero de pago por Internet, para llevarlo a cabo se requieren activos tangibles como servidores, computadoras o enlaces de comunicación y también intangibles como el *software*, número de la tarjeta de crédito, nombre del usuario, contraseña o cualquier otro tipo de información.

Los activos en forma aislada no tienen ni proporcionan valor, deben estar contextualizados en escenarios reales y funcionales de la organización y deben estar caracterizados. Caracterizar un activo implica identificar las relaciones que guarda con otras entidades en su entorno. Si se caracteriza un activo del tipo información digital, es necesario determinar los siguientes aspectos: a) dueño, b) *hardware* y *software* que procesan la información digital, c) conectividad interna y externa para accederla, d) clasificación de la información, e) propósito, f) personas que gestionan la información, g) usuarios, h) sensitividad, i) mecanismos de seguridad asociados, j) flujo de la información en los procesos y otros aspectos.

La caracterización del activo es importante para identificar las amenazas y su vulnerabilidad y poder construir escenarios de riesgo que describan situaciones en la que el activo puede ser afectado en caso de que el escenario de riesgo se materialice.

Adicional a la caracterización, los activos deben clasificarse o categorizarse de acuerdo con su criticidad dentro de la organización, es decir, es fundamental determinar para cada activo su importancia en el impacto global a la organización cuando se presenta un incidente sobre el activo. Una correcta categorización de activos permite a la organización enfocar recursos y esfuerzos para proteger aquellos activos considerados críticos.

The Security Risk Management Guide (SRMG)[29] define tres clases de activos para determinar su valor dentro de la organización: *high business impact* (HBI), *moderate business impact* (MBI) y *low business impact* (LBI).

La afectación a la confidencialidad, integridad o disponibilidad sobre un activo clasificado como HBI causa pérdidas severas o catastróficas a la organización. El impacto puede ser expresado en términos financieros, en la productividad, daño a la reputación, incumplimiento legal y regulatorio. Ejemplos de activos de clase HBI son: credenciales de autenticación (contraseñas, llaves criptográficas, *tokens*), información financiera, perfiles médicos, información personal, propiedad intelectual, entre otros.

La afectación a la confidencialidad, integridad o disponibilidad sobre un activo clasificado como MBI causa una pérdida moderada a la organización. El impacto puede interrumpir las funciones normales de la organización por lo que controles de seguridad proactivos son necesarios para minimizar el impacto para esta clase de activos. Generalmente son accedidos por grupos específicos de personas con necesidades legítimas de la organización. Ejemplos de activos de clase MBI son: directorio de los usuarios, órdenes de compra, diseño de la infraestructura tecnológica, información para operación del día a día interna, entre otros.

29 Dillard, K. et al. (2004). *The Security Risk Management Guide*. Microsoft.

La afectación a la confidencialidad, integridad o disponibilidad sobre un activo clasificado como LBI no causa ninguna pérdida a la organización, por lo que no se requiere ningún tipo de control de seguridad adicional. Este tipo de activo tiene la finalidad de ser accedido públicamente. Algunos ejemplos de activos de esta clase son: organigrama de alto nivel, información general de la infraestructura tecnológica, sitios web públicos, documentos publicitarios, entre otros.

El ISO/IEC 27005[30] establece que los activos críticos de la organización deben ser identificados con detalle para proveer suficiente información en el proceso de análisis de riesgo. Un propietario debe ser identificado para cada activo y es el responsable de su producción, desarrollo, mantenimiento, uso y seguridad. El estándar identifica dos tipos de activos: primarios y de soporte.

Los activos primarios de una organización corresponden a sus procesos de negocio y actividades, así como a su información crítica. Ejemplos de procesos de negocio y actividades consideradas activos críticos o primarios son aquellos cuya pérdida o degradación hacen imposible cumplir con la misión de la organización o impiden el cumplimiento con requerimientos contractuales, legales o regulatorios. La información considerada como activo primario es por ejemplo toda la información vital para la operación de la organización, la información personal especificada dentro del marco regulatorio de privacidad e información estratégica que representa una ventaja competitiva para la organización.

Los activos de soporte son aquellos que apoyan a los activos primarios para su operación y consisten en: equipo de cómputo (*hardware*), aplicaciones (*software*), equipos de comunicaciones, personal, instalaciones y estructura organizacional.

Una vez que han sido identificados los activos primarios y los de soporte, el estándar ISO/IEC 27005 establece que se deberá asignar un valor a cada activo. El valor asignado puede ser cuantitativo, por ejemplo, expresado en términos monetarios o cualitativo expresado generalmente como valor bajo, valor medio o valor alto. El proceso de valoración de un activo considera un criterio, una escala y dependencias.

El criterio de valoración puede considerar el costo original, de reparación o de reemplazo del activo. Otros criterios consideran el impacto cuando se presenta pérdida de confidencialidad, integridad o disponibilidad como resultado de un incidente sobre el activo. Algunos ejemplos de criterios de valoración por impacto son violación de regulación y legislación, pérdida de reputación, interrupción de actividad del negocio, exposición de datos personales, daño al medio ambiente y a la seguridad física de las personas, incumplimiento contractual, entre otros.

La escala de valoración debe ser establecida por la organización y perfectamente entendida por las personas que tienen relación directa con el activo. Una escala entre los tres y diez niveles es adecuada para la mayoría de los procesos de valoración de activos.

Otro aspecto a considerar es la dependencia que tienen los procesos de negocio u otros activos con el activo bajo valoración, es decir, entre más relevantes y numerosos sean los procesos de negocio que dependen del activo, su valor será mayor.

En COBIT-5-EI[31] uno de los activos más importantes dentro de una organización es la información. Para que la información tenga un valor como activo crítico debe alcanzar

30 Online Browsing Platform (OBP). (2011). *ISO/IEC 27005. Information technology –Security techniques– Information security risk management*. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en

31 ISACA. (2013). *Cobit 5 Enabling Information*. Recuperado de: http://www.unhas.ac.id/~rhiza/arsip/Sosialisasi_SNI/COBIT-5-Enabling-Information_Res_Eng_1113.pdf

ciertos objetivos definidos bajo un criterio de calidad de la información (CCI). El CCI se divide en tres subdimensiones:

a) Intrínseco: hasta qué sentido los valores de los datos están en conformidad con los valores reales.
b) Contextual: hasta qué sentido la información es aplicable a las actividades de las personas y es presentada de manera clara, inteligible en un contexto de uso.
c) Accesible: hasta qué sentido la información está disponible de manera segura.

La dimensión intrínseca pretende lograr los objetivos de exactitud (la información debe ser correcta y confiable), objetividad (la información debe ser imparcial y sin prejuicios), credibilidad (la información debe ser verdadera y creíble) y reputación (la información debe ser reconocida en función de su fuente y contenido).

La dimensión contextual persigue cumplir con los objetivos de relevancia (la información debe ser útil y aplicable a las tareas realizadas), completitud (la información debe ser completa y suficiente), actual (la información debe estar actualizada), cantidad apropiada (el volumen de la información debe ser adecuado), representación concisa (la información debe estar representada en forma concreta), interpretabilidad (la información debe estar en un lenguaje apropiado y con definiciones claras), comprensibilidad (la información debe ser fácilmente entendible), fácil manipulación (la información debe ser fácilmente aplicable).

La dimensión de accesibilidad tiene como finalidad dos objetivos: disponibilidad (la información debe estar lista en el momento y forma requerida) y acceso restringido (la información debe estar disponible solo para las personas autorizadas).

Para el activo "información correspondiente a datos personales", la Metodología de Análisis de Riesgo BAA (MARBAA)[32] propone una clasificación de datos en cuatro categorías, de acuerdo con la criticidad de los mismos por el nivel de riesgo inherente: 1) datos de riesgo inherente bajo; 2) datos de riesgo inherente medio; 3) datos de riesgo inherente alto y 4) datos de riesgo inherente reforzado.

Los datos de riesgo inherente bajo es información general de una persona identificada o identificable que corresponden a datos de identificación, de contacto, académicos o laborales como nombre, teléfono, nacionalidad, dirección de correo electrónico, escolaridad, profesión, entre otros. Este tipo de datos no se consideran sensibles por lo que las medidas de seguridad para proteger el activo son básicas.

Los datos de riesgo inherente medio corresponden a información de localización, patrimonial, de autenticación y jurídica como la dirección física, cuentas bancarias, información crediticia, datos biométricos, firma autógrafa, antecedentes penales, contratos, entre otros. Esta categoría se considera información relevante por lo que dicho activo se clasifica como de impacto alto en caso de ser vulnerado.

Los datos de riesgo inherente alto contemplan datos personales sensibles como lo es la información médica, genética, origen racial, creencias religiosas, preferencia sexual, entre otras. Este tipo de datos debe ser altamente protegido ya que un uso indebido puede ocasionar actos de discriminación o representar un riesgo grave para el titular.

Los datos de riesgo reforzado están asociados a personas de alto riesgo, es decir, aquellas que por su profesión, condición económica o situación política representan un alto interés para los atacantes.

32 INAI. (2015, junio). *Metodología de Análisis de Riesgo BAA*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

Actualizaciones de las medidas de seguridad

Christian Paredes González

La normatividad establece que los responsables deberán llevar a cabo la implementación de controles de seguridad que permitan la protección de datos personales permitiendo el cumplimiento previsto por la norma[33] y a su vez están sujetos a una constante revisión y actualización práctica que puede implicar la adopción de controles más estrictos o robustos en caso de que se actualice un incidente de seguridad o un evento que pudiere representar un riesgo para la seguridad de los datos personales. Los controles de seguridad para la protección de los datos personales en términos de la normatividad nacional se conocen como "medidas de seguridad" y dada la importancia de la protección de los datos personales se establecen tres tipos: físicas, técnicas y/o administrativas. Esta situación representa, naturalmente, una ventaja para el titular de los datos personales. Dichos controles en su conjunción requerirán ser puestos al día cuando el responsable y/o encargado que llevan a cabo el tratamiento de datos personales se percaten que se han actualizado algunos de los eventos previstos en el artículo 62 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).

En este contexto, el artículo 62 del RLFPDPPP obliga a los responsables y encargados del tratamiento a poner a proceder a la actualización de las medidas de seguridad físicas, técnicas y administrativas cuando se presenten los siguientes eventos:

- Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable.
- Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo.
- Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)34 y 63 del RLFPDPPP.35
- Exista una afectación a los datos personales distinta a las anteriores.

33 Deber de seguridad, las recomendaciones en materia de seguridad al artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares precisan lo siguiente:
"Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado".
El artículo 31 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala:
"Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad".

34 Artículo 20. Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

35 El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares considera vulneraciones de seguridad a los siguientes incidentes:
"Vulneraciones de seguridad
Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:
I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada".
Por su parte, el artículo 38 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala:
"Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:

Además de tomar en cuenta los factores anteriores, la adopción de las medidas de seguridad habrá de considerar, por regla general, el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.[36]

En cuanto a la temporalidad de la revisión de las medidas de seguridad, el RLFPDPPP dispone que dicha operación deberá llevarse a cabo una vez al año cuando se trate de datos personales de carácter sensible.

Las recomendaciones en materia de seguridad de datos personales para el sector privado (Recomendaciones de Seguridad) publicadas en 2013 señalan a su vez que, para cumplir con el deber de seguridad, las organizaciones deberán de implementar un sistema de gestión de seguridad de datos personales (SGSDP) basado en el modelo denominado Planificar-Hacer-Verificar-Actuar (PHVA).

Como parte de la puesta en práctica del SGSDP, las organizaciones se encuentran obligadas a actualizar las medidas de seguridad adoptadas y para ello, las Recomendaciones establecen (dentro del paso 8 del SGSDP) que se lleven a cabo revisiones y auditorías para monitorear y revisar el SGSDP:

- Paso 8. Revisiones y auditoría.
- Fase 3. Monitorear y revisar el SGSDP.

Revisiones y auditoría. Proceso de revisión del funcionamiento del SGSDP respecto a la política establecida, cada vez que exista un cambio en el contexto del alcance y objetivos del SGSDP.

- Revisión de los factores de riesgo. Consideraciones para monitorear el estado del riesgo y aplicar las modificaciones pertinentes para mejorar el SGSDP.
- Auditoría. Requerimientos para los procesos de auditoría interna/externa.
- Vulneraciones a la seguridad de la información. Consideraciones en caso de un incidente de seguridad.

De esta manera, se puede señalar que la obligación de actualizar las medidas de seguridad prevista en el artículo 62 del RLFPDPPP se corresponde con la metodología sugerida por las Recomendaciones de Seguridad para dar cumplimiento práctico al deber de seguridad.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) indica en su artículo 32 que las medidas de seguridad adoptadas deberán considerar factores como el riesgo inherente a los datos personales tratados, la sensibilidad de los datos personales tratados, el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realicen, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada".

36 Lo anterior, según dispone el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares: "Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico".

En cuanto a la actualización de las medidas de seguridad en el orden público, el artículo 36 de la LGPDPPSO establece que el documento de seguridad– que es el instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee, debe ser actualizado en los siguientes supuestos:

- Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo.
- Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión.
- Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida.
- Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

De lo anterior se desprende la obligación de realizar un monitoreo y supervisión periódica de las medidas de seguridad implementadas. En este contexto, el párrafo primero del lineamiento 63 de los Lineamientos Generales de Protección de Datos para el Sector Público señala: "el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales a fin de verificar el cumplimiento de los objetivos propuestos, y en su caso, implementar mejores de manera continua".

Acuerdo de determinación

Isabel Davara Fernández de Marcos,[37]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La expresión "acuerdo de determinación" hace referencia a un acto jurídico de carácter procesal en virtud del cual, de manera fundada y motivada, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), por conducto de sus unidades administrativas competentes, emiten, dentro del procedimiento de investigación, una resolución cuya naturaleza es, precisamente, poner fin a la investigación sustanciada, en virtud de que la autoridad considera que en determinado caso no existen elementos de convicción que permitan acreditar la comisión de actos contrarios a lo establecido por la normatividad aplicable a la protección de datos personales.

1. Acuerdo de determinación en el sector privado

El concepto "acuerdo de determinación" surge en la normatividad de datos personales del sector privado con motivo de la emisión, publicación y entrada en vigor de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de Procedimientos) publicados en el *Diario Oficial de la Federación* el 9 de diciembre de 2015. El concepto objeto de estudio está vinculado al denominado procedimiento de investigación (PI), el cual tiene su origen en los Lineamientos de Procedimientos, y no así en la LFPDPPP o su Reglamento.

37 Agradecemos a Alejandra Rojas Apaez, José Ernesto Rodríguez Duque y a Juan Carlos Salamanca Vázquez, por su apoyo en la elaboración de las entradas que los autores Isabel Davara Fernández de Marcos, Gregorio Barco Vega y Alexis Cervantes Padilla realizaron para este *Diccionario de Protección de Datos Personales.*

De forma paulatina, esta figura también ha sido recogida y regulada en la normatividad de datos personales del sector público, como abordaremos en la segunda parte de esta definición.

Así, el acuerdo de determinación es un acto jurídico consistente en una resolución emitida por la Dirección General de Investigación y Verificación para el Sector Privado (DGIVSP) dentro del PI a través de la cual se pone fin a dicho procedimiento al considerarse que no existen elementos de convicción que permitan presumir un incumplimiento, por parte del sujeto investigado, a la LFPDPPP y a su normatividad de desarrollo.

El acuerdo de determinación, al ser un acto de autoridad, debe constar por escrito y cumplir con los requisitos de fundamentación y motivación previstos en el artículo 16 constitucional.[38] En este sentido, el artículo 59 de los Lineamientos de los Procedimientos previene que el acuerdo de determinación deba expedirse siempre de forma fundada y motivada:

> Artículo 59. Una vez que, dentro del Procedimiento de Investigación, se cuente con elementos suficientes para iniciar el procedimiento de verificación o en su caso, concluir el procedimiento de investigación, la Dirección General de Investigación y Verificación podrá emitir lo siguiente:
>
> I. Acuerdo de determinación. Se expedirá, de manera fundada y motivada, cuando el Instituto no cuente con elementos suficientes para acreditar la comisión de actos contrarios a lo establecido por la Ley y su Reglamento, o
>
> II. Acuerdo de Inicio de Procedimiento de Verificación. Se dictará, cuando, de manera fundada y motivada, se presuma que el Responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la Ley y su Reglamento.

En este contexto, el acuerdo de determinación deberá expresar con precisión los preceptos legales aplicables y las circunstancias especiales, razones particulares o causas inmediatas que se hayan tenido en consideración para emitirlo. Además, es necesario que el acuerdo de determinación se apegue a los principios de congruencia y exhaustividad que rigen las sentencias. Lo anterior significa que la resolución plasmada en el acuerdo de determinación deberá ser congruente con la litis planteada, apreciando las pruebas conducentes y resolviendo sin omitir nada, ni añadir cuestiones no hechas valer.

2. Acuerdo de determinación en el sector público

A partir de la emisión de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) en enero de 2017, se habilita al INAI por medio de sus unidades administrativas competentes para realizar investigaciones que tengan por objeto dilucidar hechos que pudieren constituir un incumplimiento a la normatividad aplicable a la protección de datos personales.[39]

En relación con lo anterior, se entiende que podrán desarrollarse las acciones de investigaciones en un PI como acto preliminar al inicio de un procedimiento de verificación (PV). En consecuencia, de forma similar a lo que sucede en el sector privado, cuando el INAI, una vez agotadas las diligencias de investigación para determinar un presunto in-

38 Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

39 Artículo 189. De acuerdo con el artículo 147, último párrafo de la Ley General, previo a dar inicio al procedimiento de verificación, el Instituto, a través de la unidad administrativa competente conforme a su estatuto orgánico vigente, podrá desarrollar investigaciones previas con el fin de contar con elementos suficientes a efecto de dilucidar sobre los hechos que presuntamente podrían constituir un incumplimiento a la Ley General y los presentes Lineamientos generales […]. (Lineamientos Generales de Protección de Datos Personales para el Sector Público (LGPDPSP).

cumplimiento de la LGPDPPSO, concluya que no existen elementos para atribuir la comisión de conductas contrarias a la LGPDPPSO, podrá emitir el acuerdo de determinación respectivo con las formalidades de fundamentación y motivación aplicables.

De esta manera, es en el artículo 198 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) donde se señala que, cuando la unidad administrativa competente no cuente con elementos suficientes para acreditar actos u omisiones que presuntamente constituyan un incumplimiento a lo establecido por la LGPDPSO y los Lineamientos, deberá emitir el acuerdo de determinación de manera fundada y motivada.

> Artículo 198. Una vez concluida la investigación previa, el Instituto, a través de la unidad administrativa competente conforme a su Estatuto Orgánico vigente, deberá emitir un acuerdo de:
>
> Determinación: cuando, de manera fundada y motivada, no cuente con elementos suficientes para acreditar actos u omisiones que presuntamente constituyan un incumplimiento a lo establecido por la Ley General y los presentes Lineamientos generales, o […]

En definitiva, de acuerdo con lo previsto por los Lineamientos Generales, puede entenderse que el acuerdo de determinación es también un acto jurídico procesal administrativo que se da dentro de una investigación previa iniciada por el INAI y que tiene como efecto concluir con las mismas al no existir elementos de convicción jurídica suficientes que permitan acreditar el incumplimiento de las disposiciones de la LGPDPPSO y demás normatividad aplicable.

Acuerdo de Inicio de Procedimiento de Imposición de Sanciones

Gabriel López López

Es el acto administrativo inicial del Procedimiento de Imposición de Sanciones (Pisan) por virtud del cual el INAI, a través de la Dirección General de Protección de Derechos y Sanción, ante la presunción de la comisión de una infracción prevista en la LFPDPPP por parte de alguna persona física o moral de carácter privado que trate datos personales, de la que hubiese tenido conocimiento con motivo de lo resuelto en los procedimientos de protección de derechos o de verificación, instaura de manera fundada y motivada un procedimiento administrativo tendiente a imponer la sanción que corresponda con motivo del presunto incumplimiento de la LFPDPPP y su Reglamento.

Cabe señalar que si bien la fracción XVIII, del artículo 3, de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación y de Imposición de Sanciones (LPPDIVIS), no define de forma específica el acuerdo de inicio del Pisan, sí define a este procedimiento administrativo de la siguiente forma:

> Conjunto de actos por los cuales el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través de la Dirección General de Protección de Derechos y Sanción, en caso de presunción de incumplimiento de alguno de los principios o disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que el Pleno previamente determine en los procedimientos de protección de derechos o verificación, impone la o las sanciones que correspondan.

1. Objeto del acto

Conforme a lo previsto por los artículos 61 de la LFPDPPP y 68 de los LPPDIVIS, cuando como consecuencia de la resolución que se emita en los procedimientos de protección de derechos o de verificación, el INAI tenga conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones a la Ley, iniciará el Pisan, a efecto de determinar la sanción que corresponda.

El artículo 140 del RLFPDPPP previene que el procedimiento iniciará con la notificación de un acuerdo de inicio que se haga al presunto infractor, en el domicilio que el INAI tenga registrado, derivado de los procedimientos de protección de derechos o de verificación previamente sustanciados.

El acuerdo de inicio del Pisan, como acto de autoridad de aquellos a que se refiere el primer párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en relación con el diverso artículo 3 de la Ley Federal de Procedimiento Administrativo (LFPA) y en aras del cumplimiento del principio de legalidad que consagran dichas normas, debe constar en mandamiento escrito y ser emitido por autoridad competente, quien a su vez tiene la ineludible obligación de invocar los fundamentos legales que legitimen su actuar, así como las razones, motivos, circunstancias o causas particulares que se tomaron en consideración para la emisión del acto.

Para el cumplimiento de dicho propósito, el acuerdo debe emitirse, entre otros, con fundamento en los artículos 61 de la LFPDPPP, 140 del RLFPDPPP y 68 de los LPPDIVIS, y tiene como otro de sus propósitos, respetar la garantía de audiencia del presunto infractor, para que manifieste lo que a su derecho convenga, aporte pruebas y formule sus alegatos, en relación con las conductas infractoras que se le imputen.

2. Requisitos

Independientemente de tratarse de un acto de autoridad que deba cumplir con el principio de legalidad exigido por el artículo 16 de la CPEUM, así como con los requisitos y elementos previstos por el artículo 3 de la LFPA,[40] en el acuerdo de inicio del Pisan, según lo previenen los artículos 62 de la LFPDPPP y 70 de los LPPDIVIS, se emplazará al presunto infractor a fin de que comparezca y haga valer lo que a su derecho convenga, debiendo contener además: a) un informe que describa los hechos constitutivos de la(s) presunta(s) infracción(es), b) el otorgamiento de un término de 15 días hábiles para que rinda pruebas y manifieste lo que a su derecho convenga, mismo término que se contará a partir de que surta efectos la notificación del acuerdo. Se considera que la notificación surte efectos el día en que la misma se rea-

40 Artículo 3.- Son elementos y requisitos del acto administrativo:
I. Ser expedido por órgano competente, a través de servidor público, y en caso de que dicho órgano fuere colegiado, reúna las formalidades de la ley o decreto para emitirlo;
II. Tener objeto que pueda ser materia del mismo; determinado o determinable; preciso en cuanto a las circunstancias de tiempo y lugar, y previsto por la ley;
III. Cumplir con la finalidad de interés público regulado por las normas en que se concreta, sin que puedan perseguirse otros fines distintos;
IV. Hacer constar por escrito y con la firma autógrafa de la autoridad que lo expida, salvo en aquellos casos en que la ley autorice otra forma de expedición;
V. Estar fundado y motivado;
VI. (Se deroga)
VII. Ser expedido sujetándose a las disposiciones relativas al procedimiento administrativo previstas en esta Ley;
VIII. Ser expedido sin que medie error sobre el objeto, causa o motivo, o sobre el fin del acto;
IX. Ser expedido sin que medie dolo o violencia en su emisión;
X. Mencionar el órgano del cual emana;
XI. (Se deroga)
XII. Ser expedido sin que medie error respecto a la referencia específica de identificación del expediente, documentos o nombre completo de las personas;
XIII. Ser expedido señalando lugar y fecha de emisión;
XIV. Tratándose de actos administrativos deban notificarse deberá hacerse mención de la oficina en que se encuentra y puede ser consultado el expediente respectivo;
XV. Tratándose de actos administrativos recurribles deberá hacerse mención de los recursos que procedan,
y
XVI. Ser expedido decidiendo expresamente todos los puntos propuestos por las partes o establecidos por la ley.

lice, c) el requerimiento al presunto infractor para que presente documentación idónea que acredite su situación financiera actual y d) la puesta en conocimiento del presunto infractor de que las notificaciones subsecuentes podrán realizarse a través de medios electrónicos.

Sobre este último punto, resulta importante destacar que por lo que se refiere al emplazamiento al presunto infractor del acuerdo de inicio del Pisan, el último párrafo del artículo 70 de los LPPDIVIS establece que éste debe notificarse de manera personal, mientras que las subsecuentes notificaciones podrán efectuarse por correo electrónico.

Acuerdo de Inicio del Procedimiento de Verificación[41]

Isabel Davara Fernández de Marcos,
Gregorio Barco Vega y
Alexis Cervantes Padilla

Corresponde al primer acto procesal que lleva a cabo el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y/o los organismos garantes de las entidades federativas, según corresponda, dentro del procedimiento de verificación y cuyo principal objetivo es notificar al presunto infractor sobre la investigación a la que será sujeto para verificar su cumplimiento a la normatividad de protección de datos personales.

La emisión del Acuerdo de Inicio del Procedimiento de Verificación suele ser consecuencia del desahogo de un procedimiento de investigación por la posible existencia de un tratamiento ilícito.

En el ámbito nacional, la concreción de los aspectos relativos al Acuerdo de Inicio de Procedimiento de Verificación se da en dos ámbitos normativos específicos: de un lado, el régimen jurídico aplicable al sector privado, y, del otro, el régimen jurídico aplicable al sector público.

1. Acuerdo de Inicio del Procedimiento de Verificación en el sector privado

De acuerdo con lo previsto por el artículo 59 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),[42] el INAI tiene la facultad de verificar el cumplimiento de la LFPDPPP, su Reglamento y demás normatividad que resulte aplicable mediante la instauración del procedimiento de verificación, cuyo inicio se materializa con la emisión del Acuerdo de Inicio del Procedimiento de Verificación.

Al respecto, el artículo 129 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) indica en su segundo párrafo que el Pleno del INAI será quien determine, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente.

> Causales de procedencia:
>
> Artículo 129. El procedimiento de verificación se iniciará de oficio o a petición de parte, por

41 Agradecemos el inestimable apoyo de Juan Carlos Salamanca, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

42 Artículo 59. El Instituto verificará el cumplimiento de la presente Ley y de la normatividad que de ésta derive. La verificación podrá iniciarse de oficio o a petición de parte.
La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos a que se refiere el Capítulo anterior o se presuma fundada y motivadamente la existencia de violaciones a la presente Ley.

instrucción del Pleno del Instituto.

Cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas en la Ley y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos. **En este caso, el Pleno determinará, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente.** (Énfasis añadido).

En función de lo anterior, se puede afirmar que el Acuerdo de Inicio del Procedimiento de Verificación debe ser un acto fundado y motivado[43] por parte del Pleno del INAI a través del cual se ordena sujetar al presunto infractor a un procedimiento de verificación. Como veremos más adelante, el Acuerdo de Inicio del Procedimiento de Verificación también puede ser emitido, de manera conjunta, por el Secretario de Protección de Datos Personales y por el Director General de Investigación y Verificación en términos del acuerdo por el que se delegan al secretario de Protección de Datos Personales diversas facultades para dictar, conjuntamente con los directores generales que se indican, diversos acuerdos en los procedimientos de verificación, protección de derechos e imposición de sanciones.[44]

El Acuerdo de Inicio de Procedimiento de Verificación se emite, como decíamos, cuando la autoridad considera necesario, mediante la emisión de requerimientos de información y/o la práctica de visitas de verificación,[45] obtener información, datos y evidencia o medios de convicción suficientes para que le permitan determinar si un determinado tratamiento de datos personales resulta contrario a lo regulado en la normatividad aplicable.

La mayoría de los acuerdos de inicio de procedimientos de verificación emitidos por la autoridad son consecuencia de la investigación realizada al presunto infractor dentro del procedimiento de investigación regulado en los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de los Procedimientos).

Los Lineamientos de los Procedimientos disponen, en su artículo 59, que una vez que dentro del procedimiento de investigación se cuente con elementos suficientes para iniciar el procedimiento de verificación o en su caso, concluir el procedimiento de investigación, la Dirección General de Investigación y Verificación podrá emitir lo siguiente:

1. Acuerdo de determinación. Se expedirá, de manera fundada y motivada, cuando el Instituto no cuente con elementos suficientes para acreditar la comisión de actos contrarios a lo establecido por la LFPDPPP y su Reglamento.
2. Acuerdo de Inicio de Procedimiento de Verificación. Se dictará cuando, de manera fundada y motivada, se presuma que el responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la LFPDPPP y su Reglamento.

Del artículo de referencia puede advertirse con meridiana claridad que la emisión por

43 En relación con la fundamentación y motivación en general resulta ilustrativo el criterio de rubro. Véase: SCJN. (2003, abril). "Actos de molestia. Requisitos mínimos que deben revestir para que sean constitucionales". *Semanario Judicial de la Federación y su Gaceta.* Novena época. Tomo XVII, p. 1050. Recuperado de: https://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/184/184546.pdf

44 *Diario Oficial de la Federación*. 29 de abril de 2013.

45 En este sentido, el RLFPDPPP señala:
"Inicio
Artículo 128. El Instituto, con el objeto de comprobar el cumplimiento de las disposiciones previstas en la Ley o en la regulación que de ella derive, podrá iniciar el procedimiento de verificación, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas".

parte de la autoridad de un acuerdo de inicio del procedimiento de verificación puede ser consecuencia del desahogo por parte de la autoridad del procedimiento de investigación.

En adición a lo anterior y como adelantábamos, los Lineamientos de los Procedimientos detallan en el segundo párrafo de su artículo 60, que el Acuerdo de Inicio de Procedimiento de Verificación se emitirá de la siguiente forma:

> [...]
>
> Se emitirá el Acuerdo de Inicio de Procedimiento de Verificación, ya sea por instrucción del Pleno del Instituto, de conformidad con el artículo 129 del Reglamento, o por el secretario de Protección de Datos Personales y el Director General de Verificación(2), conjuntamente, de conformidad con el artículo 14 del Reglamento Interior del Instituto, en relación con el punto Primero del Acuerdo por el que se delegan al Secretario de Protección de Datos Personales diversas facultades para dictar, conjuntamente con los Directores Generales que se indican, diversos acuerdos en los Procedimientos de Verificación, Protección de Derechos e Imposición de Sanciones, publicado en el *Diario Oficial de la Federación* el cuatro de marzo de dos mil quince.
>
> [...]

De lo anterior, se puede advertir que las autoridades competentes para emitir el Acuerdo de Inicio de Procedimiento de Verificación son el Pleno del INAI, y/o el secretario de Datos Protección de Datos Personales de manera conjunta con el director general de Investigación y Verificación del Sector Privado.

En este mismo sentido, el estatuto orgánico del INAI[46] reserva a la DGIV las atribuciones relacionadas con la sustanciación del PV, incluyendo la emisión del Acuerdo de Inicio del Procedimiento de Verificación. Al respecto, la fracción II del artículo 41 del estatuto orgánico del INAI refiere que es función de la DGIV acordar conjuntamente con el secretario de Protección de Datos Personales, el inicio del PV de oficio o a petición de parte, así como la ampliación del periodo de resolución definitiva del procedimiento de verificación hasta por un plazo de 180 días a que se refiere el artículo 132 del RLFPDPPP, sin perjuicio de su ejercicio directo por el Pleno del INAI.[47]

Respecto al Acuerdo de Inicio de Procedimiento de Verificación, también conviene desta-

46 *Diario Oficial de la Federación*. 17 de enero de 2017.

47 Artículo 41. La Dirección General de Investigación y Verificación tendrá las siguientes funciones:
I. Realizar procedimientos de investigación, incluyendo los relativos sobre vulneraciones a la seguridad, dictaminar y emitir opiniones en materia de vigilancia y verificación relacionadas con el cumplimiento de las disposiciones de la Ley de Protección de Datos Personales, la Ley Federal, sus reglamentos y las demás disposiciones aplicables;
II. Acordar conjuntamente con el secretario de Protección de Datos Personales, el inicio del procedimiento de verificación de oficio o a petición de parte, así como la ampliación del periodo de resolución definitiva del procedimiento de verificación hasta por un plazo de ciento ochenta días a que se refiere el artículo 132 del Reglamento de la Ley de Protección de Datos Personales, sin perjuicio de su ejercicio directo por el Pleno del Instituto;
III. Sustanciar el procedimiento de verificación conforme a lo establecido en la Ley de Protección de Datos Personales, su Reglamento y las demás disposiciones legales aplicables;
IV. Elaborar informes y reportes sobre presuntas infracciones e incumplimientos, en materia de datos personales, tanto en el sector público como en el privado, de conformidad con las disposiciones legales aplicables;
V. Coordinarse con las autoridades federales, estatales y municipales, bajo la supervisión de la Secretaría de Protección de Datos Personales, y por medio del secretario ejecutivo del Sistema Nacional de Transparencia, en su caso, para obtener el apoyo necesario en el ejercicio de sus facultades;
VI. Requerir a particulares y autoridades, la información o documentación necesaria para investigar el probable incumplimiento a la Ley de Protección de Datos Personales, a la Ley Federal, su Reglamento y demás disposiciones aplicables en materia de protección de datos personales;
VII. Suscribir todo tipo de actuaciones y resoluciones para el desarrollo de investigaciones por probables incumplimientos a la Ley de Protección de Datos Personales, sus reglamentos y a las demás disposiciones aplicables, tanto para el sector público como privado, en materia de datos personales;
VIII. Suscribir todo tipo de actuaciones y resoluciones para la sustanciación del procedimiento de verificación, conforme a lo establecido en la Ley de Protección de Datos Personales, la Ley Federal, la Ley Federal de Procedimiento Administrativo y las demás disposiciones aplicables;

car que éste, al ser un acto de autoridad, debe ser notificado personalmente al presunto infractor en el domicilio que haya señalado para tal efecto, así como al denunciante en su domicilio o al medio electrónico que hubiere precisado.[48]

Finalmente, es relevante destacar que el Acuerdo de Inicio de Procedimiento de Verificación al ser el acto que da inicio al PV, representa también el momento procesal a través del cual habrá de comenzar el cómputo del plazo de duración del PV.[49]

Acuerdo de Inicio de Procedimiento de Verificación en el sector público

El Acuerdo de inicio de Procedimiento de Verificación también se encuentra regulado en la normatividad del sector público. En específico en los artículos 146 a 151 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que norman el PV.

El Acuerdo de Inicio del Procedimiento de Verificación responde a la atribución concedida por la LGPDPPSO al INAI y los órganos garantes locales para vigilar y verificar el cumplimiento de las disposiciones contenidas en la LGPDPPSO y demás ordenamientos que se deriven de ella.[50] La atribución de vigilancia, anteriormente referida, incluye la concreción de acciones de investigación preliminar que se dan a través de las unidades administrativas competentes.[51]

En relación con lo anterior, el primer párrafo del artículo 149 de la LGPDPPSO dispone que la verificación iniciará de la siguiente forma:

> La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.
>
> [...]

Dicha orden escrita que funda y motiva la actuación verificadora del INAI y/o los organis-

---

IX. Realizar las notificaciones en el ámbito de su competencia;
X. Elaborar y turnar los proyectos de resoluciones que correspondan con motivo de la sustanciación del procedimiento de verificación previsto en la Ley de Protección de Datos Personales.
XI. Las demás que deriven de la normatividad aplicable en la materia, y las que disponga el Pleno, el comisionado presidente y el secretario de Protección de Datos Personales. (Énfasis añadido).

48 Artículo 61. El Acuerdo de Inicio de Procedimiento de Verificación se deberá notificar personalmente al responsable en el domicilio que éste haya señalado para tal efecto y al denunciante en su domicilio o medio electrónico que, para el caso, haya precisado.

49 "Desarrollo de la verificación
Artículo 132. El procedimiento de verificación tendrá una duración máxima de ciento ochenta días, este plazo comenzará a contar a partir de la fecha en que el Pleno hubiera dictado el acuerdo de inicio y concluirá con la determinación del mismo, el cual no excederá de ciento ochenta días. El Pleno del Instituto podrá ampliar por una vez y hasta por un periodo igual este plazo.
El Instituto podrá realizar diversas visitas de verificaciones para allegarse de los elementos de convicción necesarios, las cuales se desarrollarán en un plazo máximo de 10 días cada una. Este plazo deberá ser notificado al responsable o encargado y, en su caso, al denunciante".

50 Artículo 146. El Instituto y los organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta.
En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los organismos garantes estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.
El responsable no podrá negar el acceso a la documentación solicitada con motivo de una verificación, o a sus bases de datos personales, ni podrá invocar la reserva o la confidencialidad de la información.

51 *Vid.* artículos 189, 190, 191, 192, 193, 194, 195, 196, 197, 198 y 199 de los Lineamientos de Protección de Datos Personales para el Sector Público.

mos garantes es el Acuerdo de Inicio del Procedimiento de Verificación. Derivado de las acciones de investigación preliminar reguladas en los Lineamientos de Protección de Datos Personales para el Sector Público (en adelante Lineamientos de Protección de Datos Personales) se señala en el artículo 198 de dicho ordenamiento que, una vez concluida la investigación previa, el INAI podrá emitir un:

a) Acuerdo de determinación: Se expedirá, de manera fundada y motivada, cuando no cuente con elementos suficientes para acreditar actos u omisiones que presuntamente constituyan un incumplimiento a lo establecido por la LGPDPPSO y los Lineamientos de Protección de Datos Personales.

b) Inicio del Procedimiento de Verificación. Cuando, de manera fundada y motivada, se presuma que el responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la Ley General y los presentes Lineamientos generales. Será resultado de la conclusión de las investigaciones previas realizadas por la autoridad garante y en virtud de las cuales, de manera fundada y motivada, se presume que el responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la normatividad de datos personales.

En este orden de ideas, los Lineamientos de Protección de Datos Personales hacen referencia al Acuerdo de Inicio de Verificación y precisan que se trata de una "orden escrita que funda y motiva la procedencia de la actuación por parte del Instituto, a través de la unidad administrativa competente conforme a su estatuto orgánico vigente, y tiene por objeto establecer las bases para requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su saco, en el lugar donde están ubicadas las bases de datos personales respectivas".[52]

En relación con los sujetos habilitados para la emisión del Acuerdo de Inicio de Verificación, los citados Lineamientos facultan al Pleno del INAI, o bien, por las unidades administrativas del INAI competentes de conformidad con lo dispuesto en el estatuto orgánico vigente al momento de emitirse el Acuerdo de Inicio de Verificación.[53]

Finalmente, debe tenerse en cuenta que el Acuerdo de Inicio de Verificación debe notificarse de forma personal al responsable en el domicilio que haya indicado para recibir notificaciones en el PV y cuando el mismo tenga origen en una denuncia, deberá ser notificado al titular de los datos en el medio que haya indicado.[54]

52 "Acuerdo de inicio:
Artículo 201. El procedimiento de verificación iniciará con la emisión del acuerdo de inicio a que hace referencia el artículo 198, fracción II de los presentes Lineamientos generales, el cual constituye una orden escrita que funda y motiva la procedencia de la actuación por parte del Instituto, a través de la unidad administrativa competente conforme a su Estatuto Orgánico vigente, y tiene por objeto establecer las bases para requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su saco, en el lugar donde están ubicadas las bases de datos personales respectivas.
[...]".

53 Artículo 201. [...] El acuerdo de inicio del procedimiento de verificación podrá ser emitido por el Pleno del Instituto, o bien, por las unidades administrativas del Instituto competentes de conformidad con lo dispuesto en el estatuto orgánico vigente al momento de emitirse el acuerdo a que se refiere el presente artículo.

54 Notificación del Acuerdo de Inicio de Procedimiento de Verificación. Artículo 203. El Acuerdo de Inicio del Procedimiento de Verificación se deberá notificar personalmente al responsable en el domicilio que hubiere señalado para tal efecto y, en los casos en que el procedimiento hubiera iniciado por medio de una denuncia, también se deberá notificar al denunciante en el medio que, para el caso concreto, hubiera designado.

Afectación significativa

Andrés Velázquez Olavarrieta

La palabra afectar se refiere a "producir algo, un determinado efecto, generalmente negativo" y "perjudicar, producir daño", entre otras acepciones.[55] En tanto que significativo se refiere a que "tiene importancia, valor o relevancia", por lo tanto, una afectación significativa se refiere a un hecho que modifica sustancialmente un estado, orden o proceso. Y dado que la afectación generalmente es negativa, esa modificación sustancial también lo es.

Para efecto de la protección de datos personales, tanto en posesión de los particulares como de sujetos obligados, una afectación significativa puede aplicarse a las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento de los datos que tengan que ver con los derechos patrimoniales o morales de los titulares.

Ámbito de aplicación

Olivia Andrea Mendoza Enríquez

El ámbito de aplicación define la validez de una ley, es decir, cuándo, dónde y a quién le son aplicables leyes determinadas. Sus componentes son a) ámbito espacial de validez: limita el territorio y espacio respecto a la aplicación de la ley y permite determinar la jurisdicción competente en su caso, b) ámbito temporal de validez: define la temporalidad de aplicación de la Ley, es decir, la obligatoriedad en el cumplimiento de la ley a partir de su publicación u otorgando periodos especiales en los transitorios de dichas leyes (en este apartado se debe considerar la interpretación del principio pro persona a favor de beneficios del titular de datos personales, pero no de perjuicios, c) ámbito personal de validez: define los sujetos obligados a cumplir con la Ley, d) ámbito material de validez: refiere a la competencia de las autoridades facultadas, pudiendo ser federal, estatal y/o municipal.

Una vez establecido lo anterior, es necesario recapitular que en México la normativa en materia de protección de datos personales se ha dividido entre la de aplicación al ámbito privado y la de aplicación al sector público y partidos políticos.

En México, el desarrollo normativo de ambas materias se ha dado de forma desfasada, ya que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) surge en 2010 y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) es publicada en 2017. Es decir, por una parte, existía un marco legal fortalecido en materia de protección de datos personales en el sector privado y casi nulas disposiciones para el tratamiento de los datos en el sector público, o en el mejor de los casos, la dimensión del derecho de protección de datos personales solo existía como un limitante del derecho de acceso a la información y no como un derecho humano autónomo.

Dicho lo anterior, en las siguientes líneas analizaremos el ámbito de aplicación establecido por las leyes mencionadas previamente y las disposiciones secundarias.

La LFPDPPP es de orden público y de observancia general en toda la República. Su objeto es la protección de los datos personales en posesión de los particulares con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.[56]

55 Real Academia Española. (2019). *Diccionario de la Lengua Española*. Disponible en: https://dle.rae.es/?id=0wAWT95. Fecha de consulta: 7 de enero de 2019.

56 Artículo 1 de la LFPDPPP.

Los sujetos regulados por esta ley son los particulares, ya sean personas físicas o morales, de carácter privado que lleven a cabo el tratamiento de datos personales, a excepción de las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal y sin fines de divulgación o utilización comercial.[57]

Por su parte, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) señala que tiene por objeto regular las disposiciones de la LFPDPPP y su ámbito de aplicación será respecto al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.[58]

El ámbito territorial de aplicación de dicho reglamento será a todo tratamiento cuando: sea efectuado en un establecimiento del responsable ubicado en territorio mexicano,[59] sea efectuado por un encargado con independencia de su ubicación a nombre de un responsable establecido en territorio mexicano, cuando el responsable no esté establecido en territorio mexicano pero le resulte aplicable la legislación mexicana derivado de la celebración de un contrato o en términos del derecho internacional y cuando el responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio —salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento.[60]

Por otro lado, la LGPDPPSO establece que es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6 base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en materia de protección de datos personales en posesión de sujetos obligados.[61] En este rubro, los sujetos obligados de la LGPDPPSO en el ámbito federal, estatal y municipal son cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Todas las disposiciones de la LGPDPPSO, según corresponda en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

Esta ley tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados.

57 Artículo 2 de la LFPDPPP.

58 Artículo 1 y 3 del RLFPDPPP.

59 En el caso de personas físicas, el establecimiento se entenderá como el local en donde se encuentre el principal asiento de sus negocios o el que utilicen para el desempeño de sus actividades o su casa habitación. Tratándose de personas morales, el establecimiento se entenderá como el local en donde se encuentre la administración principal del negocio, si se trata de personas morales residentes en el extranjero, el local en donde se encuentre la administración principal del negocio en territorio mexicano o en su defecto el que designen o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad. Lo anterior, de conformidad con el artículo 4 del RLFPDPPP.

60 Artículo 4 del RLFPDPPP.

61 Artículo 1 de la LGPDPPSO.

Amenaza

Andrés Velázquez Olavarrieta

La *Guía para la Implementación de un Sistema de Gestión de Seguridad de Datos Personales* (SGSDP) considera diversos conceptos clave, uno de ellos es el de amenaza. La define como la circunstancia o evento con la capacidad de causar daño a una organización. En el campo de la informática se habla de amenazas cibernéticas o ciberamenazas,[62] la cuales son amenazas a la seguridad de la información o a la informática. El concepto hace referencia a una situación potencial que supone un daño para un activo[63] o para un control implementado por una persona o en una organización, con cierta probabilidad de ocurrencia.

En el anexo B de la SGSDP del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se establece una serie de amenazas a partir del origen, motivación/causa y posibles consecuencias. De ahí se desprende que las amenazas varían en el tiempo y las causas pueden ser clasificadas en internas y externas, de origen natural o humano, y ser accidentales o deliberadas. Las amenazas deben ser identificadas considerando que algunas pueden afectar a más de un activo al mismo tiempo.

Dentro de las primeras está una gestión deficiente, falta de formación, ausencia de políticas y procedimientos, así como ausencia de mecanismos de disuasión, los cuales habitualmente facilitan o desencadenan un incidente de fuga de información. Las segundas tienen como actores a agentes externos a la propia red o sistema que consiguen acceder a información no autorizada y/o modificar o interferir el propio funcionamiento del sistema mediante el ataque por medios telemáticos de las vulnerabilidades del sistema. Las amenazas, tanto internas como externas, por lo general, implican la ausencia o ineficiencia de algún tipo de control o medida de seguridad.

Análisis de brecha

Andrés Velázquez Olavarrieta

El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) en el artículo 61 señala nueve acciones para la seguridad de los datos personales. La sexta considera el análisis de brecha, el cual es planteado como la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales. Por su importancia el artículo 33 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) también plantea la necesidad de realizar un análisis de brecha que también es mencionado en el artículo 35 como parte de un documento de seguridad.

Por lo tanto, el análisis de brecha se puede definir como la concentración de elementos específicos que pueden existir entre lo deseable y lo actual, para ello es importante definir con claridad cuál es la brecha que se desea analizar, identificar quiénes están involucrados, establecer cuáles son las causas más relevantes que determinan la brecha, identificar las diferencias de comportamiento entre los sistemas o actores a comparar en la brecha, identificar

62 Se pueden definir como las actividades realizadas en el ciberespacio que tienen por objeto el uso de la información para cometer diversos delitos mediante su utilización, manipulación, control o sustracción.

63 En la guía del INAI para la implementación de un sistema de gestión de seguridad de datos personales (junio 2015) es definido como "la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales, que tenga valor para la organización".

los indicadores y/o atributos de la situación actual y elaborar un listado con la finalidad de medir o caracterizar la brecha.

En síntesis, el análisis de brecha debe aportar lo contenido en los Lineamientos Generales de Protección de Datos Personales para el Sector Público, que en el artículo 61 (con relación al artículo 33, fracción V de la LGPDPPSO) establece que para la realización del análisis de brecha, el responsable deberá considerar las medidas de seguridad existentes y efectivas, las medidas de seguridad faltantes y la existencia de nuevas medidas de seguridad que pudieran reemplazar a uno o más controles implementados actualmente.

Análisis de riesgo

Andrés Velázquez Olavarrieta

Tanto el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) consideran que se debe contar con un análisis de riesgos de datos personales para identificar peligros y estimar los riesgos, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento como pueden ser, de manera enunciativa más no limitativa: *hardware, software,* personal del responsable, entre otros.

El responsable de esta actividad deberá considerar los requerimientos regulatorios, códigos de conducta o mejores prácticas de un sector específico, el valor de los datos personales de acuerdo con su clasificación previamente definida y su ciclo de vida, el valor y exposición de los activos involucrados en el tratamiento de datos personales y las consecuencias negativas para los titulares que pudieran derivar de una vulneración de seguridad ocurrida.

Los beneficios de contar con un análisis de riesgos son grandes y algunos de ellos son: soporte a decisiones estratégicas, apoyo en la definición y asignación efectiva de recursos, justificar esfuerzos en tiempo, recurso humano y financieros, promover la mejora continua, transmitir confianza a empleados, clientes y otros socios de negocio, además de servir como uno de los pilares de los Sistemas de Gestión de Seguridad de la Información.

La *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP) publicada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en junio de 2015, destaca la importancia de realizar el análisis de riesgo de los datos personales, debido a que la seguridad se basa en el entendimiento de la naturaleza del riesgo al que están expuestos los datos personales, y a que el riesgo no se puede erradicar completamente, pero sí se puede minimizar a través de la mejora continua.

Anonimización

Isabel Davara Fernández de Marcos,[64]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El término anonimización[65] se refiere a la aplicación de determinadas técnicas o procedimientos tendientes a impedir la identificación o reidentificación de una persona física[66] sin que para ello sea necesario el empleo de esfuerzos desproporcionados.

En el ámbito nacional, ni la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) ni la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) se contempla el concepto de anonimización, sino el de disociación.[67] La disociación es "el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo".[68]

No obstante, como podremos comprobar tras la lectura de esta definición, los efectos del proceso de disociación son en esencia los mismos que los de la anonimización, esto es: que el dato ya no esté asociado ni pueda asociarse a su titular, en otras palabras, que el dato deje de ser identificado o identificable, y en esencia, podemos concluir que la anonimización y disociación son equiparables.

Para comprender el alcance del término de anonimización resulta necesario referirse a la definición general de lo que se considera como anónimo, pues a partir de la aplicación de medidas específicas y legalmente admitidas, se dota a los datos personales de dicha característica con el ánimo de que no se permita identificar o reidentificar a la persona, y, por lo tanto, dejen de ser considerados datos personales.[69]

En este contexto, al analizar el concepto de dato personal, el Grupo de Trabajo del Artículo 29 (GTA29)[70] señala que los datos anónimos[71] pueden definirse como "cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona".[72]

64 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

65 En relación con el contenido de esta definición recomendamos consultar también las definiciones de "disociación", "seudonimización" y "*big-data*" que forman parte de este diccionario.

66 Recomendamos consultar la definición de "persona física identificable" que forma parte de este diccionario.

67 Se recomienda consultar la definición de "disociación" presente en este diccionario.

68 Artículo 3, fracción VIII de la LFPDPPP y en el artículo 3, fracción XIII de la LGPDPPSO.

69 De acuerdo con el *Diccionario de la Lengua Española*, la palabra anónimo tiene distintas acepciones, entre ellas podemos destacar las siguientes: 1) dicho de una obra o de un escrito que no lleva el nombre de su autor, 2) dicho de una persona, especialmente un autor de nombre desconocido o que se oculta y 3) situación de quien oculta su nombre. RAE. (2019). Anónimo. En *Diccionario de la Lengua Española*. Recuperado de: https://dle.rae.es/?id=2jjRwOu

70 Este grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

71 El Grupo de Trabajo del Artículo 29 (GTA29) ha estudiado el tema del anonimato. La Recomendación 3/97 del 3 de diciembre de 1997 está disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_es.pdf

72 GTA29. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007, WP 136, p.23. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf Fecha de consulta: 14 de noviembre de 2018.

De esta forma, en el ámbito del derecho de protección de datos personales, la anonimización hace referencia a la característica de los datos personales a partir de los cuales no es posible inferir o determinar la identidad de la persona a la que pertenecen, de modo que, los datos se consideran como anónimos conforme a la definición general antes referida. Por lo tanto, cuando los datos ya no se refieren a una persona física identificada o identificable dejan de ser personales y, en consecuencia, no se aplica la legislación. Es decir, cuando los datos son verdaderamente anónimos ya no pueden ser personales, porque no se puede conocer al titular de los mismos que es a quien protege la legislación.

En el entorno normativo internacional, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) definen a la anonimización como "la aplicación de medidas de cualquier naturaleza dirigidas a impedir la identificación o reidentificación de una persona física sin esfuerzos desproporcionados".[73] Es decir, la anonimización se considera como una forma de eliminar las posibilidades de identificación de las personas.[74]

Con base en lo anterior, se desprende que el propósito de la anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales.[75] De esta manera, los datos anonimizados son los datos anónimos que con anterioridad se referían a una persona identificable, pero cuya identificación ya no es posible.[76]

Así, el GTA29 ha destacado[77] que la anonimización cuenta con las siguientes características:

1. Puede ser el resultado de un tratamiento de datos personales realizado para impedir, de forma irreversible, la identificación del interesado.[78]

73 Artículo 2.1 a) de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

74 Agencia Española de Protección de Datos (AEPD). (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personale*s. España, p.1. Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

75 AEPD. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personale*s, p.2.

76 El Grupo de Trabajo del Artículo 29, en referencia al tema de anonimato, señala: "es preciso que esté regulada la utilización que hace el servicio de los datos de identificación que conserva". El Grupo de Trabajo del Artículo 29 ha estudiado el tema del anonimato. La Recomendación 3/97 del 3 de diciembre de 1997 puede consultarse en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1997/wp6_es.pdf

77 GTA29. (2014). *Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014, WP 216*, p.7. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf Fecha de consulta: 14 de noviembre de 2018.

78 El GTA29 ha destacado que debe subrayarse que además de que la anonimización ha de ajustarse a las restricciones legales que recuerda el Tribunal de Justicia de la Unión Europea en su sentencia sobre el asunto C-553/07 (College van burgemeester en wethouders van Rotterdam contra M.E.E. Rijkeboer) y que se refieren a la necesidad de conservar los datos en un formato identificable a fin de que puedan ejercerse, por ejemplo, los derechos de acceso por parte de los interesados. En concreto, el Tribunal señala que "el artículo 12, letra A de la Directiva [95/46/CE] obliga a los Estados miembros a garantizar un derecho de acceso a la información sobre los destinatarios o categorías de destinatarios a quienes se comunican los datos y al contenido de la información comunicada, no solo para el presente, sino también para el pasado. Corresponde a los Estados miembros fijar un plazo de conservación de dicha información, así como el acceso correlativo a ésta, guardando un justo equilibrio entre, por un lado, el interés del afectado en proteger su intimidad, concretamente a través de las distintas vías de intervención y de recurso previstas por la directiva y, por otro, la carga que la obligación de dicha información puede representar para el responsable del tratamiento". GTA29. Dictamen 05/2014 sobre técnicas de anonimización. Adoptado el 10 de abril de 2014.

2. Pueden considerarse varias técnicas de anonimización sin que la legislación contenga ninguna norma prescriptiva. Por ejemplo, el GTA29 señala que las técnicas de anonimización más comunes se dividen en dos enfoques generales: aleatorización y generalización.[79]
3. Hay que dar importancia a los elementos contextuales: debe considerarse "el conjunto de los medios que puedan ser razonablemente utilizados" para la identificación por parte del responsable del tratamiento o de un tercero, prestando especial atención a lo que se entiende, en el estado actual de la técnica, como "medios que puedan ser razonablemente utilizados" (dado el incremento de la potencia de las computadoras y de las herramientas disponibles).
4. La anonimización lleva implícito un factor de riesgo que ha de tenerse en cuenta al evaluar la validez de las técnicas, incluidos los posibles usos de los datos "anonimizados" mediante éstas, además de considerarse la gravedad y probabilidad del riesgo. Sobre este particular, el GTA29[80] señala que existe tres riesgos claves de la anonimización que pueden darse de forma separada:

   a) Singularización: la posibilidad de extraer de un conjunto de datos algunos registros —o todos los registros— que identifican a una persona.

   b) Vinculabilidad: la capacidad de vincular como mínimo dos registros de un único interesado o de un grupo de interesados, ya sea en la misma base de datos o en dos bases de datos distintas.

   c) Inferencia: la posibilidad de deducir con una probabilidad significativa el valor de un atributo a partir de los valores de un conjunto de otros.

En cuanto al momento de su confección, el proceso de anonimización es recomendado desde las etapas iniciales del diseño[81] del sistema de información o del producto utilizado para el proceso de anonimización y durante todo el ciclo de vida de dicho producto o sistema de información. Se ha admitido[82] que el concepto de privacidad desde el diseño en los procesos de anonimización puede resumirse en la aplicación de los siguientes principios:

1. Principio proactivo. La Agencia Española de Protección de Datos (AEPD) destaca que la protección de la privacidad es el primer objetivo de la anonimización y su gestión debe realizarse de forma proactiva y no reactiva. Es decir, desde el inicio conceptual del diseño del sistema de información o producto a utilizar en el proceso de anonimización se tomarán las medidas necesarias para garantizar la privacidad de las personas.[83]
2. Principio de privacidad por defecto.[84] En relación con este principio la AEPD puntualiza que es necesario que desde el inicio del sistema de información o producto se

79 GTA29. (2014). *Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014, WP 216*, p.7. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

80 Ídem.

81 Recomendamos consultar la definición de "protección de datos personales por diseño" que forma parte de este *Diccionario de Protección de Datos Personales*.

82 Agencia Española de Protección de Datos. (2016). Orientaciones y garantías en los procedimientos de anonimización de datos personales. España, Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

83 El Principio proactivo también señala que "la privacidad no puede garantizarse a posteriori como el resultado de la reparación de brechas existentes en el proceso de anonimización o perjuicios ocasionados a los interesados". Agencia Española de Protección de Datos. (2016) *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. España, Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

84 En relación con este concepto, recomendamos consultar la definición de "Protección de datos personales por defecto" que forma parte de este diccionario.

salvaguarde la privacidad teniendo en cuenta la granularidad o grado de detalle final que deben tener los datos anonimizados.[85]

3. Evaluación de Impacto en la Protección de Datos (EIPD). En relación con este principio se recomienda la práctica de una EIPD[86] considerando las particularidades del tratamiento presente, así como los elementos normativamente requeridos.
4. Principio de privacidad objetiva. Señala la AEPD que como resultado de la EIPD existirá un umbral[87] de riesgo o índice de riesgo residual de reidentificación que será asumido por el responsable del tratamiento como riesgo aceptable y será tenido en consideración para el diseño del proceso de anonimización.
5. Principio de plena funcionalidad. En relación con este principio se ha precisado que desde el inicio del diseño del sistema de información se tendrá en cuenta la utilidad final de los datos anonimizados, garantizando, en la medida de lo posible, la inexistencia de distorsión con relación a los datos no anonimizados.[88]
6. Principio de privacidad en el ciclo de vida de la información. De acuerdo con la AEPD, este principio demanda que las medidas que garantizan la privacidad de los interesados sean aplicables durante el ciclo completo de la vida de la información partiendo de la información sin anonimizar.[89]
7. Principio de información y formación. Según este principio es necesario que se facilite formación e información al personal involucrado en el proceso de anonimización y en la explotación de la información anonimizada. Es decir, que, durante el ciclo de vida de la información, todo el personal con acceso a los datos anonimizados o no anonimizados debe estar convenientemente formado e informado sobre sus obligaciones.[90]

De acuerdo con las características y elementos conceptuales anteriormente explicados, la anonimización es entendida como un caso particular de tratamiento posterior de datos personales y que puede considerarse compatible con el fin original del tratamiento, aunque solo con la condición de que el proceso de anonimización genere fiablemente información anonimizada en el sentido anteriormente descrito.[91]

85 Agencia Española de Protección de Datos. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. España. Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

86 En relación con este concepto, recomendamos consultar la definición de "Evaluación de Impacto en la Protección de Datos" que forma parte de este diccionario.

87 La Agencia Española de Protección de Datos, explica que el umbral de riesgo residual de reidentificación será conocido por el destinatario de la información anonimizada y, cuando los datos anonimizados sean para uso público, también se dará a conocer públicamente informando de dicho riesgo a las personas o entidades que utilicen la información. Orientaciones y garantías en los procedimientos de anonimización de datos personales. España. Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

88 En algunos casos, y con el fin de garantizar la privacidad de las personas, puede ser necesario utilizar distorsiones de rango geográficas como en el caso de personas con patologías extremadamente raras, de requerir mayor información puede consultar: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

89 Agencia Española de Protección de Datos. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. España. Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

90 Agencia Española de Protección de Datos. (2016). *Orientaciones y garantías en los procedimientos de anonimización de datos personales*. España. Disponible en: https://www.aepd.es/media/guias/guia-orientaciones-procedimientos-anonimizacion.pdf

91 GTA29. (2014). *Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014, WP 216*, p.7. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Aprendizaje de máquinas

Erik Huesca Morales

Derivado del desarrollo de la inteligencia artificial en las ciencias de la computación, el aprendizaje de máquinas o aprendizaje automático es la capacidad que se le da a un programa de computadora para adquirir (basado en reglas heurísticas y éticas bien definidas) nuevos conocimientos derivados del procesamiento de datos y su análisis estadístico. En la actualidad esta función se asocia, de manera biunívoca, a las redes neuronales o a conceptos como aprendizaje profundo, siendo estas dos últimas mecanismos o estrategias para reflejar un aprendizaje de máquinas.

Por lo general, dichos programas están orientados a generalizar comportamientos y crear modelos sobre los mismos. Los comportamientos pueden ser de la naturaleza o derivados de las acciones humanas en terrenos específicos. Para lograrlo, los programas de aprendizaje de máquinas dependen fuertemente de las reglas éticas[92] con las que fueron programados, así como de los modelos para el manejo de los datos, de los cuales se distinguen —al menos— tres categorías: geométricos, probabilísticos y lógicos.

La importancia de este término radica en que tiene implicaciones en el manejo de datos personales pues su aplicación, por lo general, va desde conocer secuencias genéticas hasta el manejo del mercado de valores.

Otro de los aspectos éticos necesarios de explicitar en el aprendizaje automático o de máquinas son los modelos en los que se basa dicho aprendizaje, es decir la forma en que procesará los datos para emitir un resultado. Estas formas o modelos de procesamiento pueden ser:

a) Supervisado. Basado en ejemplos y patrones de datos dados al programa que constituyen su universo para la toma de decisiones, por lo que especifica qué conjuntos de datos son satisfactorios para el objetivo del aprendizaje.
b) No supervisado. Contiene ejemplos y patrones de datos iniciales, pero no se tiene información sobre los patrones de los ejemplos, por lo tanto, el programa no cuenta con datos que definan qué información es adecuada y tiene que ser capaz de crear nuevas clasificaciones.
c) Semisupervisado. Una combinación de datos etiquetados en ejemplos, patrones y datos no etiquetados.

Los resultados obtenidos estarán, en todos los casos, retroalimentado al modelo y su toma de decisiones.

Archivo electrónico

Jonathan Gabriel Garzón Galván

Un archivo electrónico debe analizarse en dos sentidos: amplio y estricto. En sentido amplio, debe siempre ser conceptualizado como un tipo de mensaje de datos. Lo anterior debido a que un archivo electrónico, de forma general, siempre es información generada, almacenada o transmitida a través de medios electrónicos, ópticos o por cualquier otra tecnología, lo cual consiste en la propia definición de mensaje de datos.[93]

92 Se puede consultar la definición de “ética de los objetos”.

93 Véase la definición de “documento electrónico (mensaje de datos)” del presente diccionario.

En este sentido, el 12 de junio de 2009 la Ley Federal del Procedimiento Contencioso Administrativo (LFPCA) fue modificada para dar vida al Juicio en Línea, adicionando a dicha ley el capítulo X al título II, así como un artículo 1-A de definiciones,[94] dentro de las cuales se encuentra la de archivo electrónico, documento electrónico o digital y expediente electrónico, pero no se encuentra la definición de mensaje de datos.

> [...]
>
> II. Archivo electrónico: información contenida en texto, imagen, audio o video generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología que forma parte del Expediente Electrónico.
>
> [...]
>
> VIII. Documento electrónico o digital: todo mensaje de datos que contiene texto o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología que forma parte del Expediente Electrónico.
>
> IX. Expediente electrónico: conjunto de información contenida en archivos electrónicos o documentos digitales que conforman un juicio contencioso administrativo federal, independientemente de que sea texto, imagen, audio o video, identificado por un número específico.
>
> [...]

Si comparamos estas definiciones con las de "mensaje de datos" contenidas en la Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) de 1996 y las del Código de Comercio incluidas en mayo del 2000, podemos observar que hay grandes similitudes, por lo que es posible utilizarlos en algunos casos de manera indistinta.

Artículo 89 del Código de Comercio:[95]

> Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Artículo 2 de la Ley Modelo de Comercio Electrónico de la CNUDMI:[96]

> Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), correo electrónico, telegrama, télex o telefax.

De estos artículos podemos concluir que en materia contenciosa administrativa debemos diferenciar el archivo y el documento electrónico por el medio en que la información es manejada, para el primero es viable que sea texto, audio, video o imagen, y para el segundo únicamente textos escritos. Ambos deberán ser parte del expediente electrónico para cumplir los requisitos de esta definición.

Retomando el análisis que se realiza al inicio, en sentido estricto, un archivo electrónico tiene una función especifica inmersa en su conceptualización, que es la de archivar. Por ello, es posible diferenciar el concepto de archivo electrónico del de mensaje de datos, para hacer referencia a un conjunto de documentos electrónicos o mensajes de datos que tienen características en común o se encuentran relacionados entre sí, y por lo tanto son agrupados para su mejor gestión, guarda, custodia y/o control dentro de un sistema de cómputo de

94 Ley Federal del Procedimiento Contencioso Administrativo. Última reforma *Diario Oficial de la Federación*. 27 de enero de 2017. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf

95 DOF. (2018, marzo 28). "Código de Comercio, última reforma". *Diario Oficial de la Federación*. Disponible en: http://www.diputados.gob.mx/Leyes Biblio/pdf /3_280318.pdf

96 Ley modelo de la CNUDMI sobre comercio electrónico y su guía para su incorporación al derecho interno. Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

alguna dependencia o entidad pública. Lo anterior se realiza conforme a la definición base de la palabra "archivo".[97]

> Archivo: del lat. *archīvum* y éste del gr. *ἀρχεῖον archeîon.*
>
> Conjunto ordenado de documentos que una persona, sociedad o institución produce en el ejercicio de sus funciones o actividades.
>
> Conjunto de datos almacenados en la memoria de una computadora y que puede manejarse con una instrucción única.

Al diferenciar el concepto de archivo electrónico de mensaje de datos, es posible establecerle requerimientos, especificaciones, reglas y condiciones especiales al manejo, trazabilidad y almacenamiento de conjuntos de mensajes de datos en las actuaciones administrativas o en su conservación por valor histórico.

La Ley General de Archivos, que tiene por objeto establecer los principios y bases generales para la organización y conservación, administración y preservación homogénea de los archivos físicos y electrónicos en posesión de cualquier sujeto obligado,[98] aporta varias definiciones en su artículo 4 relacionadas al archivo electrónico:[99]

a) Archivo: conjunto organizado de documentos producidos o recibidos por los sujetos obligados en el ejercicio de sus atribuciones y funciones, con independencia del soporte, espacio o lugar que se resguarden.
b) Expediente: unidad documental compuesta por documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados.
c) Expediente electrónico: conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.
d) Documento de archivo: es aquel que registra un hecho, acto administrativo, jurídico, fiscal o contable producido, recibido y utilizado en el ejercicio de las facultades, competencias o funciones de los sujetos obligados, con independencia de su soporte documental.
e) Documentos históricos: son los que se preservan permanentemente porque poseen valores evidenciables, testimoniales e informativos relevantes para la sociedad, y que por ello forman parte íntegra de la memoria colectiva del país y son fundamentales para el conocimiento de la historia nacional, regional o local.
f) Gestión documental: tratamiento integral de la documentación a lo largo de su ciclo vital, a través de la ejecución de procesos de producción, organización, acceso, consulta, valoración documental y conservación.
g) Trazabilidad: cualidad que permite, a través de un sistema automatizado para la gestión documental y administración de archivos, identificar el acceso y la modificación de documentos electrónicos.

97 Real Academia Española. (2017). *Diccionario de la Lengua Española.* Recuperado de: http://dle.rae.es/ Fecha de consulta: agosto 2018.

98 Son sujetos obligados toda autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la federación, las entidades federativas y los municipios, así como personas físicas o morales que cuenten con archivos privados de interés público.

99 Cámara de diputados. (2018). *Ley General de Archivos.* Recuperada de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA_150618.pdf

Como se puede percibir gracias a estas definiciones, un archivo puede ser conservado y manejado a través de medios electrónicos, ya que permiten el resguardo y gestión del conjunto de documentos en cualquier soporte, dando vida así al archivo electrónico. Así mismo, el expediente electrónico se entiende como un conjunto de documentos electrónicos (o mensajes de datos) vinculados entre sí, al pertenecer a una actuación administrativa. En ambos casos el concepto de trazabilidad adquiere relevancia para mantener su integridad y accesibilidad.

En conclusión, los conceptos "archivo electrónico" y "documento electrónico y/o mensaje de datos" pueden ser usados indistintamente, con excepción de:

a) La materia archivística, donde las prácticas de gestión de la información electrónica y la organización de los archivos —cuyo tratamiento es automatizado a través de sistemas de cómputo— requiere de principios y procesos archivísticos diferentes para su acceso controlado y conservación de integridad durante todo el ciclo de vida de la misma.

b) La materia contenciosa administrativa, donde en adición al concepto de mensaje de datos se requiere que pertenezca a un expediente electrónico.

Auditoría

Christian Paredes González

El término "auditoría" viene del verbo latino *audire* que significa "oír" y que a su vez tiene su origen en los primeros auditores que ejercían su función juzgando la verdad o falsedad de lo que les era sometido a su verificación, principalmente mirando. Desde su acepción genérica hace referencia a la "revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse".[100]

En materia de protección de datos personales, el término auditoría aparece referido en la normatividad como parte de una de las acciones para garantizar la seguridad de los datos personales. De forma tal que la fracción VII del artículo 61 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) dispone que, a fin de establecer y mantener la seguridad de los datos personales, el responsable deberá lleva a cabo revisiones y/o auditorías.

Las Recomendaciones de Seguridad de Datos Personales publicadas en 2013 señalan a su vez que, para cumplir con el deber de seguridad, las organizaciones deberán de implementar un sistema de gestión de seguridad de datos personales (SGSDP) basado en el modelo denominado Planificar-Hacer-Verificar-Actuar (PHVA). Como parte de los procesos necesarios para el cumplimiento del deber de seguridad, las Recomendaciones indican que en el paso 8 de la metodología que sustenta el SGSDP se deberán comprender revisiones y auditorías para monitorear y revisar el SGSDP:

Paso 8. Revisiones y auditoría.

Fase 3. Monitorear y revisar el SGSDP

Revisiones y auditoría. Proceso de revisión del funcionamiento del SGSDP respecto a la política establecida, cada vez que exista un cambio en el contexto del alcance y objetivos del SGSDP.

100 Real Academia Española. 2019). "Auditoría". *Diccionario de la lengua española*. Disponible en: http://dle.rae.es/?id=4NVvRTc

- Revisión de los factores de riesgo. Consideraciones para monitorear el estado del riesgo y aplicar las modificaciones pertinentes para mejorar el SGSDP.
- Auditoría. Requerimientos para los procesos de auditoría interna/externa.
- Vulneraciones a la seguridad de la información. Consideraciones en caso de un incidente de seguridad.

En cuanto a la concreción práctica de las auditorías referidas en las Recomendaciones de Seguridad, la *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP), publicada en 2015,[101] señala que dentro del paso 8, para la implementación del SGSDP, las organizaciones deberán contar con un programa de auditoría interna para monitorear y revisar la eficacia y eficiencia del SGSDP.

La GISGSDP establece que el programa de auditoría interna debe planearse, establecerse y mantenerse tomando en cuenta la política de gestión de datos personales. En su caso, se recomienda que se establezcan y consideren auditorías a través de externos para procesos y circunstancias especiales, por ejemplo, cuando la organización desea unirse a un esquema de certificación.

Además se indica que, como parte del programa de auditoría de datos personales, se deben establecer previamente los objetivos del programa de auditoría, el cual debe incluir el alcance e indicar explícitamente cualquier tratamiento de datos personales interno y externo a la organización, responsables, recursos, criterios a utilizar durante la auditoría, así como los procesos y/o áreas que serán auditadas.

Un elemento fundamental en la práctica de auditorías, según lo recomendado por la GISGSDP, es asegurar la objetividad e imparcialidad del programa de auditoría mediante la apropiada selección de auditores y la conducción de la auditoría.

De esta manera, la GISGSDP recomienda que las auditorías deben llevarse a cabo en intervalos de tiempo planeados para determinar si el SGSDP:

a) está operando de acuerdo con la política de gestión de datos personales y con los procedimientos establecidos y
b) ha sido implementado y mantenido de acuerdo con los requerimientos tecnológicos.

Adicionalmente, se previene que como parte del proceso de auditoría se debe proporcionar a la alta dirección los reportes de las auditorías sobre el SGSDP, detallando cualquier desviación significativa de la política de gestión de datos personales, como pueden ser asuntos relacionados con los procesos de seguridad que puedan afectar su cumplimiento.

La GISGSDP detalla que la auditoría debe ofrecer al responsable información detallada respecto a cambios ocurridos en el SGSDP, además se debe realizar una auditoría inmediatamente después de la implementación de modificaciones mayores en el SGSDP o en los procesos críticos de la organización respecto al tratamiento de datos personales.

Se indica que, como resultado de una auditoría, se deben obtener observaciones sobre riesgos existentes para aplicar medidas preventivas, es decir, controles para que no ocurra una vulneración, así como observaciones sobre puntos que requieren medidas correctivas inmediatas.

En el sector público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) dispone en la fracción V de su artículo 30 que, para dar cumplimiento al principio de responsabilidad, los responsables deberán establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.

101 INAI. (2015). *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales.* Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

El párrafo primero del lineamiento 63 de los Lineamientos Generales de Protección de Datos para el Sector Público (Lineamientos Generales) señala que "el responsable deberá evaluar y medir los resultados de las políticas, planes, procesos y procedimientos implementados en materia de seguridad y tratamiento de los datos personales a fin de verificar el cumplimiento de los objetivos propuestos, y en su caso, implementar mejores de manera continua".

La LGPDPPSO incorpora también la figura de las auditorías voluntarias en su artículo 151[102] y señala que los responsables podrán, voluntariamente, someterse a la realización de auditorías por parte del Instituto o los organismos garantes, según corresponda y que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente ley y demás normativa que resulte aplicable.

El proceso de auditoría voluntaria aparece regulado en los Lineamientos Generales a partir del artículo 218 y hasta el artículo 231. En particular, el artículo 218 de los Lineamientos indica que dichas auditorías tendrán por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para cumplir con las disposiciones de la LGPDPPSO y los Lineamientos Generales.

Derivado de lo anterior, el 31 de agosto de 2018 se publicó en el *Diario Oficial de la Federación* (DOF) el acuerdo mediante el cual se aprobó el "Manual de Procedimientos para la realización de las auditorías voluntarias a que hace referencia el artículo 151 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados".[103] El manual citado es un importante referente en las auditorías para el sector público ya que facilita y estandariza las actividades de trabajo de las auditorías voluntarias en materia de protección de datos personales, desde la presentación de la solicitud correspondiente hasta la presentación del informe final de auditoría y, eventualmente, el seguimiento de los aspectos referidos en el citado manual.

Autenticación

Jonathan Gabriel Garzón Galván

Es aquella característica de un documento que permite identificar y vincular a las personas que lo crearon y/o que han aceptado o expresado su consentimiento para obligarse en términos de su contenido, sin que estas puedan repudiar su consentimiento o voluntad. Al respecto el *Diccionario de la Real Academia de la Lengua Española* (DRAE) señala: "documento auténtico. Der. Documento que está autorizado o legalizado".[104]

102 "Artículo 151. Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto o los organismos garantes, según corresponda, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.
El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan".

103 El citado acuerdo y su anexo están disponibles en: http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-08-08-2018.06.pdf

104 Real Academia Española. (2017). *Diccionario de la lengua española*. Recuperado de: http://dle.rae.es/ Fecha de consulta: agosto 2018.

El concepto de autenticación está unido al concepto de integridad y de atribución.[105] Dado que si un documento no es íntegro (está incompleto o ha sufrido modificaciones y/o alteraciones no autorizadas) no podrá ser atribuible a una persona, tanto en su autoría como en su vínculo con el contenido, y por lo tanto no sería auténtico. En este sentido, si un documento es auténtico, entonces es íntegro, pero no inversamente, porque requeriría, adicionalmente, ser atribuible a las personas. Es posible utilizar aquí un criterio de la Suprema Corte de Justicia de la Nación (SCJN):

> DOCUMENTOS AUTÉNTICOS. Decir que un documento es auténtico equivale a atribuirle tanto valor como si hubiera sido reconocido, puesto que el reconocimiento no tiene otro objeto que establecer la autenticidad del documento.[106]

Asimismo, vale la pena diferenciar las características de autenticación y no repudio. Ignacio Mendívil escribe sobre ello "... usted puede presenciar que un documento es escrito por alguien si lo vio hacerlo en persona. Si el documento no está firmado autógrafamente, usted estará absolutamente convencido de su autenticidad, pero no podrá probarlo ya que sin la firma autógrafa es imposible establecer el vínculo entre la voluntad de la persona y el contenido del documento. Si se puede probar a terceros, que efectivamente el documento es auténtico, entonces se dice que el documento es no repudiable. Si un documento es no repudiable es auténtico, pero no viceversa".[107]

Por lo comentado, es posible conocer quién es el autor de un documento, pero no necesariamente refleja su intención de vincularse con su contenido (no se cuenta con la atribución o su consentimiento para obligarse), ya que no hay vínculo entre la voluntad de la persona y el contenido del documento y por lo tanto no hay autenticidad del documento. Para lograr la atribución, generalmente se utiliza la firma como medio idóneo,[108] si bien no hay referencia legal explicita de lo anterior, el artículo 204 del Código Federal de Procedimientos Civiles (CFPC) hace alusión a la subscripción.[109]

Esta característica es relevante ya que los documentos auténticos son aquellos que proporcionan certeza probatoria al juzgador de los hechos que les conciernen y en caso de que sea objetada su autenticidad estos requerirán del cotejo y/o ratificación de firmas y/o contenido.[110]

105 Tellez, J. (2004). *Derecho Informático.* México, p. 248.

106 Robles, J. (1942, agosto 27). "Documentos auténticos". *Semanario Judicial de la Federación*. Disponible en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/352/352108.pdf

107 Mendívil, I. (2000). *El ABC de los Documentos Electrónicos Seguros*. SEGURIDATA, p. 1.

108 La Tercera Sala de la Suprema Corte de Justicia de la Nación ha establecido en tesis: "En principio, la firma estampada en un escrito constituye una manifestación de la voluntad que entraña conformidad con lo que ahí se asienta y además la autentifica; consecuentemente, quien reconoce como suya la que aparece en un documento, implícitamente reconoce el texto del mismo pues no sería propio que se expresara que la firma es propia pero el contenido es ajeno. No obstante, esta regla no debe aplicarse si de algún modo se demuestra que el interesado firmó en blanco, a la fuerza, que hay alteraciones o que se le impidió leerlo". Amparo directo 10250/83. Leyva Méndez Construcciones, S.A. de C.V. 23 de junio de 1986. Cinco votos. Ponente: Mariano Azuela Güitrón. Véase: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/239/239952.pdf

109 Código Federal de Procedimientos Civiles, última reforma. *Diario Oficial de la Federación*. 9 de abril de 2012. Véase: http://www.diputados .gob.mx/LeyesBiblio/pdf/6.pdf
"Artículo 204. Se reputa autor de un documento privado al que lo suscribe, (...) se entiende por subscripción la colocación, al pie del escrito, de las palabras que, con respecto al destino del mismo, sean idóneas para identificar a la persona que subscribe.
La subscripción hace plena fe de la formación del documento por cuenta del subscriptor, aun cuando el texto no haya sido escrito ni en todo ni en parte por él, excepto por lo que se refiere a agregados interlineales o marginales, cancelaciones o cualesquiera otras modificaciones contenidas en él, las cuales no se reputan provenientes del autor, si no están escritas por su mano, o no se ha hecho mención de ellas antes de la subscripción".

110 Código Federal de Procedimientos Civiles, última reforma. *Diario Oficial de la Federación*. 9 de abril de 2012. Véase: http://www.diputados .gob.mx/LeyesBiblio/pdf/6.pdf
Artículo 138**.** Podrá pedirse el cotejo de firmas, letras o huellas digitales, siempre que se niegue o que se ponga en duda la autenticidad de un documento privado.

No debe perderse de vista que la autenticación es requerida tanto para documentos físicos como para mensajes de datos y que el medio práctico más utilizado en ambos casos, como ya se mencionó, es la firma, aunque las nuevas tecnologías pueden proporcionar diversas formas de hacerlo como la autenticación cruzada vía redes sociales, *check box*, biométricos (huellas dactilares o estructura facial), entre otros.

Miguel Ángel Davara Rodríguez hace énfasis en que el problema de la firma, que conlleva la autenticación del documento, es la principal batalla para la real aceptación y efectos probatorios del mensaje de datos o documento electrónico, e incluso hace referencia a la Unión Europea a través del memorándum de acuerdo *Libre acceso al comercio electrónico de las PYME europeas* emitido, el cual indica que en los esquemas electrónicos la seguridad jurídica y técnica depende de una autenticación fiable y que sin ellos no se podrá contar con la confianza suficiente para la adopción del comercio electrónico.[111]

Por su parte, y continuando con la autenticación en medios electrónicos, la guía para la incorporación al derecho interno de la Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) hace especial énfasis en ello, relacionándolo con el propio artículo 7 de dicha comisión:[112]

> 56. Para evitar que se niegue validez jurídica a un mensaje que deba autenticarse por el mero hecho de que no está autenticado en la forma característica de los documentos consignados sobre papel, el artículo 7 ofrece una fórmula general. El artículo define las condiciones generales que, de cumplirse, autenticarían un mensaje de datos con suficiente credibilidad para satisfacer los requisitos de firma que actualmente obstaculizan el comercio electrónico [...].
>
> 59. [...] Así pues, puede considerarse que el artículo 7 establece una norma mínima de autenticación para los mensajes de datos intercambiados en ausencia de una relación contractual previa y, al mismo tiempo, da orientación sobre lo que eventualmente podría suplir la firma cuando las partes recurrieran a comunicaciones electrónicas en el contexto de un convenio de comunicaciones. Por consiguiente, la ley modelo tiene la finalidad de aportar una orientación útil cuando el derecho interno deje totalmente a la discreción de las partes la cuestión de la autenticación de los mensajes de datos [...]

Finalmente, y para ahondar más en la relación entre el concepto de autenticidad y firma electrónica, el apartado 3 de la guía para su incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre firmas electrónicas señala que la finalidad de esta segunda

---

[...]
Código de Comercio, última reforma. *Diario Oficial de la Federación*. 28 de marzo de 2018. Véase: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_311218.pdf
Artículo 1250. En caso de que se niegue o se ponga en duda la autenticidad de un documento, objetándolo o impugnándolo de falso, podrá pedirse el cotejo de letras y/o firmas.
[...]
Artículo 1250 bis**.** En el caso de impugnación y objeción de falsedad de un documento, además de lo dispuesto en el artículo anterior, se observará lo dispuesto en las siguientes reglas:

I. La parte que objete la autenticidad de un documento o lo redarguya de falso, deberá indicar específicamente los motivos y las pruebas;
II. cuando se impugne la autenticidad de un documento privado o público sin matriz deberán señalarse los documentos indubitables para el cotejo, y promover la prueba pericial correspondiente y
III. sin los requisitos anteriores se tendrá por no objetado ni redargüido o impugnado el instrumento;

[...]

111 Davara, M. (2008). *Manual de Derecho Informático.* España. Thomson Aranzadi, p. 451.

112 Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno. Véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf
Artículo 7. — Firma 1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) Si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente. (...)

CNUDMI es cubrir la necesidad de la creación de un marco jurídico específico para reducir la incertidumbre con respecto a las consecuencias jurídicas que pueden derivarse del empleo de técnicas modernas de autenticación electrónica (a las que puede denominarse en general "firmas electrónicas") en sustitución de las manuscritas.[113]

Autodeterminación informativa

Isabel Davara Fernández de Marcos,[114]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El derecho a la autodeterminación informativa es un derecho fundamental que habilita a la persona para decidir, por sí sola, sobre la difusión y utilización de sus datos personales con un fin determinado y con independencia del tipo de soporte (físico o electrónico) en el que se encuentren los datos personales.

La expresión "autodeterminación informativa" tuvo su origen en la sentencia del Tribunal Constitucional alemán del 15 de diciembre de 1983 y hace referencia a un derecho autónomo que se entrelaza con el derecho humano a la protección de datos personales,[115] que se relaciona estrechamente con los de intimidad y privacidad[116] y cuyo objeto es otorgar protección al individuo frente a la obtención, almacenamiento, utilización y transmisión de sus datos personales, al otorgarle la facultad para decidir sobre su difusión y uso con un fin determinado.

Desde una acepción genérica, el término "autodeterminación" significa "determinar por sí mismo", que se puede traducir como la capacidad de decidir por uno mismo, y en relación con el tratamiento de los datos personales esta expresión se vincula con la facultad del titular de los datos para decidir sobre el uso que se da a su información y tener control sobre la misma.

En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) comienza su articulado exponiendo su objeto y señala:

> Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Origen del concepto

La noción de autodeterminación, en sentido general como un derecho inherente al humano, tiene su origen en la ética kantiana. En concreto, deriva del principio moral de autonomía de la voluntad, elaborado en 1785 por Immanuel Kant. Para el filósofo prusiano, la autonomía es "el fundamento de la dignidad de la naturaleza humana y de toda naturaleza racional".[117] Según Kant, el ser humano tiene una naturaleza racional, lo que le permite decidir

113 Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno. Pp. 21 y 22. Véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

114 Agradecemos el inestimable apoyo para la elaboración de este trabajo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez.

115 Sentencia del 15 de diciembre de 1983. (Ref. 1 BvR 209/83). (Fondo) Ley del Censo.

116 Para una pronta referencia de los conceptos "intimidad", "privacidad" y "protección de datos personales" se recomienda consultar las definiciones correspondientes que se contienen en este diccionario.

117 Kant, I. (2007). *Fundamentación de la Metafísica de las Costumbres.* San José, p. 49.

de forma libre por sí mismo, es decir, por su propia voluntad. En este sentido, el referido autor entiende que la autonomía de la voluntad presupone la libertad del individuo, pues sin ésta, el individuo no obraría por su propia voluntad, sino por elementos externos. Así, los seres racionales se distinguen de las cosas que únicamente tienen un valor relativo como medios para un fin, mientras que a los seres racionales se les llama personas "porque su naturaleza los distingue ya como fines en sí mismos, esto es, como algo que no puede ser usado meramente como medio".[118] Así pues, el hombre y todo ser racional existen "como fin en sí mismo" y tienen dignidad,[119] mientras que las cosas son medios y tienen un precio. El valor absoluto de las personas deriva de su naturaleza racional.

En este sentido, también el derecho a la protección de datos personales tiene su fundamento[120] en el respeto a la dignidad e identidad de las personas.[121] Del mismo modo, en nuestro ordenamiento jurídico se considera que la dignidad humana es un valor supremo —establecido en el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM)— en virtud del cual se le reconoce una calidad única y excepcional a todo ser humano por el simple hecho de serlo, cuya plena eficacia debe ser respetada y protegida integralmente sin excepción alguna.[122]

Siguiendo con la exposición anterior, Kant explica que la voluntad de todos los seres racionales es una voluntad universalmente legisladora, que es capaz de someterse a las leyes morales creadas por sí misma. "La voluntad, de esta suerte, no está sometida exclusivamente a la ley, sino que lo está de manera que puede ser considerada como legislándose a sí propia, y por eso mismo, y solo por eso, sometida a la ley (de la que ella misma puede considerarse autora)".[123] Así pues, la autonomía de la voluntad es la base sobre la que se sustenta la moralidad, dado que permite la creación de leyes morales que determinan el contenido de la misma.

Desde su concepción, el derecho a la protección de datos personales (que es muy cercano a la privacidad) recae fuertemente en un reconocimiento de la autodeterminación del individuo.

En el derecho estadounidense, Samuel Warren y Louis Brandeis,[124] en su afamado ensayo *The Right to Privacy*, conceptualizan el derecho a la privacidad como el "derecho a ser dejado solo". Los autores explican que este derecho se basa en el poder del individuo de evitar la publicación de sus pensamientos, sentimientos y emociones. Para Warren y Brandeis, el bien jurídico que este derecho protege lo distingue del derecho de propiedad, ya que ra-

118 Kant, I. (2007). *Fundamentación de la Metafísica de las Costumbres.* San José, p. 42

119 No puede pasar desapercibido que, en términos de nuestro ordenamiento jurídico, la dignidad humana es el origen, la esencia y el fin de todos los derechos humanos. SCJN. (2011, octubre) "Tesis I.5o.C. J/30". En *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo III, p. 1528.

120 Se recomienda ver la definición de derecho a la protección de datos personales en este diccionario.

121 Escalante, G. (2008, octubre). *El derecho a la privacidad*. Cuadernos de Transparencia nº 2. IFAI, Ciudad de México. Referido en Piñar, José Luis. "¿Existe la Privacidad?". En *Protección de Datos Personales: Compendio de lecturas y legislación.* Tiro Corto. Ciudad de México.

122 Dignidad humana. Su naturaleza y concepto. La dignidad humana es un valor supremo establecido en el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos, en virtud del cual se reconoce una calidad única y excepcional a todo ser humano por el simple hecho de serlo, cuya plena eficacia debe ser respetada y protegida integralmente sin excepción alguna. SCJN. (2011, octubre). Tesis I.5o.C. J/31. *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo III, p. 1529.

123 Kant, I. (2007). *Fundamentación de la Metafísica de las Costumbres.* San José, p. 45

124 D. Warren, S. y Louis D. Brandeis. (1980, diciembre 15). "The Right to Privacy*". Harvard Law Review*. Vol. 4. No. 5. Estados Unidos, pp. 193-220. Disponible en: http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%-3C193%3ATRTP%3E2.0.CO%3B2- Fecha de consulta: 16 de octubre de 2018.

dica en "la tranquilidad del espíritu y en el alivio que proporciona el poder de impedir [la publicación de sus pensamientos, sentimientos y emociones]".[125] Ese reconocimiento al poder de decisión no es otra cosa más que un reconocimiento a la voluntad del individuo, su poder de determinar por sí solo si se publican o no sus ideas.

Sin embargo, Warren y Brandeis limitan el alcance del derecho de privacidad al momento de la publicación de los "pensamientos, sentimientos y emociones". Será hasta después, con el desarrollo de la autodeterminación informativa que se pasará a concebir en un sentido mucho más amplio el alcance del poder que tienen los titulares sobre su información personal.[126] Esta noción deriva de la conceptualización de privacidad de Alan Westin, desarrollada en su libro *Privacy and Freedom* (1967) como la facultad de "determinar por sí mismo cuándo, cómo y hasta qué punto su información personal se comunica a otros".[127] Westin concibe así a la privacidad como un derecho que permite al individuo decidir qué, cómo, a quién y cuándo la información personal se comunica, pero donde el control sobre la propia información permanece tras la publicación.[128]

El concepto "autodeterminación informativa" como lo conocemos ahora fue presentado por primera vez, como ya señalábamos, por el Tribunal Constitucional de la República Federal de Alemania el 15 de septiembre de 1983 en una sentencia sobre la Ley del Censo.[129] En términos de la sentencia, la autodeterminación informativa garantiza "… la capacidad de los individuos para determinar, en principio, la divulgación y empleo de sus datos personales" y únicamente pueden establecerse límites al derecho con base en interés general y con un fundamento legal y constitucional.[130] La sentencia deduce el derecho a la autodeterminación informativa del derecho general a la personalidad protegido por su Ley Fundamental "…es facultad del individuo, derivada de la idea de autodeterminación de decidir básicamente por sí mismo cuándo y dentro de qué limites procede a revelar situaciones referentes a su propia vida".[131] Dicha sentencia sería el germen de lo que en Europa se conocería como derecho a la autodeterminación informativa y de forma posterior en la legislación de diversos Estados en Latinoamérica, como es el caso de México, que lo reconoce expresamente en el artículo 1 de la LFPDPPP como hemos visto.

125 D. Warren, S. y Louis D. Brandeis. (1980, diciembre 15). "The Right to Privacy". *Harvard Law Review*. Vol. 4. No. 5. Estados Unidos, pp. 193-220. Disponible en: http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%-3C193%3ATRTP%3E2.0.CO%3B2- Fecha de consulta: 16 de octubre de 2018.

126 Por ejemplo, en relación con este derecho, autores como Diego García Ricci consideran que el derecho a la autodeterminación informativa es el segundo de dos componentes que forman el derecho a la privacidad, donde el primer componente refiere al derecho de excluir a terceros de lo privado y el segundo es la autodeterminación informativa entendida como el control sobre la información privada. Aunque esta categorización puede servir doctrinalmente, en los sistemas jurídicos la autodeterminación informativa ha sido concebida como un derecho autónomo e independiente de otros. *Vid*. García, D. (2013). "Artículo 16 Constitucional. Derecho a la Privacidad". En *Derechos Humanos en la Constitución, Comentarios de Justicia Constitucional e Interamericana*. México. Suprema Corte de Justicia de la Nación-Instituto de Investigaciones Jurídicas y Fundación Konrad Adenauer Stiftung, p. 1047.

127 Westin, A. (1967). *Privacy and Freedom*. Estados Unidos. IAPP, p. 7.

128 Piñar, J. (2010). "¿Existe la Privacidad?". En *Protección de Datos Personales: Compendio de lecturas y legislación*. Tiro Corto. Ciudad de México. 2010.

129 Westin, A. (1967). *Privacy and Freedom*. Estados Unidos. IAPP.

130 Tribunal Constitucional Federal Alemán. (2009). "Sentencia BVerfGE 65,1 [Censo de Población]". En *Cincuenta años de jurisprudencia del Tribunal Constitucional Federal*. Jürgen Schwabe (compilador) y Marcela Anzola (traducción), p. 94.

131 Daranas, D. (traductor). (1984, enero). "Sentencia de 15 de diciembre de: Ley del Censo. Derecho de la personalidad y dignidad humana". *Boletin de Jurisprudencia Constitucional*. Madrid. Dirección de Estudios y Documentación del Congreso de los Diputados. Tomo IV, núm. 3, p. 152.

Naturaleza jurídica

La autodeterminación informativa es un reconocimiento a la libre autonomía de la persona para controlar lo que ocurre con su información personal. Por control no se refiere únicamente a la publicación o revelación de la misma, sino a un poder de decisión que va más allá, una vez que la información está fuera de su poder. Es decir, se trata de un derecho que establece la voluntad de la persona como una base jurídica para el tratamiento de datos personales. Por ello, inicialmente el Tribunal Constitucional alemán lo derivó del derecho a la personalidad, dado que el control de la información personal es una prerrogativa necesaria para el desarrollo del individuo.

De acuerdo con el tribunal germano, el derecho fundamental a la autodeterminación informativa garantizaba, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales.[132]

El auge de la sociedad y las tecnologías de la información y la comunicación (TIC), desde finales del siglo XX, ha reforzado la necesidad de dotar al individuo de la facultad de control sobre su propia información. Sin embargo, el acelerado uso de las TIC también puede colocar a la persona en una situación de vulnerabilidad donde se vuelve más difícil —e incluso hoy en día materialmente imposible— que el titular pueda controlar el uso que se hace de su información personal, sobre todo en el entorno electrónico. Es por ello que, en la actualidad, el derecho a la autodeterminación informativa requiere de la ayuda de otros factores y en especial como responsabilidad proactiva y de la ética de todos los que intervienen en el tratamiento, para la consecución final de su objetivo, que es el lícito tratamiento de la información personal.

Así, en nuestros días, adquiere relevancia el razonamiento del Tribunal Constitucional Federal alemán cuando señaló que la proliferación de centros de datos había hecho posible, gracias a los avances tecnológicos, producir "una imagen total y pormenorizada de la persona respectiva —un perfil de la personalidad— incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en *hombre de cristal*. Es decir, la preocupación que el Tribunal señaló subsiste hasta nuestros días pero con mayores dimensiones, pues ahora las personas se encuentran cada vez más expuestas a intensivos tratamientos de datos personales y gozan de menos control frente a una identidad digitalmente construida.

132 En relación con este tema, señala la sentencia del 15 de diciembre de 1983 (Ref. 1 BvR 209/83) (Fondo) Ley del Censo: "Ahora bien, la autodeterminación del individuo presupone —también en las condiciones de las técnicas modernas de tratamiento de la información— que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en caso, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada. El que no pueda percibir con seguridad suficiente que informaciones relativas a él son conocidas en determinados sectores de su entorno social y quien de alguna manera no sea capaz de aquilatar lo que puedan saber de sus posibles comunicantes, puede verse substancialmente cohibido en su libertad de planificar o decidir por autodeterminación. No serian compatibles, con el derecho a la autodeterminación informativa, un orden social y jurídico que hiciese posible al primero, en el ciudadano ya no pudiera saber quién, qué, cuándo y con qué motivo sabe algo sobre él. Quien se siente inseguro de sí en todo momento se registran cualesquiera comportamientos divergentes y se catalogan, utilizan o transmiten permanentemente a título de información procurara no llamar la atención con esa clase de comportamiento. Quien sepa de antemano que su participación, por ejemplo, en una reunión o en una iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para el por este motivo renunciara presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales [artículo 8° y 9° de la Ley Fundamental (17). Esto no solo menoscabaría las oportunidades de desarrollo de la personalidad individual, sino también el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos.
De lo que antecede se deduce lo siguiente: la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión limitada de los datos concernientes a la persona. Esa protección cae, por lo tanto, dentro del ámbito del derecho fundamental del artículo 2°, párrafo 1, en relación con el artículo 1°, párrafo 1, de la Ley Fundamental. El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales".

Ante estos nuevos retos, y reconociendo la importancia de proteger los datos personales de los titulares para salvaguardar la dignidad de las personas, el debate en la materia ha cuestionado el planteamiento actual de las diferentes legislaciones y si los principios en protección de datos serán suficientes para garantizar adecuadamente la integridad de la persona. En este sentido, el supervisor europeo de protección de datos ha reconocido que urge considerar la ética y la posición de la dignidad humana en las tecnologías del futuro y evaluar si las tendencias actuales requerirán de un nuevo enfoque.[133]

1. Relación del derecho a la autodeterminación informativa y el derecho a la protección de datos personales

La relación entre el derecho a la autodeterminación informativa y el derecho a la protección de datos personales es estrecha, pues resulta imposible entender uno en ausencia del otro.

Por un lado, el enfoque del derecho a la autodeterminación informativa entiende a la voluntad del titular como a la adecuada para determinar y controlar la divulgación y el uso de los datos personales como el bien jurídico protegido. En este sentido, la voluntad —expresada mediante el consentimiento— es el sustento preponderante para legitimar los tratamientos de datos personales y cualquier otra base de legitimación al tratamiento es meramente una excepción.[134]

La protección de datos personales, en cambio, aporta los medios legales necesarios para garantizar la autodeterminación informativa a través del reconocimiento de derechos específicos para los titulares, como son los llamados derechos ARCO.[135] Así, el derecho a la *protección de datos personales* reconoce que el bien jurídico protegido no se restringe a la voluntad del titular. Este entendimiento es el que le ha permitido evolucionar de mejor manera para adaptarse, de forma más congruente, a la realidad de los nuevos tratamientos, por ejemplo, en el reconocimiento de que existen varias bases para legitimar el tratamiento de datos personales con la misma jerarquía que el consentimiento del titular —como, por ejemplo, puede serlo el cumplimiento de un contrato, el interés legítimo del responsable o la salud pública. Este enfoque también ha permitido que se reconozca la necesidad de poner límites a ciertos tratamientos de datos personales, incluso cuando hubiere consentimiento por parte del titular, además de que ha trasladado obligaciones a los responsables y encargados del tratamiento.

En este sentido, el derecho a la autodeterminación informativa queda subsumido dentro del derecho de protección de datos personales como la faceta que reconoce el papel del titular y su poder de decisión en el tratamiento, manifestándose concretamente en el ejercicio de los derechos ARCO.[136]

133 Supervisor Europeo de Protección de Datos. (2015, septiembre 11). *Dictamen 4/2015. Hacia una nueva ética digital: Datos, dignidad y tecnología.*

134 Por eso, como venimos diciendo, si bien el derecho a la autodeterminación informativa sigue siendo un sustento esencial, lo cierto es que en la actualidad existen un gran número de tratamiento de datos, realizados mediante tecnologías avanzadas que no permiten establecer al consentimiento como la única columna vertebral de la protección de datos personales y que se dirigen al establecimiento de otras bases de legitimación en igualdad de condiciones.

135 Derechos de acceso, rectificación, cancelación y oposición. En la esquela pública, además, se perfila el derecho de portabilidad.

136 Ver definición de “derechos ARCO” en este diccionario.

2. Reconocimiento constitucional y legal

El derecho a la autodeterminación informativa se incluye en la descripción que realiza el segundo párrafo del artículo 16 constitucional sobre el reconocimiento del derecho a la protección de los datos personales y los denominados derechos ARCO a favor de cualquier persona:

> [...]
>
> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.
>
> [...] (Énfasis añadido).

Con base en lo anterior, se entiende que el texto constitucional reconoce a cada persona la facultad de decidir de manera libre e informada sobre el uso y destino de sus datos personales.[137]

Como mencionábamos al iniciar este escrito, la LFPDPPP prevé el derecho el derecho a la autodeterminación informativa en su artículo 1, que implica el reconocimiento específico del derecho a la autodeterminación de las personas y de las prerrogativas legales que de él se desprenden y concretan en dicha Ley y su normatividad de desarrollo.

En definitiva, se puede afirmar que el derecho de autodeterminación informativa persigue que la protección de la identidad del individuo (persona física) sea realmente efectiva en un momento en que la tecnología permite que la información viaje sin restricciones y cuya recopilación masiva pone en riesgo el libre desarrollo de la personalidad atacando los resortes de los derechos humanos que están basados en el respeto a la dignidad humana.[138]

Autoridad de control

Isabel Davara Fernández de Marcos,[139]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La autoridad de control es el órgano público de carácter unipersonal o pluripersonal autónomo que, de forma imparcial e independiente, ejerce sus potestades y funciones para supervisar el cumplimiento de la normatividad de protección de datos personales con el fin de proteger los derechos y libertades fundamentales de las personas sobre el tratamiento de sus datos personales.

137 Ver definición de "protección de datos personales" en este diccionario.

138 La dignidad humana funge como "un principio jurídico que permea en todo el ordenamiento, pero también como un derecho fundamental que debe ser respetado en todo caso, cuya importancia resalta al ser la base y condición para el disfrute de los demás derechos y el desarrollo integral de la personalidad. Así las cosas, la dignidad humana no es una simple declaración ética, sino que se trata de una norma jurídica que consagra un derecho fundamental a favor de la persona y por el cual se establece el mandato constitucional a todas las autoridades, e incluso particulares, de respetar y proteger la dignidad de todo individuo, entendida ésta —en su núcleo más esencial— como el interés inherente a toda persona, por el mero hecho de serlo, a ser tratada como tal y no como un objeto, a no ser humillada, degradada, envilecida o cosificada". *Vid*, SCJN. (2014, octubre). Tesis 1a. CCCLIV/2014. *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo I, p. 602.

139 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

El término de autoridad de control es empleado de forma específica en el panorama internacional para referirse a las instancias nacionales —del ámbito federal y/o local— encargadas de vigilar el cumplimiento de las normas domésticas de protección de datos personales y resguardar el derecho a la protección de los datos personales. De forma concreta, es en los Estándares Internacionales de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) y el Reglamento General de Protección de Datos Personales (RGPD) donde se refiere este término y se delimitan sus alcances.

En el ámbito nacional, la normatividad de datos personales no hace uso de este término, pero se refiere de forma genérica a las autoridades garantes de la protección de datos personales del orden federal y local que conocen sobre la aplicación de la normatividad de datos personales en los sectores público y privado, como se explica a continuación:

a) Autoridad garante federal (INAI): El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) se erige como la autoridad garante del orden federal, encargada de supervisar el cumplimiento de la normatividad de datos personales en el orden público (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y privado (Ley Federal de Protección de Datos Personales en Posesión de los Particulares LFPDPPP).[140]
b) Órganos garantes locales: se constituyen como entidades autónomas que supervisan la correcta aplicación de las distintas legislaciones locales en materia de protección de datos personales para el sector público. Estas autoridades garantes corresponden a cada una de las entidades federativas que integran la República mexicana.[141]

Con base en lo anterior, se puede precisar que en México existen dos tipos de autoridades de control identificadas con los dos ámbitos principales de aplicación de la normatividad. Es decir, la autoridad de control federal que conoce sobre la aplicación de la legislación del sector privado, y del sector público en el orden federal, y en el otro extremo, las autoridades de control locales a las que corresponde la aplicación de la normatividad de datos personales para las entidades de las administraciones públicas locales.

1. Características

Como se desprende de la definición presentada, las autoridades de control, en primer lugar, son instituciones adscritas al Estado y que tienen la naturaleza de una entidad de derecho público. En segundo orden debe destacarse que éstas se caracterizan también por ser autónomas, es decir, aunque tengan la naturaleza de derecho público, tienen plena independencia para desarrollar sus funciones y emitir sus fallos. Lo anterior responde precisamente a la importante labor que desempeñan para la efectiva tutela del derecho fundamental de protección de datos personales en cada Estado.

Otra característica que vale la pena señalar es que estas autoridades deben ser imparciales, tanto en su actuar como en la emisión de sus fallos. Lo anterior implica que las autoridades de control no están sujetas a ningún designio o prevención a favor de persona o entidad alguna, lo que permite que resuelvan con rectitud los asuntos que se someten a su consideración o que resultan de su competencia.

140 Recomendamos la lectura de la definición de "Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales" en este diccionario.

141 En relación con este tema recomendamos revisar la definición de "organismos garantes locales" que forma parte de este diccionario.

Los Estándares Iberoamericanos, en su artículo 42, al establecer la obligación de que los Estados Iberoamericanos cuenten con una o más autoridades de control, indican, asimismo, las siguientes características:

- Gozan de plena autonomía de conformidad con la legislación nacional aplicable.
- Pueden integrarse en forma de órganos unipersonales o pluripersonales.
- Tienen el deber de actuar imparcial e independiente en sus potestades, siendo ajenas a toda influencia externa, ya sea directa o indirecta, y sin solicitar o admitir orden ni instrucción alguna.
- Deben otorgárseles, de parte de la legislación nacional, suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de la normatividad, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.
- Sus decisiones únicamente deben estar sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional aplicable.
- Deben contar con los recursos humanos y materiales necesarios para el cumplimiento de sus funciones.

Por otro lado, el RGPD, en su artículo 51, obliga a los Estados miembros de la Unión Europea (UE) a establecer una o varias autoridades de control, encargadas de supervisar la aplicación del RGPD y señala, en su artículo 52, que éstas habrán de ser independientes, para lo que deberá cumplirse con lo siguiente:

- Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes.
- El miembro o los miembros de cada autoridad de control serán ajenos —en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el RGPD— a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.
- El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán —mientras dure su mandato— en ninguna actividad profesional que sea incompatible (remunerada o no).
- Cada Estado miembro garantizará que cada autoridad de control disponga, en todo momento, de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité Europeo de Protección de Datos.
- Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.
- Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual (público e independiente) que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Finalmente, debe mencionarse también que una característica importante de las autoridades de control es que, derivado de su independencia, los fallos que éstas emiten son vinculantes y están sujetas al control jurisdiccional.[142]

142 En este sentido los Estándares Iberoamericanos señalan: "42.5. Las decisiones de las autoridades de control únicamente

2. Potestades y funciones

Las autoridades de control, con la finalidad de hacer cumplir y vigilar la observancia de la normatividad de datos personales, deben tener robustas potestades y gozar de un amplio catálogo de funciones.

En el ámbito nacional las potestades y funciones de las autoridades de control del orden público y privado se regulan en la legislación particular de cada sector de actividad:

a) Sector privado: Las potestades de la autoridad de control federal en el orden privado se regulan en los artículos 38 y 39 de la LFPDPPP.

b) Sector público: Las potestades de la autoridad de control federal en el orden público se regulan en los artículos 88 y 89 de la LGPDPPSO. Mientras que las atribuciones de los órganos de control locales se prevén en los artículos 90 y 91 de la LGPDPPSO, así como en las distintas leyes locales vigentes en cada una de las entidades federativas del país.

En relación con lo anterior, el artículo 42.4 de los Estándares Iberoamericanos indica que la normatividad nacional deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de la normatividad, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

Por su parte, el RGPD confiere a las autoridades de control tres tipos de poderes, los de investigación (apartado 1 del artículo 58), los correctivos (apartado 2 del artículo 58) y los de autorización y consultivos (apartado 3 del artículo 58). Del mismo modo, el artículo 57 del RGPD establece un catálogo de funciones bastante amplio que incluye todas las acciones necesarias para hacer cumplir el RGPD.

De acuerdo con lo anterior, se puede constatar que el término autoridad de control se refiere a las entidades autónomas responsables de vigilar el cumplimiento de la normatividad de datos personales en el orden federal, público y privado, así como en el orden local público.

Autoridades coadyuvantes

María Marván Laborde

El entramado institucional que ha desarrollado el Estado mexicano para garantizar el derecho a la protección de datos personales es complejo y difícil de entender, ya que existen varias autoridades que forman parte de dicho entramado sin que la relación entre estos sea necesariamente jerárquica.

A pesar de la diversidad de autoridades, desde 2002 hasta la fecha, el corazón de la autoridad ha estado en el órgano garante de la transparencia, el acceso a la información y la protección de los datos personales. Si atendemos a una explicación cronológica, encontramos ocho momentos de creación legislativa.

1) En 2002 se aprueba la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG). El Pleno del Instituto Federal de Acceso a la Información (IFAI) es la autoridad que debe resolver sobre los recursos de revisión interpuestos por las personas que habiendo hecho solicitudes de acceso a sus datos personales no hubiesen recibido una respuesta satisfactoria.

estarán sujetas al control jurisdiccional, conforme a los mecanismos establecidos en la legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia y su derecho interno".

2) En 2007 se reforma el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) y ahí se establecen las características del IFAI y la autoridad que tiene para resolver asuntos relativos a la protección de datos personales.
3) El 1 de junio de 2009 se modifica nuevamente la CPEUM, ahora en su artículo 16 al que se le adiciona el siguiente párrafo: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".
4) Un año más tarde, el 5 de julio de 2010, se expide la Ley Federal de Protección de Datos Personales en Posesión de Privados (LFPDPPP), en ella se establece claramente en el Capítulo VI, llamado "De las Autoridades", la sección I se dedica al IFAI que por virtud de esta ley cambia su nombre para convertirse en el Instituto Federal de Acceso a la Información Pública y Protección de Datos Personales. Su acrónimo no cambió. En la sección II de este mismo capítulo, llamado "De las Autoridades Reguladoras" se establece que la Secretaría de Economía tiene la responsabilidad de coadyuvar al IFAI.
5) La reforma constitucional del 7 de febrero de 2014 le otorga autonomía constitucional al IFAI y confirma en el artículo 6 que esta es la institución encargada de garantizar tanto la transparencia y el acceso a la información pública como la protección de los datos personales. En esta reforma se crea el Consejo Consultivo que también tendrá competencias en materia de acceso a la información y protección de datos personales. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley. El organismo garante tendrá un consejo consultivo, integrado por 10 consejeros, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.
6) El 4 de mayo de 2015 se expidió la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) que añade una nueva autoridad en materia de protección de datos personales al crear el Sistema Nacional de Transparencia (que carece de fundamento constitucional) y de ahí se desprende el Consejo Nacional de Transparencia. La LGTAIP reconoce como autoridades en la materia a los 33 órganos garantes, el organismo federal y los 32 de cada una de las entidades y al consejo consultivo ya mencionado.
7) Al expedirse la Ley Federal de Acceso a la Información Pública, el 9 de mayo de 2016, se deroga la LFTAIPG de 2002. Esta ley reconoce que en el ámbito federal la autoridad máxima es órgano garante,[143] pero cuando se refiere a las autoridades habla específicamente del Instituto Nacional de Transparencia, Acceso a la Información y

143 De acuerdo con la LGTAIP esta es la definición de organismos garantes: "Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales en términos de los artículos 6, 116, fracción VIII y 122, apartado C, BASE PRIMERA, Fracción V, inciso ñ de la Constitución Política de los Estados Unidos Mexicanos".

Protección de Datos Personales (INAI) cuya máxima autoridad es el Pleno. Esta ley le asigna nueve facultades. Además, reconoce al consejo consultivo establecido por la LGTAIPG al que le asigna 12 atribuciones.

8) Por último, pero no por ello menos importante, el 26 de enero de 2017 se expidió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), entendiendo por sujetos obligados los mismos que establece el artículo 6 de la CPEUM y la LGTAIP, es decir todo el sector público. En esta ley se reconocen como autoridades al SNT, a los órganos garantes y al consejo consultivo ya mencionados en la LGTAIP.

1. Facultades de las autoridades coadyuvantes

Las autoridades en las que recaen las principales obligaciones para garantizar el derecho a la protección de datos personales y, por supuesto la transparencia y el derecho de acceso a la información pública, son los órganos garantes que por mandato constitucional deben ser órganos constitucionales autónomos tanto en la Federación como en las entidades. (artículos 6 y 116 constitucional).

Las principales funciones de los órganos garantes se pueden encontrar en la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) en su artículo 41. En este artículo se establecen nueve facultades —todas ellas encaminadas a la capacidad de garantizar plenamente ambos derechos— para ello se le otorga al Pleno la facultad de resolver los recursos de revisión que surgen de la inconformidad de los ciudadanos que han hecho valer sus derechos frente a los sujetos obligados y han recibido una respuesta insatisfactoria.

Los 33 órganos garantes son los responsables de diseñar las políticas públicas tanto de protección de datos personales en posesión de entes privados y públicos, como en materia de transparencia y acceso a la información, también deberán capacitar a los ciudadanos en el ejercicio de estos derechos y a los servidores públicos y entes privados para la implementación plena y satisfactoria de los cuatro ordenamientos legales de la materia.

El principal propósito de la LGTAIP es garantizar que todos los ciudadanos, sin importar la entidad en la que vivan, gocen de los mismos derechos y también que todos los sujetos obligados tengan los mismos parámetros de exigencia sin tomar en cuenta si estamos hablando del ámbito federal, local o municipal. Por ello son especialmente importantes las facultades y atribuciones que esta ley les confiere a los órganos garantes: son institutos poderosos que frente a los sujetos obligados gubernamentales tienen la última palabra.

El Sistema Nacional de Transparencia (SNT) es, fundamentalmente, un organismo de coordinación entre todos los órganos garantes que pone a la cabeza del mismo al INAI. Para lograr una implementación exitosa de un aparato normativo tan ambicioso contará con la participación de la entidad de fiscalización superior de la Federación (Auditoría Superior de la Federación), con el organismo encargado de regular la captación, procesamiento y publicación estadística y geográfica (INEGI) y con el Archivo General de la Nación.

De acuerdo con el artículo 28 de la LGTAIP el SNT tiene el "objeto de fortalecer la rendición de cuentas del Estado mexicano". Para lograrlo deberá coordinar y evaluar las acciones relativas a la política transversal de transparencia, acceso a la información y protección de datos personales, así como establecer e implementar los criterios y lineamientos necesarios para que se puedan alcanzar sus objetivos.

Cada órgano garante deberá tener un consejo consultivo integrado por consejeros honoríficos que durarán en su encargo un máximo de siete años y deberán acceder al cargo de manera escalonada. Es función de estos consejos emitir opiniones sobre el quehacer del Instituto y la interpretación que hacen de las leyes de transparencia y de protección de datos personales. También, emiten opiniones sobre su programa anual de trabajo, el proyecto de presupuesto y proponen programas de trabajo que faciliten el ejercicio de ambos derechos. En ningún caso sus opiniones tendrán el carácter de vinculantes.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP artículos 40 a 44) agrega como autoridad reguladora a la Secretaría de Economía (SE) y le otorga las siguientes atribuciones: difundir el conocimiento en materia de protección de datos en el ámbito comercial, fomentar buenas prácticas, emitir lineamientos y disposiciones administrativas de carácter general, fijar parámetros para medidas de autorregulación, propiciar la adopción de códigos deontológicos o de buenas prácticas y fomentar estudios que ayuden al mejor ejercicio del derecho de la protección de los datos personales en posesión de particulares.

La adopción del modelo regulatorio presente en nuestro país implica la existencia de autoridades reguladoras, pues dada la especialización en temas como comercio, comunicaciones y transportes o salud, la Comisión de Gobernación de la LX Legislatura que emitió el dictamen de proyecto por el que se expidió la LFPDPPP y consideró pertinente dotar a las secretarías de Estado del ramo específico la potestad de emitir lineamientos, recomendaciones y criterios que permitan la adecuada observancia de los principios y derechos que rigen en materia de protección de datos. En este tenor, el artículo 40 de la LFPDPPP indica que ésta última constituye el marco normativo que las dependencias deben observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del INAI.

Una autoridad reguladora como la SE únicamente tiene atribuciones de carácter complementario relacionadas con la emisión de disposiciones complementarias a las de la LFPDPPP, el desarrollo de esquemas de mejores prácticas en la materia y el fortalecimiento de la cultura de la protección de datos personales en el orden comercial, sin que esté habilitada para conocer aspectos relacionados directamente con el cumplimiento de la Ley, como son los procedimientos de la materia que por su naturaleza son de exclusiva sustanciación ante el Instituto.

También se consideran autoridades coadyuvantes a las unidades y comités de transparencia que deben establecerse en todos y cada uno de los sujetos obligados del sector público. Su descripción y funciones podrán consultarse en esta misma obra en la entrada correspondiente.

Autorregulación

Rosa María Franco Velázquez

Etimológicamente "autorregulación" proviene del latín *aut(o)-autos*, que actúa por sí mismo o sobre sí mismo y del latín regula (inglés *rule*, francés *regle*, italiano *regola*) "regla", y *-á – tión(em)* latín "proceso de", y se refiere a la capacidad que tiene un sujeto o una institución, organización o asociación, de regularse a sí misma bajo controles voluntarios. Se constituye como la potestad de establecer reglas por parte de cada sujeto dentro de su esfera de acción, estableciendo, de manera voluntaria,[144] normas deontológicas y códigos de autocontrol.[145]

144 Los Estándares de Protección de Datos Personales dedican su artículo 40 a los mecanismos de autorregulación en el que, en lo fundamental, indica que: "El responsable podrá adherirse, de manera voluntaria, a esquemas de autorregulación vinculante, que tengan por objeto, entre otros, contribuir a la correcta aplicación de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia y establecer procedimientos de resolución de conflictos entre el responsable y el titular".

145 Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI. Quinta entrega. Disponible en: https://prosoft.economia.gob.mx/Imagenes/imagenesMaster/Estudios%20Prosoft/FREF_04.pdf

De acuerdo con los parámetros de autorregulación vinculante,[146] ésta es una actividad a través de la cual el responsable (entendido como aquella persona que decide sobre el tratamiento de datos personales) o el encargado (quien de manera individual o, conjuntamente con otras, trata datos personales por cuenta del responsable) se comprometen de manera voluntaria a protegerlos.[147]

En el caso mexicano,[148] la autorregulación no resulta de la ausencia de reglas que regulen la protección de datos personales, sino que ésta debe complementar los mínimos que se encuentran establecidos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),[149] en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[150] y demás normatividad que resulte aplicable en el caso del sector privado. Por lo que se refiere al sector público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) incluye entre las mejores prácticas la relativa a adoptar esquemas de mejores prácticas que son de autorregulación.[151]

Es importante destacar que la adhesión a un esquema de autorregulación es de carácter voluntario, pero una vez que un responsable o encargado decide adherirse al mismo, el esquema se vuelve vinculante para ellos.[152] Los parámetros de autorregulación vinculante definen un esquema de autorregulación vinculante "como el conjunto de principios, normas y procedimientos de adopción voluntaria y cumplimiento vinculante, que tiene como finalidad regular el comportamiento de los responsables y encargados respecto a los tratamientos de datos personales que lleven a cabo". [153]

Cuando un responsable o encargado adopte y cumpla un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda en caso de verificarse algún incumplimiento a lo dispuesto por la LFPDPPP y el RLFPDPPP.[154]

Los esquemas de autorregulación se pueden traducir en:

- códigos deontológicos o de buena práctica profesional
- sellos de confianza
- políticas de privacidad

146 Parámetros de Autorregulación en Materia de Protección de Datos Personales. *Diario Oficial de la Federación*. 29 de mayo de 2014. (Los Parámetros).

147 Considerandos de los Parámetros.

148 En el Derecho comparado puede atenderse en particular el Reglamento General de Protección de Datos en la Unión Europea que impulsa, tanto los códigos de conducta (artículos 40 y 41) como la certificación (artículos 42 y 43) que se aprueben conforme al procedimiento previsto en el mismo. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la directiva 95/46/CE (Reglamento General de Protección de Datos). (Texto pertinente a efectos del EEE).

149 Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. 5 de julio de 2010. (La Ley)

150 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. 21 de diciembre de 2011. (El Reglamento).

151 Artículos 72 y 73 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

152 Artículo 80 de la Ley.

153 Numeral 4, fracción IV, de los Parámetros.

154 Artículo 81 de la Ley.

- reglas de privacidad corporativas y
- otros mecanismos

En todo caso, deberán contener reglas o estándares específicos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas cuando exista un incumplimiento[155] y permitir armonizar los tratamientos de datos efectuados por los adheridos, así como facilitar el ejercicio de los derechos de los titulares.

Podemos resumir los principales objetivos de los esquemas de autorregulación en los siguientes:[156]

I. Coadyuvar al cumplimiento del principio de responsabilidad […];
II. Establecer procesos y prácticas cualitativos […]que complementen lo dispuesto en la Ley;
III. Fomentar que los responsables establezcan políticas, procesos y buenas prácticas para el cumplimiento de los principios de protección de datos personales, garantizando la privacidad y confidencialidad de la información personal […];
IV. Promover que los responsables […] cuenten con constancias o certificaciones sobre el cumplimiento de lo establecido en la Ley, y mostrar a los titulares su compromiso con la protección de datos personales;
V. Identificar a los responsables que cuenten con políticas de privacidad alineadas al cumplimiento de los principios y derechos previstos en la Ley, así como de competencia laboral para el debido cumplimiento de sus obligaciones en la materia;
VI. Facilitar la coordinación entre los distintos esquemas de autorregulación reconocidos internacionalmente;
VII. Facilitar las transferencias con responsables que cuenten con esquemas de autorregulación como puerto seguro;
VIII. Promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de privacidad, incluyendo herramientas, transparencia, supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación, y
IX. Encauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.

Los esquemas de autorregulación deberán ser notificados de manera simultánea a las autoridades sectoriales y al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), a fin de demostrar el cumplimiento de las obligaciones previstas en la normativa.[157] Aquellos esquemas de autorregulación notificados al INAI formarán parte del Registro de Esquemas de Autorregulación Vinculante (REA), que será administrado por el INAI. En el REA se incluirán los esquemas de autorregulación que cumplan con los requisitos que establecen los Parámetros de Autorregulación Vinculante.

De acuerdo con los Parámetros de Autorregulación Vinculante, la autorregulación en materia de protección de datos personales puede ser de tres clases:[158]

155 Artículo 44 de la Ley.

156 Artículo 80 del Reglamento.

157 Artículo 44 de la Ley y 79 y 80 del Reglamento.

158 Numeral 9 de los Parámetros.

A. Las reglas emitidas con objeto de adaptar la normativa aplicable en materia de protección de datos personales a la realidad y actividades de un sector específico.
B. Los esquemas con validación. Aquellos que el INAI valida cuando satisfagan los requisitos previstos para ello.
C. Los esquemas con certificación reconocida. Aquellos que son certificados por un organismo de certificación en materia de protección de datos personales y reconocidos por el INAI a través de su inscripción en el REA.

De conformidad con el RLFPDPPP, los esquemas de autorregulación que se desarrollen deberán contener como mínimo:[159]

I. El tipo de esquema convenido […];
II. Ámbito de aplicación de los esquemas de autorregulación;
III. Procedimientos o mecanismos que se emplearán para hacer eficaz la protección de datos personales […], así como para medir la eficacia;
IV. Sistemas de supervisión y vigilancia internos y externos;
V. Programas de capacitación para quienes traten los datos personales;
VI. Mecanismos para facilitar los derechos de los titulares de los datos personales;
VII. Identificación de las personas físicas o morales adheridas, que posibilite reconocer a los responsables que satisfacen los requisitos exigidos por determinado esquema de autorregulación y que se encuentran comprometidos con la protección de los datos personales que poseen, y
VIII. Medidas correctivas eficaces en caso de incumplimiento.

Para que un esquema sea validado por el INAI o cuente con una certificación reconocida por el INAI deberá al menos: i) señalar su denominación, ii) el nombre completo, denominación o razón social de los responsables o encargados adheridos, iii) el sector o actividad a la que se aplica, iv) su alcance, v) el ámbito personal de aplicación, es decir, el tipo de titulares a los que se aplica el tratamiento, vi) desarrollar e implementar un sistema de gestión de datos personales (SGDP), vii) documentarse en español y viii) proporcionar datos de contacto o un medio para que los interesados conozcan más acerca del esquema.

En concreto, la autorregulación vinculante consiste en la adopción de mecanismos de adhesión voluntaria —pero que una vez adoptados se vuelven obligatorios— que permiten a los responsables y encargados complementar la legislación en materia de protección de datos personales, armonizar el tratamiento de datos llevado a cabo por los adheridos y facilitar el ejercicio de los derechos de los titulares, así como las transferencias de datos personales y la resolución de conflictos entre titulares y responsables del tratamiento. Toda vez que contienen reglas o estándares para medir la eficacia en la protección de los datos, así como consecuencias y medidas correctivas cuando exista un incumplimiento, ya que sirven para garantizar el principio de responsabilidad y promueven la confianza por parte de los titulares en los responsables y encargados que se encuentren adheridos al mecanismo.

Aviso de privacidad

Jorge Antonio Orta Villar

La privacidad es un derecho fundamental que encuentra cobijo en diversos sistemas jurídicos democráticos. Su conceptualización tiene como fundamento la intimidad y su

159 Artículo 82 del Reglamento.

referente normativo más ejemplificativo se localiza en la Declaración Universal de los Derechos Humanos (DUDH). Varios países latinoamericanos se han sumado a una tendencia internacional por incorporar el derecho a la protección de datos personales en sus ordenamientos constitucionales y el desarrollo de normativa especial en esta materia. Este fervor legislativo de la actualidad es, finalmente, un estallido de la conciencia colectiva por preservar la individualidad a través de la defensa de los derechos a la identidad, la dignidad y la libertad.[160]

En 1948, la Asamblea General de las Naciones Unidas adoptó el documento conocido como "Declaración Universal de Derechos Humanos" en el cual se encuentra la base de la ideología jurídica de la protección de datos personales. El artículo 12 de este documento señala lo siguiente: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques…".[161]

1. Introducción

Nuestro sistema jurídico ha vivido en los últimos 20 años una modernización importante que va desde la reconceptualización de instituciones jurídicas hasta el establecimiento de principios legales fundamentales.

En materia de protección de datos se dieron cambios constitucionales que permitieron identificar el derecho a la privacidad, más que como un derecho humano, como un derecho fundamental. Es así, que dentro del artículo 16 de la carta magna "se reconoce que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos…".[162]

Del espíritu protector de la privacidad de los mexicanos se desprenden dos pilares preponderantes: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP). La LFPDPPP establece una serie de principios para la protección de datos personales. Estos principios son de obligado cumplimiento para los particulares que los tratan y, en su conjunto, garantizan un adecuado manejo de los mismos, a favor de la privacidad y de la autodeterminación informativa de los titulares. El RLFPDPPP brinda una clarificación de mayor precisión respecto del reconocimiento y desarrollo de los derechos inherentes a los titulares de los datos personales.

Ambas normativas coinciden y convergen en la materialización de un principio de información a través de la puesta a disposición del aviso de privacidad al titular, por lo que es trascendental la comprensión del concepto y sus alcances. Podemos considerarlo como la declaratoria formal de las reglas del juego. Es el mecanismo mediante el cual la persona receptora y poseedora legítima de la información, que será sujeta de protección y resguardo, informa al propietario sobre los términos bajo los cuales serán tratados sus datos personales.

El aviso de privacidad[163] es el mecanismo de comprobación de que el titular tuvo la posibilidad de discernir y que lo hizo de manera libre e informada sobre el tratamiento de sus datos personales.

160 ONU: Asamblea General, Declaración Universal de Derechos Humanos, 10 diciembre 1948, 217 A (III), disponible en: https://www.refworld.org.es/docid/47a080e32.html

161 Artículo 12, ONU: Asamblea General, Declaración Universal de Derechos Humanos, 10 diciembre 1948, 217 A (III), disponible en: https://www.refworld.org.es/docid/47a080e32.html

162 Art 16, Constitución Política de los Estados Unidos Mexicanos, México, 1917.

163 Art 3, fracción I, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, México, 2010.

2. Definición

La definición "aviso de privacidad" no puede entenderse sin el principio de información. El derecho fundamental de protección de datos personales tiene su base en un elenco de principios que lo configuran como tal derecho, de modo que constituyen su núcleo básico y por tanto cualquier fallo o violación de éstos, implica una violación al propio derecho.

Dentro de esta gama de principios se encuentra el de información, el cual impone, al responsable del tratamiento, la obligación de informar al titular de los datos personales, entre otras cosas, quién es el responsable del tratamiento, para qué fines se utilizarán, con quién se compartirán y cómo ejercer los derechos de protección de datos personales que les reconoce la normatividad.

En términos de la normatividad aplicable de datos personales en México, el principio de información se materializa a través de la puesta a disposición del aviso de privacidad al titular de los datos personales que serán sujetos a tratamiento. De este punto reviste el rol protagónico que tiene el aviso de privacidad en la normatividad de datos personales en México, ya que la única manera que un responsable pueda cumplir con el principio de información es mediante el aviso de privacidad.

El aviso de privacidad garantiza la salvaguarda del derecho de autodeterminación informativa reconocido en las normatividades de protección de datos personales en México.

Es importante saber que tanto la normatividad de sector privado que regula la figura del aviso de privacidad (LFPDPPP, RLFPDPPP y Lineamientos del Aviso de Privacidad), como la de sector público (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales), prevén requisitos de información que resultan similares, tales como:

A. la identidad del responsable del tratamiento;
B. las finalidades, primarias y secundarias;
C. los terceros a quienes se transferirán los datos personales (si éste fuera el caso);
D. los mecanismos para que el titular pueda ejercer los derechos vinculados a la protección de datos personales;[164]
E. un procedimiento para comunicar los cambios en los avisos de privacidad;
F. el posible tratamiento de datos personales sensibles, entre otras cuestiones.

Algunos de los requisitos de información específicos que se exigen en la regulación aplicable para el sector público son los siguientes:

A. fecha de elaboración o de última actualización del aviso de privacidad;
B. el fundamento legal que faculta al responsable para llevar a cabo el tratamiento, con independencia de que se requiera o no el consentimiento (incluir artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que lo faculta o le confiera atribuciones para realizar el tratamiento de datos personales que informa en el aviso de privacidad, precisando su fecha de publicación o, en su caso, la fecha de la última reforma o modificación);
C. el domicilio de la unidad de transparencia (calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa, así como su número y extensión telefónica).

164 Este mecanismo se denomina Ejercicio de Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

El concepto "aviso de privacidad" se define tanto en la LGPDPPSO como en la LFPDPPP. Para efectos de la presente definición tomaremos como referencia la prevista en el artículo 3 de la LGPDPPSO, el cual expresa con toda claridad lo que debemos entender por "aviso de privacidad":

> […] II. Aviso de privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos [...][165]

Como se mencionaba anteriormente, de la explicación conceptual del aviso de privacidad se desprende la obligación del responsable a informarle al titular la existencia y características principales del tratamiento al que serán sometidos sus datos personales. La mencionada obligación, regulada en la normatividad de sector público, se encuentra consignada en el artículo 26 de la LGPDPPSO, misma que a la letra se lee:

> [...] El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.
>
> Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable.
>
> Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla.
>
> Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva […]

La ley obliga a quien da tratamiento de la información a: i) informar, siendo el mecanismo idóneo el aviso de privacidad, ii) como parte del contenido del aviso, explicar el uso que se le dará a los datos, iii) recurrir a la publicidad del aviso de privacidad, iv) contar con una redacción apropiada, clara y sencilla, que permita una fácil comprensión y v) ante una imposibilidad para la presentación del aviso, puede buscarse medidas compensatorias para hacerlo.

Al igual que en el sector público, en el sector privado se exige que el aviso de privacidad sea un mecanismo de información eficiente y práctico, que deberá ser sencillo, con información necesaria, expresado en español, con lenguaje claro y comprensible y con una estructura y diseño que faciliten su entendimiento.

Asimismo, las disposiciones secundarias para el sector privado emitidas por el INAI aclaran que para que el aviso de privacidad reúna las características antes señaladas, el responsable debe asegurarse de "no usar frases inexactas, ambiguas o vagas; tomar en cuenta los perfiles de los titulares; no incluir textos o formatos que induzcan al titular a elegir una opción en específico; en caso de que se incluyan casillas para que el titular otorgue su consentimiento, no se deberán marcar previamente; no remitir a textos o documentos que no estén disponibles para el titular".

El aviso de privacidad tiene tal nivel de importancia que puede ejemplificarse como "las reglas del juego" sobre las cuales los jugadores (el responsable y el titular de la información) basarán su actuar dentro del marco de sus derechos y obligaciones. De hecho, una condición necesaria para que el consentimiento del tratamiento de datos personales sea válido, es que sea informado, lo que implica que el titular conozca el aviso de privacidad previo a la manifestación de su voluntad.

165 Cámara de diputados. (2017, enero 26). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados". *Diario Oficial de la Federación*. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

De esta forma y bajo esta tesitura, el tratamiento de datos personales que efectúe el responsable únicamente deberá circunscribirse a las finalidades informadas dentro del aviso de privacidad, las cuales deberán ser concretas, lícitas, explícitas y legítimas.

Toda vez que es obligación del responsable tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad,[166] resulta trascendental cuidar, tanto la forma de obtener los datos personales, como el tratamiento que se le da a los mismos, ya que de no cumplirse con las características referidas en el párrafo anterior, se puede correr el riesgo de estar frente a una actuación engañosa o fraudulenta por parte del responsable de la información.

Se considera que existe una actuación fraudulenta o engañosa cuando: i) existe dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento, ii) se vulnere la expectativa razonable de privacidad del titular a la que refiere el artículo 7 de la Ley o iii) las finalidades no sean las informadas en el aviso de privacidad.

Consecuentemente, el responsable no podrá tratar datos personales para finalidades distintas a las establecidas en el aviso de privacidad, salvo que cuente con atribuciones conferidas en la ley y medie el consentimiento del titular.[167]

No solo será importante contar con el aviso de privacidad sino darle una debida difusión. Algunas de las obligaciones que impone la normatividad en relación con la debida difusión del aviso de privacidad se encuentran las siguientes: difundirlo por medios electrónicos y físicos y ubicarlo en un lugar visible que facilite la consulta del titular y que le permita acreditar fehacientemente el cumplimiento de esta obligación ante el Instituto.

Es importante considerar que al presentarse una controversia entre el titular y el responsable de la información respecto de la acreditación de la puesta a disposición del aviso de privacidad, quien tendrá la carga probatoria será, en todos los casos, el responsable.

166 "Artículo 7. Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley. En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables".
"Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:
I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;
II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
VIII. Cuando los datos personales figuren en fuentes de acceso público;
IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o
X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia".

167 "Artículo 21 de la LGPDPPSO: El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología. El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario. Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente. Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta Ley".

Con base en lo antes expuesto, puede decirse que el aviso de privacidad tiene un doble objeto. Desde la perspectiva del titular de los datos, el aviso delimita e informa los alcances y condiciones generales del tratamiento para que la persona a la que pertenecen pueda tomar decisiones informadas sobre el uso de sus datos personales y tener control y disposición sobre la información que le atañe. Por otra parte, desde la faceta de quien lo emite, permite transparentar los tratamientos de datos personales y con ello fortalecer el nivel de confianza con los titulares.

Por ello, su presencia es imprescindible incluso en aquellos casos en los que el consentimiento para el tratamiento pudiera no ser requerido como consecuencia de una excepción normativa, pues si bien el responsable puede estar exento de recabar el consentimiento, en ningún caso la Ley le exime de la responsabilidad de informar al titular de los datos sobre las generalidades aplicables al tratamiento de los datos personales. Lo anterior significa que, a diferencia del principio del consentimiento, el principio de información no cuenta con excepciones legales.

Finalmente, es importante tener presente que en el supuesto de que el responsable requiera modificar los términos del aviso de privacidad, éste estará obligado a poner a disposición del titular un nuevo aviso de privacidad, cuando se presenten alguno de los siguientes supuestos: a) cambie su identidad, b) requiera recabar datos personales sensibles, patrimoniales o financieros adicionales a aquéllos informados en el aviso de privacidad original, cuando los mismos no se obtengan de manera personal o directa del titular y se requiera el consentimiento, c) cambien las finalidades que dieron origen o son necesarias para la relación jurídica entre el responsable y el titular, o bien, se incorporen nuevas que requieran del consentimiento del titular o d) se modifiquen las condiciones de las transferencias o se vayan a realizar transferencias no previstas inicialmente, y el consentimiento del titular sea necesario.

NOTAS

NOTAS

NOTAS

Bb

Bases de datos

Isabel Davara Fernández de Marcos,[168]
Gregorio Barco Vega y
Alexis Cervantes Padilla

Según la normatividad mexicana, una base de datos es un conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización. Tanto la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) como la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) incluyen el término en sus definiciones.

Definición de base de datos	
Artículo 3, fracción II de la LFPDPPP	Artículo 3, fracción III de la LGPDPPSO
El conjunto ordenado de datos personales referentes a una persona identificada o identificable. [169]	Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

168 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

169 Cabe notar que el artículo 3 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLGPDPPP) establece, al determinar el ámbito objetivo de aplicación del mismo, que este aplicará a: "[…] datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización […]".

De acuerdo con el contenido de las definiciones legales anteriores podemos distinguir los siguientes elementos:

- Se refiere a un grupo de datos personales.
- Los datos personales deben estar ordenados u organizados bajo criterios determinados.
- Los datos personales deben ser concernientes a una persona física identificada o identificable.
- Para que los datos personales pasen a formar una base de datos no son relevantes aspectos como la forma o modalidad de su creación, el soporte empleado, el procesamiento, el almacenamiento ni la forma de su organización.

Además de los criterios señalados y teniendo en cuenta que es una definición legal que implica que el tratamiento de dichos datos, se tendrá que adaptar a un régimen jurídico concreto, es relevante discernir el concepto desde este enfoque y esto se determina teniendo en cuenta no solo los datos personales que están sujetos a tratamiento sino muy particularmente la finalidad o finalidades jurídicas para las cuales dichos datos personales son objeto de tratamiento. Es por ello que, conforme a la normatividad de datos personales, habrá que distinguir o diferenciar las bases de datos en relación con la finalidad o finalidades bajo las cuales se sustenta el tratamiento de los datos personales que las integran.[170]

1. Distinción sobre los usos del término

Se podrían establecer diversas clasificaciones, entre las que seleccionaremos un criterio de contenido y uno de titularidad:

- Por su delimitación física y/o conceptual:

  1. Base de datos física. El criterio para determinar la existencia de la base de datos física es el tipo de soporte en que se encuentra, de forma tal que será aquella que obre en un soporte físico.[171]

  2. Base de datos lógica. Se puede distinguir la base de datos por la organización lógica de la información, esto es, por donde se almacena y trata la información, que no es de una manera física. Esta delimitación, del mismo modo que la física, no tiene por qué coincidir con la delimitación legal o jurídica que veremos después.

  3. Base de datos jurídica. Como decíamos en la sección anterior, las bases de datos personales que denominamos jurídicas o legales son las que se tienen que determinar en función de la finalidad del tratamiento y los datos que se incluyen en el mismo, pero el criterio delimitador esencial sería el de la finalidad, puesto que como hemos ya señalado, ésta permitirá enjuiciar la licitud del tratamiento en cuestión.
- Por su titularidad: se pueden distinguir las bases de datos, tratamientos o "ficheros" —los cuales explicaremos más adelante— a partir de la naturaleza jurídico pública o jurídico privada del responsable.[172]

170 "Artículo 12. El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en el aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular".

171 En este sentido, el RLFPDPPP indica que el soporte físico es el medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales (artículo 3, fracción XI).

172 Agencia Española de Protección de Datos. Informe 0298/2009.

2. Bases de datos que contienen datos personales sensibles

Como criterio particular, la creación de bases de datos con información personal de carácter sensible se sujeta a reglas legales más estrictas y se encuentra vedada salvo que existan finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado o bien exista una base concreta de legitimación del tratamiento.

En este orden de cosas, tanto la LGPDPPSO como la LFPDPPP establecen que la creación de estas bases de datos, además de cumplir con la finalidad del tratamiento, puedan justificarse dentro de las actividades legítimas del responsable y prohíben la creación de bases de datos que contengan datos personales sensibles sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el responsable del tratamiento:

El artículo 7 de la LGPDPPSO indica: "Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley".

Por su parte, el artículo 9, párrafo segundo de la LFPDPPP, dice que: "No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado".

Asimismo, el artículo 56 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) es contundente al concretar:

> En términos de lo previsto en el artículo 9, segundo párrafo de la Ley, solo podrán crearse bases de datos que contengan datos personales sensibles cuando:
>
> I. obedezca a un mandato legal;
>
> II. se justifique en términos del artículo 4 de la Ley[173] o
>
> III. el responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

De esto se desprende entonces, que la creación de bases de datos personales con información sensible debe estar debidamente justificada por parte del responsable.

3. Derecho comparado: el concepto de fichero

En el derecho comparado podemos observar que la normatividad de datos personales tiende a emplear el término "fichero" en lugar del término "base de datos" porque ambos conceptos tienen elementos coincidentes.

La directiva 95/46/CE[174] acuñó el término "fichero" y lo definió, en el inciso b de su artículo 16, de la siguiente forma: "Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".[175] De forma posterior, las normatividades europeas de protección de datos personales acogieron dicho término para la concreción de definiciones legales.

---

173 "Artículo 4. Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros. (LFPDPPP)".

174 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

175 "Artículo 3.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y accesos".

En este sentido, la ley orgánica 15/1999 de protección de datos de carácter personal (LOPD), del 13 de diciembre, acogió el término de fichero en idénticos términos a los de la directiva 95/46/CE,[176] que distingue entre ficheros de titularidad pública y privada.[177]

Posteriormente, el reglamento de la LOPD,[178] en las letras (l) y (m) del número primero de su artículo 5 contempló la definición, tanto de los ficheros de titularidad privada como pública, disponiendo lo siguiente:

> l. Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.
>
> m. Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos.

Actualmente se encuentra en trámite una nueva ley orgánica de protección de datos que derogará la LOPD[179] y cualquier otra normatividad que sea incompatible con lo dispuesto en el reciente Reglamento General de Protección de Datos Personales (RGPD o GDPR por sus siglas en inglés), que como es de aplicación directa, desplaza a dicha normatividad, salvo algunas consideraciones muy específicas. En este orden de ideas, cabe señalar que el RGPD aporta una definición precisa de fichero en el apartado 6 de su artículo 4 y señala que se entenderá por "fichero" a "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".[180] Esta definición tiene el mérito de aportar, como característica de "fichero" (entendido como un conjunto de datos personales), el que pueda encontrarse centralizado, descentralizado o repartido de forma funcional o geográfica.

176 "Artículo 3.
Definiciones.
a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso".

177 Agencia Española de Protección de Datos. Informe 0298/2009.

178 Reglamento de desarrollo de la ley orgánica 15/1999 de protección de datos de carácter personal, del 13 de diciembre, aprobado por real decreto 1720/2007 el 21 de diciembre.

179 Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal. Disponible en: http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-3.PDF

180 "Artículo 4.
6) fichero: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica".

Big data

Isabel Davara Fernández de Marcos,[181]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El concepto de *big data*, traducido en ocasiones como macrodatos, suele emplearse para referirse a las grandes cantidades de datos que únicamente pueden ser procesadas por supercomputadoras, así como a las nuevas técnicas de análisis de dichos datos basadas en el uso de algoritmos que se han desarrollado para extraer valor de esta información.

El estudio de este concepto es imprescindible para explicar el fenómeno que se deriva del desarrollo de tecnologías en las últimas décadas, las cuales permiten amasar y procesar datos en cantidades mucho más grandes y variadas y a mayor velocidad que en cualquier momento de la historia de la humanidad. La magnitud del desarrollo se ha traducido asimismo en nuevos y distintos usos de la información en diversos sectores de la sociedad, que han descubierto en la información un valor antes desconocido. Es por esto que a la información se le conoce como el petróleo del siglo XXI y a la analítica de datos se le ha comparado, en importancia, con la creación del motor de combustión interna.[182] En 2011, el Foro Económico Mundial describió a los datos personales como "la nueva clase de activo" que impacta a todos los aspectos de la sociedad.[183]

El concepto "*big data*" es amplio e incluyente, y encuentra una diversidad de definiciones que enfatizan diferentes elementos, dependiendo de la fuente y el contexto considerados para su elaboración. Por ejemplo, enfocándose en la analítica de la información, el Supervisor Europeo de Protección de Datos lo define como "la práctica de combinar grandes volúmenes de información procedentes de fuentes diversas y analizarlos, mediante el uso frecuente de algoritmos autodidactas como método para fundamentar las decisiones".[184]

La multicitada[185] definición del glosario de Gartner IT (que incorpora las tres ya famosas "v": volumen, variedad y velocidad) define el concepto "*big data*" enfatizando las características de la información que se compone en estos entornos: "Big data son los activos de información de gran volumen, gran velocidad y gran variedad que requieren de formas innovadoras de procesamiento para poder obtener una perspectiva, tomar decisiones y automatizar procesos de forma mejorada".[186]

---

181 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez en la elaboración de este trabajo.

182 Sondengaard, P. (2017, febrero 2). "La información es la gasolina del siglo XXI, y la analítica de datos el motor de combustión". En *BBVA*. Recuperado de: https://bbvaopen4u.com/es/actualidad/la-informacion-es-la-gasolina-del-siglo-xxi-y-la-analitica-de-datos-el-motor-de> Fecha de consulta: 2 de octubre de 2018.

183 World Economic Forum. (2011, febrero 17). *Personal Data: The Emergence of a New Asset Class*. Recuperado de: https://www.weforum.org/reports/personal-data-emergence-new-asset-class. Fecha de consulta: 2 de octubre de 2018.

184 European Data Protection supervisor. (2015, septiembre 11). *Dictamen 4/2015 Hacia una nueva ética digital. Datos, dignidad y tecnología,* p. 7. Recuperado de: https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_es.pdf

185 Citada, entre otros, por la Oficina del Comisionado de Información del Reino Unido (ICO por sus siglas en inglés) en su reporte *Big data, artificial intelligence, machine learning and data protection v.2* de 2017 y por el Consejo de Consultores en Ciencia y Tecnología del Presidente de Estados Unidos (PCAST por sus siglas en inglés) en su reporte *Big data and Privacy- a technological perspective* de mayo de 2014. Sin embargo, citan una versión ya desactualizada de la definición.

186 Gartner. "Big Data". En *Gartner IT Glossary.* Disponible en: https://www.gartner.com/it-glossary/big-data/ Fecha de consulta: 2 de octubre de 2018.

El Consejo de Asesores en Ciencia y Tecnología del presidente de los Estados Unidos (PCAST por sus siglas en inglés),[187] durante la administración del presidente Obama, al estudiar el concepto de *big data*, precisó que la definición varía dependiendo de su contexto, por ejemplo, si el que la formuló es un informático, un analista financiero o un emprendedor. De la misma forma, señala que la mayoría de las definiciones refleja la creciente capacidad tecnológica de capturar, agregar y procesar datos en grandes volúmenes, velocidad y variedad.[188] Sin embargo, el PCAST puntualiza que para efectos de responder las preguntas planteadas a las normas legales, éticas y sociales lo que en verdad importa son los usos potenciales de la analítica del *big data.*[189]

Por otro lado, Vicktor Mayer-Schönhberger y Kenneth Cukier abordan el concepto de forma más amplia: "Big Data refiere a lo que puede hacerse a gran escala que no puede hacerse en una escala pequeña, para extraer nuevos conocimientos o crear nuevas formas de valor, en formas que cambien mercados, organizaciones, relaciones entre ciudadanos y gobiernos, y más".[190]

Por su parte, el Grupo de Trabajo del Artículo 29 (GTA29)[191] ha destacado que *big data* es un término amplio que cubre un gran número de operaciones de tratamiento de datos personales, algunas de las cuales pueden ser identificadas, mientras que otras, todavía son poco claras y muchas más, de futuro desarrollo.[192]

Finalmente, en estudios de carácter más práctico, se ha puntualizado que este término "hace referencia al conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo".[193]

De esta forma, una vez que se ha precisado lo que implica el término *"big data"* podemos identificar sus características más representativas. En este sentido, se ha destacado que el *big data* se distingue de otras tecnologías afines porque su análisis puede conjugar, al mismo tiempo, tres características que antes eran incompatibles, dadas las limitaciones

187 President's Council of Advisors on Science and Technology. Disponible en: https://obamawhitehouse.archives.gov/administration/eop/ostp/pcast

188 Gracias a que la capacidad informática de procesamiento —debido a la progresión de la potencia de los nuevos procesadores informáticos, la progresión de la capacidad de memoria, etc.— se viene multiplicando exponencialmente al ritmo de lo que se conoce como la Ley de Moore, aunque ya hay varias voces que cuestionan su viabilidad en los próximos años.

189 Consejo de Consultores en Ciencia y Tecnología del Presidente de Estados Unidos. (2014, mayo). *Big Data: Seizeing Opportunities, Preserving Values*. Washington, p. 2.

190 Mayer-Schönberger, V. y Kenneth C. (2014). *Big Data.* Mariner Books. Nueva York, p.6.

191 Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. Actualmente este grupo ha sido sustituido por el Comité Europeo de Protección de Datos Personales. Disponible en: https://edpb.europa.eu

192 "Big data is a broad term that covers a great number of data processing operations, some of which are already well-identified, while others are still unclear and many more are expected to be developed in the near future". Cita extraida de: ARTICLE 29 DATA PROTECTION WORKING PARTY. (2014, septiembre 16). *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, WP221.* Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp221_en.pdf

193 Agencia Española de Protección de Datos (AEPD) y la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Fórum Spain. *Código de buenas prácticas para protección de datos en proyectos de Big Data*. España. Disponible en: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf Fecha de consulta: 15 de noviembre de 2018.

tecnológicas, las ya mencionadas tres "v": [194] volumen, variedad y velocidad. A continuación se desarrollan brevemente estas características.[195]

- Volumen. De acuerdo con esta característica del *big data* es posible que una gran cantidad de datos puedan recopilarse y analizarse gracias a las nuevas tecnologías. Sin embargo, no existe un consenso para determinar a partir de qué cantidad un conjunto de datos puede ser *big data*, aunque se suele aceptar que éste puede incluir de 30 a 50 *terabytes* hasta varios *petabytes*.
- Variedad. Esta característica del *big data* hace referencia a su capacidad de recoger datos de fuentes heterogéneas (estructuradas o no estructuradas) que pueden comprender información proveniente de internet, dispositivos móviles, internet de las cosas, datos sectoriales recopilados por empresas especializadas, datos experimentales, entre otras muchas fuentes.
- Velocidad. Según esta característica el *big data* sirve para analizar grandes conjuntos de datos de forma rápida —incluso en tiempo real— de forma tal, que es posible transferir datos de forma barata y eficiente.[196]

Además de las características anteriores, autores como Elena Gil destacan que dichas características pueden ser ampliadas con tres "v" más:

- Veracidad. Esta característica se concreta en el nivel de fiabilidad o calidad de los datos, pues en función de su naturaleza, muchos de ellos pueden ser inciertos y ninguna técnica de limpieza de datos podría garantizar su corrección, por lo que lidiar con la incertidumbre de estos tratamientos es algo frecuente.
- Visualización. Esta característica demanda "la posibilidad de poder visualizar los datos para comprenderlos y tomar decisiones en consonancia".
- Valor. Según esta característica, "la finalidad última de los procesos de *big data* es crear valor, ya sea entendido como oportunidades económicas o como innovación".

Además de las características señaladas, el *big data* también se distingue de otras herramientas de procedimiento tradicional por hacer uso intensivo de algoritmos y utilizar los datos para nuevos fines.

En lo que toca a sus usos, el *big data* tiene múltiples aplicaciones que cubren muchos y diversos sectores y actividades como salud, educación, comercio, seguros, laboral, y financiero en el sector público y privado.[197]

194 Gil, E. (2016). *Big data, privacidad y protección de datos*. Agencia Española de Protección de Datos. Madrid, p. 21.

195 La autoridad de protección de datos personales del Reino Unido Information Commissioner's Office (ICO, por sus siglas en inglés), al abordar las características del *big data,* precisa que éste es descrito a menudo con base en estos rasgos, donde el volumen se relaciona con los conjuntos masivos de datos, la velocidad se relaciona con los datos en tiempo real y la variedad se refiere a las distintas fuentes de los datos. Véase: ICO. (2017). *Big data, artificial intelligence, machine learning and data protection*. Disponible en: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

196 Gil, E. (2016). *Big data, privacidad y protección de datos*. Agencia Española de Protección de Datos. Madrid, pp., 22-28

197 En relación con este tema se pueden consultar los siguientes documentos: Gil, E. (2016). *Big data, privacidad y protección de datos*. Agencia Española de Protección de Datos. Madrid, ICO. (2017). *Big data, artificial intelligence, machine learning and data protection.* Disponible en: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf y Agencia Española de Protección de Datos (AEPD) y a la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain. (2018 noviembre 15). *Código de buenas prácticas para protección de datos en proyectos de Big Data*. España, p.5. Disponible en: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf Fecha de consulta: 15 de noviembre de 2018.

Hasta ahora hemos descrito únicamente las características y contenido del *big data* sin entrar aún en sus implicaciones en protección de datos personales. En este sentido, en tanto que a través de la información obtenida o empleada por esta tecnología se puede identificar a la persona, habrá que tener en cuenta la normatividad de datos personales.

Aquí, como lo señalan diversas autoridades y organizaciones, "la identificabilidad, que supone la aplicación de la normativa, se refiere a que una persona pueda ser identificada por un dato o por la combinación de información de diversas fuentes".[198]

De esta forma, cuando el *big data* entraña el tratamiento de datos personales será pertinente tener en cuenta el cumplimiento, al menos, de las siguientes obligaciones:

1. Principios de licitud y lealtad: es fundamental que las organizaciones faciliten a los titulares la información sobre el tratamiento de sus datos, así como evaluar los efectos del tratamiento en las personas y las expectativas que tienen respecto al destino que se dará a sus datos.[199]
2. Principio de consentimiento: en términos generales, para poder dar tratamiento a los datos personales para proyectos de *big data*, el responsable debería contar con el consentimiento libre, específico e informado (tácito, expreso o expreso y por escrito), salvo que el mismo no sea requerido en términos de Ley.[200] Sin embargo, la legitimación por medio del consentimiento en muchas ocasiones es difícil de emplear en estos tratamientos, puesto que la definición de la finalidad, en particular del resultado que se obtenga de este análisis, es muy complicada, si no imposible.
3. Principio de información: de acuerdo con este principio, se debe informar a los titulares sobre las condiciones generales a las que se sujetará el tratamiento de sus datos personales por medio del aviso de privacidad que contenga los elementos requeridos por la Ley, en particular, la concreción de las finalidades del tratamiento, las cuales legitimarán el uso de sus datos, o incluso, en la medida de lo posible, aquéllas que podrían derivarse de una finalidad consentida por el titular. Como decíamos, éste es uno de los puntos más complicados y controvertidos en el análisis de *big data,* porque el algoritmo puede generar patrones de aprendizaje propios que hagan imposible conocer el resultado que se obtendrá de dicho tratamiento, poniendo en cuestión la concreción de la finalidad y, por ende, el principio de información (además del de consentimiento que hemos mencionado). En todo caso, la transparencia en la información, realizando el mejor de los esfuerzos y teniendo en cuenta que una de las características definitorias es la opacidad del algoritmo, es clave para el éxito y legitimación de estos tratamientos.
4. Principio de legitimación (interés legítimo): aunque este principio no se prevé en la normatividad nacional, es importante tener en cuenta que para la realización legítima de estos tratamientos sería necesario reformar el régimen regulatorio actual para dar

198 Agencia Española de Protección de Datos (AEPD) y a la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain. (2018, noviembre 15). *Código de buenas prácticas para protección de datos en proyectos de Big Data*. España, p.5. Disponible en: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf. Fecha de consulta: 15 de noviembre de 2018.

199 *Vid*, ICO. (2017). *Big data, artificial intelligence, machine learning and data protection*. Disponible en: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

200 Recomendamos consultar la definición de principio consentimiento en este diccionario.

lugar a la inclusión de esta figura y, de forma concreta, determinar si el tratamiento puede ampararse en una base de legitimación distinta del consentimiento.[201]

5. Principio de calidad: este principio, de forma general, demanda no conservar datos personales más allá del período en que sea necesario su tratamiento. Sin embargo, en proyectos de *big data* esto puede representar dificultades considerando la capacidad de almacenamiento de los sistemas y la habilidad de estas tecnologías para procesar grandes volúmenes de datos, por lo que las organizaciones necesitan ser claras con el titular sobre lo que esperan aprender o ser capaces de hacer al dar tratamiento a los datos. El reto, de nuevo, es definir las finalidades del tratamiento y establecer qué datos serán relevantes para su cumplimiento.[202]
6. Principio de finalidad: este principio no necesariamente crea una barrera para el *big data* pero sí entraña, como adelantamos, una especial dificultad, la cual requerirá que el responsable realice un análisis de compatibilidad sobre las finalidades del tratamiento consentidas por el titular frente a aquellos tratamientos que permite legitimar sin la base del consentimiento por las cuestiones anteriormente expuestas. Por ello, la licitud del tratamiento es un factor clave para determinar si el análisis de *big data* resulta incompatible con las finalidades originalmente autorizadas por el titular.[203]
7. Principio de proporcionalidad: para dar cumplimiento a este principio es preciso que el responsable recabe únicamente los datos mínimos necesarios para dar cumplimiento a las finalidades del tratamiento y no dé tratamiento a datos personales que resulten excesivos o no sean requeridos para cumplir con los fines del tratamiento. De nuevo, al pensar que precisamente el *big data* se define por la ingente cantidad de datos tratados, este principio parece entrar en contradicción.
8. Principio de responsabilidad: según este principio, es menester que, previo a la puesta en marcha de un proyecto de *big data*, el responsable adopte las medidas para cumplir con la normatividad de datos personales, entre ellas, la elaboración de una evaluación de impacto en la protección de datos, adoptar los enfoques de protección de datos por defecto y protección de datos por diseño, regular adecuadamente las relaciones con los encargados o terceros que intervengan en el tratamiento y adoptar un enfoque de ética digital y responsabilidad algorítmica.
9. Deber de seguridad: derivado de este deber será necesario que, considerando en particular la naturaleza de los datos y los riesgos existentes y/o futuros, el responsable establezca las medidas de seguridad físicas, técnicas y administrativas que resulten suficientes y necesarias para proteger los datos personales.
10. Deber de confidencialidad: este deber obliga al responsable a mantener la secrecía de aquella información que obre en su poder, así como de aquélla que pudiera derivarse de la instrumentación de proyectos de *big data*.
11. Derechos de los titulares: el responsable se encuentra obligado a atender, y en caso de resultar procedentes, hacer efectivos los derechos de acceso, rectificación, cancelación, oposición y portabilidad. No obstante, en particular deberá proporcionar acceso a los datos utilizados para la instrumentación de procesos de toma de deci-

201 Recomendamos consultar la definición de interés legítimo en este diccionario.

202 *Vid*, ICO. (2017). *Big data, artificial intelligence, machine learning and data protection*. Disponible en: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

203 Ídem.

siones sin intervención humana y permitir la rectificación de los mismos. Las dificultades de atender estos derechos en este tipo de proyectos son más que evidentes, de nuevo, teniendo en cuenta el volumen de dichos datos.

En definitiva, y según lo ya antes mencionado, hay que concluir que el *big data* es un concepto dinámico con múltiples implicaciones en la esfera del derecho a la protección de datos personales en caso de que la persona física sea identificada o identificable, por lo que su adopción requerirá de un análisis a consciencia de las implicaciones que estos proyectos podrían tener para los titulares involucrados, procurando eliminar enfoques poco objetivos, sesgados o que pudieran repercutir negativamente en la esfera de derechos individuales.

Bloqueo de los datos personales

María Solange Maqueo Ramírez

De conformidad con el artículo 3, fracción III, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), el bloqueo consiste en "[l]a identificación y conservación de datos personales una vez que cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y, transcurrido éste, se procederá a su cancelación en la base de datos que corresponde." Esta misma definición se encuentra en el artículo 3, fracción IV, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).[204]

En ese sentido, el bloqueo constituye una acción o etapa previa a la supresión o borrado de datos personales durante la cual se impide su tratamiento o posible reutilización por parte del responsable o encargado hasta en tanto prescribe cualquier acción relativa a posibles responsabilidades que pudieran surgir de la relación jurídica entre el titular y el responsable que motivó el tratamiento de dichos datos. Así, el bloqueo supone una forma de tratamiento de datos personales acotada a su propia conservación y, en su caso, puesta a disposición de las autoridades competentes (administrativas o jurisdiccionales) ante el supuesto de que se llegara a actualizar una posible responsabilidad.

1. Supuestos que dan lugar al bloqueo

El responsable del tratamiento de los datos personales debe proceder a su bloqueo cuando éstos han dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, en atención al "principio de calidad" en el tratamiento de los datos personales,[205] sea como consecuencia natural del agotamiento de las propias finalidades establecidas en el aviso de privacidad, o bien, a instancia del titular de los datos personales o de su representante mediante el ejercicio de su derecho de cancelación.

204 "Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda" (Artículo 3, fracción IV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Diario Oficial de la Federación*. 26 de enero de 2017).

205 Cfr. Artículo 11. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. 5 de julio de 2010; artículo 23. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Diario Oficial de la Federación*. 26 de enero de 2017 y numeral 19 de los Estándares de Protección de Datos para los Estados Iberoamericanos, aprobados por la Red Iberoamericana de Protección de datos en junio de 2017.

2. Plazos de conservación

El periodo de bloqueo supone un plazo adicional y posterior a aquél que es necesario para el cumplimiento de las finalidades que motivaron el tratamiento de los datos personales. Su duración, entonces, debe considerar los plazos legales y contractuales que resulten aplicables para demostrar posibles responsabilidades, todo lo cual depende, a su vez, de la materia de la que se trate. Asimismo, debe considerarse que en ocasiones existen disposiciones jurídicas que establecen plazos específicos de conservación de datos personales, por ejemplo, en materia fiscal o contable, administrativa o histórica, mismos que deberán tomarse en consideración antes de proceder a la supresión de la información. En ocasiones, éstos últimos pueden coincidir con el periodo de bloqueo.[206]

3. Obligaciones relacionadas con el bloqueo

El responsable del tratamiento de los datos personales está obligado a documentar el procedimiento de bloqueo, de acuerdo con el artículo 24 de la LGPDPPSO y 38 del Reglamento de la LFPDPPP. Ello supone la realización de un escrito en el que se establezca, no solo que se ha llevado a cabo el bloqueo correspondiente, sino también cómo se ha implementado y el periodo de tiempo que durará el mismo antes de la supresión. Esta documentación resulta necesaria, en su caso, para acreditar la realización del bloqueo ante los órganos garantes que llegaran así a requerirlo.

En relación con lo anterior, el artículo 33 de la LGPDPPSO establece para los responsables del tratamiento de datos personales del sector público la obligación de elaborar un inventario de datos personales. Sobre el particular, el artículo 59 de los Lineamientos Generales de Protección de Datos Personales para el sector público establece que en dicho inventario se deberá documentar la información básica de cada tratamiento realizado, entre lo cual se incluye el ciclo de vida del dato. En consecuencia, siendo el bloqueo parte de ese ciclo de vida, éste deberá constar en el inventario correspondiente.

Por su parte, dado que el bloqueo, junto con la supresión de los datos personales, constituyen la forma de atender las solicitudes de cancelación de los datos personales, las disposiciones jurídicas relativas a este procedimiento introducen algunas obligaciones adicionales para los responsables del tratamiento de los datos personales. Al respecto, el artículo 107 del Reglamento de la LFPDPPP establece lo siguiente:

> De resultar procedente la cancelación [...], el responsable deberá:
>
> I. Establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo al titular o a su representante en la respuesta a la solicitud de cancelación, que se emita dentro del plazo de veinte días que establece el artículo 32 de la Ley;
>
> II. Atender las medidas de seguridad adecuadas para el bloqueo;
>
> III. Llevar a cabo el bloqueo en el plazo de quince días que establece el artículo 32 de la Ley, y
>
> IV. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas por el responsable.

En términos análogos por lo que se refiere a la notificación que corresponde al titular de los datos personales, pero con una mayor precisión en cuanto a lo que deberá informársele, el artículo 94 de los Lineamientos generales de protección de datos personales para el

206 Cfr. Secretaría de Protección de Datos del IFAI (ahora INAI). (2014, julio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. México, p. 59.

sector público (Lineamientos Generales) indican que la obligación de cancelar los datos personales se dará por cumplida cuando el responsable notifique al titular, previa acreditación de su identidad y, en su caso la identidad y personalidad de su representante, una constancia que señale que: I. los documentos, bases de datos personales, archivos, registros, expedientes y/o sistemas de tratamiento donde se encuentren los datos personales objeto de cancelación; II. el periodo de bloqueo de los datos personales, en su caso; III. las medidas de seguridad de carácter administrativo, físico o técnico implementadas durante el periodo de bloqueo, en su caso y IV. las políticas, métodos y técnicas utilizadas para la supresión definitiva de los datos personales, de tal manera que la probabilidad de recuperarlos o reutilizarlos sea mínima.

De tal forma que, de acuerdo con lo anterior, el bloqueo de datos personales obliga a los responsables del tratamiento a notificar su realización al titular o a su representante, así como a implementar medidas de seguridad adecuadas para garantizar que se impida el tratamiento de los datos personales bloqueados, salvo por lo que se refiere a su almacenamiento (o conservación) y, en su caso, puesta a disposición de las autoridades competentes ante una eventual responsabilidad.

NOTAS

NOTAS

NOTAS

NOTAS

Ciclo de vida de datos personales

Uciel Fragoso Rodríguez

Los datos personales —como cualquier tipo de información— están sometidos a un ciclo de vida conformado por diversas fases. En la guía COBIT 5[207] *Enabling Information*[208] se identifican seis fases que constituyen el ciclo de vida de la información, las cuales son:

1) planear
2) diseñar
3) construir/adquirir
4) usar/operar
5) monitorear
6) eliminar

La fase de planeación consiste en el entendimiento de cómo la información será utilizada en los procesos de la organización, determinar el valor del activo, realizar su clasificación, identificar sus objetivos y definir la arquitectura tecnológica para su procesamiento.

En la fase de diseño se detallan aspectos de la información como su representación, operación de los sistemas informáticos, desarrollo de estándares y definiciones para los procesos de tratamiento de datos.

La fase de construcción y adquisición de datos es donde la información es creada, adquirida o alimentada de fuentes externas.

La fase de uso y operación corresponde a la etapa más importante del ciclo de vida de la información. En esta fase se realizan actividades de almacenamiento en forma electrónica o en papel (inclusive en la memoria humana), actividades de compartición mediante mecanismos de distribución como pudiera ser un sistema de mensajería o una base de datos y propiamente actividades de uso de consulta o procesamiento para completar las tareas importantes de la organización.

207 COBIT 5 es un marco integral que ayuda a las empresas a lograr sus objetivos para la gobernanza y gestión de la tecnología de la información empresarial (TI).

208 ISACA. (2013). *Cobit 5 Enabling Information*. Recuperado de: http://www.unhas.ac.id/~rhiza/arsip/Sosialisasi_SNI/COBIT-5-Enabling-Information_Res_Eng_1113.pdf

En la fase de monitoreo se garantiza que las fuentes de información continúen operando correctamente y que la información se mantenga actualizada y de calidad.

La fase de eliminación implica que la información ya no es de utilidad en la operación del día a día de la organización, por lo que se debe aislar y retener o en su defecto destruir.

En el artículo 59 de Lineamiento General de Protección de Datos Personales para el Sector Público (Lineamientos Generales)[209] se establece que el responsable de los datos personales deberá identificar los riesgos inherentes en el ciclo de vida de los datos y los activos involucrados en su tratamiento.

Las actividades consideradas dentro del ciclo de vida de los datos personales son obtención, almacenamiento, uso, divulgación, bloqueo y cancelación.

La obtención de datos personales comprende todas las tareas en donde los datos personales son creados de manera directa por fuentes autorizadas o en forma indirecta a través de transferencias o generados mediante procedimientos de deducción. El almacenamiento es el proceso por medio del cual se guardan los datos personales en forma electrónica, impresa o cualquier otro medio. El uso de los datos personales implica el acceso, manejo y procesamiento para el propósito que fueron creados. La divulgación consiste en las remisiones y transferencias de los datos personales hacia otras instancias que requieren y tienen autorización para el tratamiento de los datos personales. El bloqueo se realiza cuando los datos personales ya no son de utilidad, pero por alguna disposición regulatoria interna o externa deben retenerse. La cancelación o destrucción de datos personales implica la eliminación de la información cuando deja de ser útil para el propósito que fue creada.

En la fase I de la *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP)[210] se establece que el ciclo de vida de los datos personales debe estar soportado por una política de gestión de datos personales que fije los lineamientos de los medios a través de los cuales se recaban los datos, que identifique los procesos de la organización que los utilizan, con quién se comparten y en qué momento y por qué medios se suprimen.

La GISGSDP identifica el tipo de tratamiento al que son sometidos los datos personales y que está relacionado directamente con el ciclo de vida, considerando:

a) obtención
b) almacenamiento
c) uso (acceso, manejo, aprovechamiento, monitoreo y procesamiento)
d) divulgación (remisiones y transferencias)
e) bloqueo
f) cancelación o destrucción

La fase de obtención corresponde a la recolección de datos personales directamente del titular, creación o transferencia desde terceros previo consentimiento del titular.

El almacenamiento consiste en el guardado de los datos personales en medios electrónicos como base de datos o servidores de archivos, también pueden almacenarse en forma impresa o cualquier otro tipo de medio. En esta fase es importante dimensionar la cantidad de datos almacenados, diseñar la arquitectura tecnológica para obtener buen des-

209 INAI. (2017). *Lineamientos Generales de Protección de Datos Personales para el Sector Público.*

210 INAI. (2015, junio). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, pp. 14-15. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

empeño e implementar los mecanismos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

La fase de uso es la etapa más importante del ciclo de vida de los datos personales, ya que es ahí donde la información es utilizada para los fines que fueron creados u obtenidos. En esta etapa es donde se especifica quiénes tienen autorización de acceso a los datos personales y el tipo de tratamiento en base a sus roles y responsabilidades.

La fase de divulgación consiste en la remisión de los datos personales hacia terceros para su tratamiento, quedando la responsabilidad dentro de la organización. La transferencia es el envío de los datos a entidades externas convirtiéndose ahora en responsable de los mismos.

En la fase de bloqueo se deshabilitan los datos personales para su uso debido a que ya no son de utilidad para la finalidad de la organización o debido a alguna disposición legal.

La última fase del ciclo de vida de los datos personales es la cancelación o destrucción. Esta tarea debe realizarse acorde a las políticas establecidas y con las medidas de seguridad requeridas.

El ciclo de vida de los datos personales está altamente relacionado con el flujo de la información en los procesos de negocio de la organización, con el tratamiento de los datos personales por parte de las personas, —según sus roles y responsabilidades— los mecanismos de seguridad existentes y faltantes en cada etapa, la valoración de las propiedades de los datos personales en cada fase y el cumplimiento de los principios de privacidad descritos en las principales regulaciones enfocados a la protección de datos personales.

Existe una estrecha relación del ciclo de vida de los datos personales con el flujo de información embebido en los procesos de negocio de la organización. Las organizaciones, para el cumplimiento de su misión, diseñan, implementan y gestionan procesos, por lo que es importante identificar a detalle en qué parte del proceso se tratan datos personales, qué categoría tienen los datos para determinar su nivel de criticidad y qué perfiles tienen las personas que manipulan los datos personales en cada etapa del proceso.

En todos los procesos donde se tratan datos personales se identifican los roles y responsabilidades de las personas que tienen acceso a los datos, para ello se crea una matriz de responsabilidades en donde se especifica, para cada tipo de datos personal, qué perfil tiene acceso a los datos y con qué nivel de privilegio. La matriz de responsabilidades proporciona una gran visibilidad de los posibles riesgos sobre el mal uso de los datos personales debido a una incorrecta asignación de permisos o privilegios, así como cierto tipo de perfiles que no debieran tener acceso a ellos. Con esta información es posible crear escenarios de riesgo que son pieza fundamental en el proceso de análisis de riesgos dentro del proceso de gestión de seguridad de datos personales.

Una de las tareas importantes en la especificación de los escenarios de riesgo es la identificación de mecanismos de seguridad existentes y faltantes necesarios para mitigar el riesgo. Existen medidas de seguridad tecnológicas que protegen la confidencialidad de los datos personales como por ejemplo mecanismos de cifrado o funciones de filtrado para evitar la fuga de información. Existen también medidas de seguridad organizacionales para proteger los datos personales como la definición correcta de perfiles con funciones y responsabilidades y la asignación adecuada de privilegios a dichos perfiles sobre los diferentes tipos de datos personales. Una incorrecta definición de funciones puede provocar que una persona tenga acceso a datos personales aun cuando sus actividades no lo requieran. Una inadecuada asignación de privilegios puede causar que una persona modifique o

elimine un dato personal por error o de manera intencional. Las medidas de seguridad del procedimiento permiten que se realicen modificaciones en la definición de los procesos, cambiando o eliminando tareas que pudieran poner en riesgo los datos personales.

Los datos personales tienen asociadas propiedades que van cambiando a lo largo de su ciclo de vida. Las principales propiedades de los datos son:

a) propósito y valor
b) nivel de privacidad
c) pertenencia
d) responsabilidad
e) calidad

Es importante identificar el propósito y valor de los datos personales en cada una de las etapas de su ciclo de vida. Definir el propósito significa contestar a la pregunta ¿para qué se requieren los datos personales en esta etapa? y determinar su valor representa identificar la importancia de los datos en una fase específica del ciclo de vida.

El requerimiento del nivel de privacidad de los datos personales puede variar en las diferentes etapas del ciclo de vida de los datos personales debido a las obligaciones de cumplimiento o a las actividades dentro de los procesos de negocio que exponen los datos provocando un riesgo a su privacidad.

La pertenencia de los datos personales es asociada generalmente al titular, sin embargo, puede cambiar, por ejemplo, en caso de alguna situación judicial o un evento de seguridad nacional. El propietario de los datos personales es quién toma la decisión y otorga el consentimiento sobre el trato que puede realizarse sobre sus datos. El consentimiento puede otorgarse de manera explícita o tácita, dependiendo de la normatividad interna de la organización o de la legislación vigente de carácter nacional o internacional.

La responsabilidad indica quién está a cargo de los datos personales en las diferentes etapas del ciclo de vida. Esta propiedad queda explícitamente definida a través de la matriz de responsabilidades explicada anteriormente. En caso de algún incidente que dañe el dato personal, el responsable del tratamiento del dato —en esa etapa del ciclo de vida— deberá responder y actuar en conformidad para reparar el daño y mitigar el impacto.

La calidad exige que los datos personales estén completos y sean correctos a lo largo del ciclo de vida, inconsistencias en los datos puede provocar que se atente contra su integridad, que el resultado de su uso no sea el adecuado y que se incumpla con disposiciones regulatorias. Las acciones para garantizar la calidad de los datos consisten en localizar las inconsistencias y realizar tareas de limpieza.

Las regulaciones existentes en una gran cantidad de países con relación a la protección de datos personales se basan en el cumplimiento de principios. En el caso de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[211] y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[212] establecen los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

211 Segob. (2010, julio). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

212 Segob. (2017, enero). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Diario Oficial de la Federación.* Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

Los principios de protección de datos personales expresados en las leyes y regulaciones están relacionados a las fases del ciclo de vida. Por ejemplo, en la fase de obtención de datos, deben ser recolectados a través de medios lícitos y el titular debe estar informado sobre la finalidad del tratamiento de sus datos personales. En las fases de almacenamiento, uso y divulgación se debe cumplir con el principio de calidad y responsabilidad garantizando la calidad de los datos y las medidas adecuadas de seguridad.

Ciclo de vida de la acreditación

Rosa María Franco Velázquez

Para poder certificar en el marco de los Parámetros de Autorregulación Vinculante,[213] el organismo de certificación, que es el que emite la correspondiente certificación en materia de protección de datos personales,[214] tendrá que cumplir con los requisitos necesarios para poder obtener la acreditación por parte de la entidad de acreditación, conforme a la normatividad aplicable.[215] La entidad de acreditación será una persona moral que haya obtenido la autorización por parte de la Secretaría de Economía (SE)[216] para acreditar organismos de certificación en materia de protección de datos personales.[217]

Es así que la acreditación tiene un ciclo de vida que se inicia con el acto de acreditación del organismo de certificación por la entidad de acreditación, hasta que sea, en su caso, suspendida, cancelada o renovada.

Tanto la entidad de acreditación como el organismo de certificación son actores del sistema de certificación en materia de protección de datos personales,[218]siendo necesario considerar que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) tiene atribuciones relevantes con relación a las acreditaciones y puede requerir a la SE o a una entidad de acreditación que inicie un procedimiento de suspensión o revocación de la autorización a la entidad de acreditación, lo que podría dejar sin validez a la acreditación otorgada a uno o varios organismos de certificación.

La solicitud de acreditación[219] tendrá que ser presentada por la entidad candidata ante la SE conforme a lo dispuesto por la Ley Federal sobre Metrología y Normalización, de manera

213 Parámetros de Autorregulación en materia de Protección de Datos Personales. *Diario Oficial de la Federación*. 29 de mayo de 2014.

214 El numeral 54 de los Parámetros indica:
"Certificaciones en materia de protección de datos personales
54. Las certificaciones en el marco de los presentes Parámetros serán otorgadas por organismos de certificación que hayan sido acreditados para tal fin por parte de una entidad de acreditación autorizada por la Secretaría de Economía, en términos de lo dispuesto por la Ley sobre Metrología."

215 La fracción I del numeral 5 de los Parámetros define la acreditación como "acto por el cual una entidad de acreditación aprobada en términos de la Ley Federal sobre Metrología y Normalización, reconoce la competencia técnica y confiabilidad de organismos de certificación para la evaluación de la conformidad de la Ley, el Reglamento, los presentes Parámetros y demás normativa aplicable".

216 La entidad de acreditación es definida en la fracción IV del artículo 5 de los Parámetros de la siguiente manera: "Persona moral autorizada por la Secretaría de Economía, de conformidad con la Ley Federal sobre Metrología y Normalización, para acreditar organismos de certificación en materia de protección de datos personales".

217 Numeral 61 de los Parámetros.

218 Numeral 58 de los Parámetros.

219 El formato para solicitar el reconocimiento e inscripción en el registro de una entidad de acreditación fue publicado por el INAI en el vínculo electrónico http://rea.inai.org.mx/Formatos%20REA/C-1%20Autorizaciones.pdf.

que cuando se cumpla con los requisitos exigibles ésta emitirá la autorización correspondiente. Será necesario también que la autorización otorgada por la Secretaría de Economía se inscriba en el Registro de Esquemas de Autorregulación Vinculante (REA) del INAI.

Cuando la entidad de acreditación otorga a un organismo de certificación la acreditación correspondiente, la constancia deberá contener, como mínimo, la siguiente información:[220]

I. El nombre y el logotipo de la entidad de acreditación;

II. El nombre, número de acreditación y logotipo del organismo de certificación;

III. La información de las oficinas que se encuentran amparadas por la constancia de acreditación;

IV. La fecha de expedición de la constancia de acreditación y la vigencia de la misma;

V. Descripción del alcance de la acreditación, y

VI. Una declaración de conformidad con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), los presentes Parámetros y demás normativa aplicable.

La vigencia de la acreditación queda sujeta a que el organismo de certificación cumpla con los requisitos exigibles, sin perjuicio de que el INAI pueda, en su caso, requerir la suspensión o cancelación de una acreditación "cuando disponga de los elementos suficientes para justificar esa actuación" conforme a la normatividad aplicable.

Como parte del ciclo de vida de la acreditación, ésta podría ser modificada si la entidad de acreditación así lo decide, siendo necesario, en dicho caso, que desarrolle "las actividades necesarias para determinar si amplía o disminuye el alcance de las acreditaciones otorgadas".[221] Cuando se proceda a realizar la modificación, la entidad de acreditación tendrá que notificar al INAI dicha circunstancia.

La acreditación, a lo largo de su ciclo de vida, puede ser objeto de suspensión y cancelación, siendo necesario que las entidades de acreditación establezcan los procedimientos al respecto conforme a la Ley sobre Metrología y Normalización. En este caso, la entidad de acreditación tendrá que notificar sobre la suspensión o cancelación de la acreditación al INAI "y exponer los motivos por los cuales se llevó a cabo la suspensión o cancelación, según corresponda".[222] El INAI también podrá instar a una entidad de acreditación a que inicien alguno de estos dos procedimientos.

Por tanto, que la acreditación se mantenga vigente es el requisito para que un organismo de certificación pueda, a su vez, emitir certificaciones en materia de protección de datos personales.

Finalmente, corresponde al INAI mantener un listado actualizado de entidades de acreditación autorizadas[223] en virtud de lo dispuesto por los Parámetros de Autorregulación Vinculante.

220 Numeral 70 de los Parámetros.

221 Párrafo primero del numeral 72 de los Parámetros.

222 Numeral 73 de los Parámetros.

223 El INAI mantiene el listado de entidades de acreditación y organismos de certificación en el vínculo electrónico http://rea.inai.org.mx/_catalogs/masterpage/Sec6_1.aspx.

Ciclo de vida de la autorización

Rosa María Franco Velázquez

Se prevé en los Parámetros de Autorregulación Vinculante[224] que la autorización, emitida por la Secretaría de Economía (SE), es necesaria para que una persona moral, que cumpla con los requisitos exigibles, pueda convertirse en entidad de acreditación[225] para acreditar[226] a organismos de certificación en materia de protección de datos personales. De manera que la entidad de acreditación autorizada será la que, a su vez, pueda acreditar a organismos de certificación que emitan los certificados en materia de protección de datos personales a los responsables o encargados del tratamiento que cumplan con los requisitos aplicables.

En concreto, "para operar como entidad de acreditación en materia de protección de datos personales, se deberá contar con la autorización previa de la SE en los términos previstos por la Ley sobre Metrología".[227]

En relación con la autorización de la SE a la entidad de acreditación, es necesario que se proceda a su inscripción en el Registro de Esquemas de Autorregulación Vinculante (REA) del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que mantendrá la lista actualizada de entidades de acreditación.[228] Para la inscripción en el REA, será necesario que la SE notifique al INAI aquellas autorizaciones para operar como entidad de acreditación que sean otorgadas en términos de la Ley sobre Metrología".[229]

Una vez que la entidad de acreditación ha obtenido la autorización para poder operar como tal, será necesario que cumpla con las obligaciones que le son exigibles con el fin de poder mantener dicha autorización. El numeral 65 incluye las obligaciones adicionales a las previstas en la Ley sobre Metrología que deberán cumplir las entidades de acreditación y que son las relativas a:

I. resolver las solicitudes de acreditación de personas que busquen fungir como organismos de certificación en materia de protección de datos personales;

II. mantener información actualizada sobre el estado de las acreditaciones que haya otorgado y su alcance;

III. proporcionar al Instituto la información que le requiera sobre acreditaciones en materia de protección de datos personales;

IV. presentar anualmente ante el Instituto un reporte de sus actividades con relación a las acreditaciones en materia de protección de datos personales;

V. notificar al Instituto del otorgamiento, modificación, suspensión y cancelación de las acreditaciones que otorgue a organismos de certificación en materia de protección de datos personales;

224 Parámetros de Autorregulación en materia de Protección de Datos Personales. *Diario Oficial de la Federación*. 29 de mayo de 2014.

225 La entidad de acreditación es definida en la fracción IV del artículo 5 de los Parámetros de la siguiente manera: "Persona moral autorizada por la Secretaría de Economía, de conformidad con la Ley Federal sobre Metrología y Normalización, para acreditar organismos de certificación en materia de protección de datos personales".

226 La acreditación es definida en la fracción I del artículo 5 de los Parámetros como "Acto por el cual una entidad de acreditación aprobada en términos de la Ley Federal sobre Metrología y Normalización, reconoce la competencia técnica y confiabilidad de organismos de certificación para la evaluación de la conformidad de la Ley, el Reglamento, los presentes Parámetros y demás normativa aplicable".

227 Numeral 61 de los Parámetros.

228 Disponible en el vínculo electrónico http://rea.inai.org.mx/_catalogs/masterpage/Sec6_1.aspx.

229 *Vid.* http://rea.inai.org.mx/_catalogs/masterpage/Sec3_2.aspx.

VI. establecer procedimientos y planes para llevar a cabo evaluaciones periódicas de mantenimiento y vigilancia, incluyendo visitas, en intervalos anuales para asegurar el cumplimiento continuo por parte de los organismos de certificación, y

VII. ajustarse a las reglas y procedimientos que se establezcan en la Ley, el Reglamento, los presentes Parámetros, las Reglas de Operación del Registro y demás normativa aplicable.

El cumplimiento de estas obligaciones por la entidad de acreditación es necesario para poder mantener la autorización.

El INAI puede requerir a la SE que inicie un procedimiento de suspensión o revocación de la autorización otorgada a las entidades de acreditación cuando disponga de elementos suficientes para justificar esa actuación en los términos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),[230] el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[231] y los Parámetros de Autorregulación Vinculante.[232]

Por lo tanto, el ciclo de vida de la autorización comienza con la obtención de la misma —cuando la persona moral cumple con los requisitos necesarios— y continúa siempre que no sea suspendida o revocada por la SE y en caso de que transcurra el período de vigencia, quedará sin efecto, siendo necesario en su caso proceder a su renovación.

Ciclo de vida del certificado

Rosa María Franco Velázquez

Un certificado es el documento expedido y acreditado por un organismo de certificación, mediante el cual se hace constar la certificación en materia de protección de datos personales de un responsable o un encargado. Dicha certificación es el procedimiento llevado a cabo por el organismo de certificación por el cual se asegura que un esquema y su implementación se ajustan a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),[233] al Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[234] y a los Parámetros de Autorregulación Vinculante.[235]

Cuando el responsable o encargado que aspira a la certificación cumple con los requisitos (tanto formales como de contenido aplicable), el organismo de certificación emitirá el certificado correspondiente que, como mínimo, contendrá:[236]

I. el nombre y el logotipo del organismo de certificación;

II. el nombre y número de certificación del responsable o encargado certificado;

230 Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* 5 de julio de 2010.

231 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* 21 de diciembre de 2011.

232 Numeral 59, fracción I, de los Parámetros de Autorregulación Vinculante.

233 Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* 5 de julio de 2010.

234 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. 21 de diciembre de 2011.

235 Parámetros de Autorregulación en materia de Protección de Datos Personales. *Diario Oficial de la Federación* 29 de mayo de 2014.

236 Numeral 79 de los Parámetros.

III. la información de las oficinas y, en su caso, servicios que se encuentren amparados por el certificado;

IV. la fecha efectiva de otorgamiento del certificado y su vigencia;

V. descripción del alcance de la certificación, y

VI. una declaración de conformidad con la LFPDPPP, el RLFPDPPP, los presentes Parámetros y demás normativa aplicable.

Para poder obtener la certificación es necesario que la organización, ya sea responsable o encargado del tratamiento, cumpla con todos los requisitos exigidos en virtud del esquema correspondiente de certificación. Si los requisitos exigibles se cumplen, la organización podrá solicitar al organismo de certificación iniciar el proceso de certificación durante el cual procederá a verificar que sea así.

En el ciclo de vida del certificado es necesario considerar que la certificación puede ser objeto de renovación, suspensión y cancelación.

Es así que toda certificación tiene una vigencia que inicia con su emisión, y que implica que el responsable o encargado del tratamiento que la haya obtenido tiene que cumplir con los requisitos necesarios para poder mantenerla.

Una vez que se llegue a la fecha de expiración de la validez del certificado, será necesario que el responsable o encargado del tratamiento que la hubiera obtenido proceda a su renovación. Al respecto, las certificaciones otorgadas en virtud de los Parámetros de Autorregulación Vinculante "tendrán una vigencia de dos años".[237] Si durante ese período no se produce una circunstancia que pudiera dar lugar a la suspensión o cancelación del certificado y una vez que transcurra la vigencia, será necesario que el responsable o encargado del tratamiento procedan a renovar el certificado.

El responsable o encargado del tratamiento "podrán solicitar la renovación ante el organismo de certificación, el cual evaluará la pertinencia de concederla de acuerdo con los procedimientos establecidos para tal efecto".[238]

Si se obtiene la renovación solicitada, el certificado nuevamente tendrá una vigencia de dos años, debiendo proceder a su renovación expirada la misma.

Sin perjuicio de lo anterior, la vigencia de un certificado podría ser objeto, tanto de una suspensión —dejando por tanto de estar vigente durante un período— o incluso de cancelación, en cuyo caso dejaría de tener vigencia.

En el primer caso, el organismo de certificación que hubiera otorgado el certificado al responsable o encargado del tratamiento podrá decidir sobre la suspensión del certificado cuando se den las circunstancias previstas al respecto en la normatividad aplicable.[239] De producirse la suspensión de un certificado en materia de protección de datos personales, el organismo de certificación tendrá que comunicarlo al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y exponer los motivos que dieron lugar a esta situación. Además, el INAI podrá solicitar al organismo de certificación la suspensión de un certificado.

En el caso de la cancelación, será también el organismo de certificación (cuando se den las circunstancias necesarias) el que proceda a iniciar dicho procedimiento. La cancelación dejaría sin efecto al certificado emitido y, por tanto, sería necesario que el responsable o encargado del tratamiento iniciase de nuevo los trámites para obtener una nueva certificación.

237 Numeral 80 de los Parámetros.

238 Numeral 80 de los Parámetros.

239 Ley Federal sobre Metrología y Normalización. *Diario Oficial de la Federación*. 1 de julio de 1992.

Al igual que en el caso de la suspensión, el INAI podrá solicitar al organismo de certificación que proceda a la cancelación de un certificado. Por otra parte, la certificación en materia de protección de datos personales podría ser objeto de modificaciones. En este sentido, será el organismo certificador quien, en su caso, podrá decidir modificar el alcance de la certificación, siendo necesario que determine si la modificación tiene por objeto la ampliación o disminución de su alcance.[240]

Es así que, el ciclo de vida de una certificación en materia de protección de datos personales implica que, una vez que el responsable o encargado del tratamiento lo obtiene al cumplir con los requisitos necesarios, será válido en tanto que no se produzca su suspensión, cancelación o la expiración del plazo de vigencia. En caso de que se produjera alguna de estas circunstancias sería necesario que el responsable o encargado del tratamiento esperase a que se diese fin a la suspensión y, si fuera posible, solicitar un nuevo certificado, en caso de que fuera cancelado, o lo renovará, si ha terminado su vigencia.

Comisionado

Sergio López Ayllón

De manera sucinta se define como el vocablo por el que se nombra a las personas integrantes del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), así como de los organismos garantes de las entidades federativas y de la Ciudad de México que fungen como servidores públicos y gozan de experiencia en materia de acceso a la información pública y protección de datos personales.[241]

1. Delimitación conceptual y conceptos correlacionados

De acuerdo con el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), la Federación debe contar con un organismo autónomo especializado, imparcial y colegiado que garantice los derechos de acceso a la información y de protección de datos personales. Por su parte, el artículo 16, fracción VIII y el 122, sección A, fracción VII establecen que las constituciones de los estados y la de la Ciudad de México tienen que contemplar que sus respectivos organismos autónomos cuenten con los mismos fines y características.

La CPEUM prevé que el Instituto se integre por siete comisionados, en su integración se procurará que exista equidad de género.[242] Los comisionados son servidores públicos y deben contar con las competencias, formación y experiencia necesarias para que, tanto en lo individual como de manera colegiada, puedan cumplir con los principios rectores de los organismos garantes, que son: autonomía, especialización, colegiación, certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.[243]

240 El numeral 82 de los Parámetros, en su párrafo primero, indica, al respecto, que:
"Modificación de la certificación 82. El organismo de certificación podrá modificar el alcance de la certificación otorgada a un responsable o encargado, para lo cual deberá desarrollar las actividades necesarias para determinar si amplía o disminuye el alcance de la certificación otorgada, de conformidad con lo establecido en el numeral 57 de los presentes Parámetros".

241 Artículo 6, apartado A, fracción VIII, párrafo octavo de la Constitución Política de los Estados Unidos Mexicanos.

242 Artículo 6, apartado A, fracción VIII, párrafo octavo de la Constitución Política de los Estados Unidos Mexicanos.

243 Para una explicación de estos principios, véase la voz "órganismos garantes" en este mismo diccionario.

Los comisionados del Instituto, para ser designados, deberán cumplir con los requisitos previstos en las fracciones I, II, IV, V y VI del artículo 95 de la CPEUM. Es decir 1) ser ciudadanos por nacimiento, en pleno ejercicio de sus derechos políticos y civiles, 2) tener por lo menos 35 años cumplidos el día de su designación, 3) gozar de buena reputación y no haber sido condenado por delito que amerite pena corporal de más de un año de prisión (con excepción de algunos delitos en los que se inhabilita automáticamente del cargo sin importar la pena), 4) haber residido en el país durante los dos años anteriores al día de la designación y 5) no haber sido secretario de Estado, fiscal general de la República, senador, diputado federal, ni titular del poder Ejecutivo de alguna entidad federativa, durante el año previo al día de su nombramiento.

Además, éstos no podrán tener otro empleo, cargo o comisión, con excepción de los no remunerados en instituciones docentes, científicas o de beneficencia.

El procedimiento de designación está diseñado para favorecer la autonomía e independencia de los comisionados. De acuerdo con lo establecido en la CPEUM, corresponde a la Cámara de Senadores nombrarlos, a propuesta de los grupos parlamentarios, con el voto de las dos terceras partes de los miembros presentes, previa realización de una amplia consulta a la sociedad.[244] Para esto, los senadores deberán emitir una convocatoria con el objeto de realizar una amplia consulta pública nacional dirigida a toda la sociedad para que presenten sus postulaciones de aspirantes a ocupar el cargo.[245]

El artículo 20 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) establece que el Senado de la República deberá acordar el procedimiento que se debe llevar a cabo, los plazos y los pormenores del proceso de selección. Entre los mecanismos más relevantes para garantizar la publicidad del proceso —y que se tienen que decidir por el senado— se encuentran: 1) hacer pública la lista de los aspirantes a comisionado, 2) hacer públicos los documentos que hayan sido entregados para su inscripción en versiones públicas y, 3) respecto al dictamen que se presente al Pleno a propuesta de los grupos parlamentarios, deberá hacerse público al menos un día antes de su votación. Cabe añadir que, en los últimos procesos de selección, las comisiones de participación ciudadana y justicia del Senado invitaron a la conformación de un comité de acompañamiento ciudadano para el proceso de evaluación de los candidatos.[246]

Es relevante mencionar que la CPEUM también prevé un procedimiento de objeción al nombramiento de comisionados. El mismo solo puede realizarse por el presidente de la República en un plazo de 10 días hábiles después de la designación hecha por el Senado. En caso de que el presidente objetara el nombramiento, la Cámara de Senadores nombrará una nueva propuesta en los mismos términos, pero ahora se requerirá una votación de las tres quintas partes de los miembros presentes. Si este segundo nombramiento fuera nuevamente objetado, la Cámara de Senadores, con la votación de las tres quintas partes de los miembros presentes, designará al comisionado que ocupará la vacante.[247]

Respecto a los organismos garantes estatales, el artículo 32 establece que en el procedimiento, además de la participación de la sociedad, se deberá garantizar la transparencia y la independencia. El cargo no será mayor de siete años y la designación se hará de manera

244 Artículo 6, apartado A, fracción VIII, párrafo octavo de la Constitución Política de los Estados Unidos Mexicanos

245 Artículo 19 de la Ley Federal de Transparencia y Acceso a la Información Pública.

246 Acuerdo de las juntas directivas de las comisiones de anticorrupción, de participación ciudadana y de justicia relativo al formato y metodología para la evaluación de los candidatos a ocupar el cargo de comisionado del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Disponible en: https://bit.ly/2NVe4vP

247 Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos.

escalonada.[248] Como se puede observar, para los órganos estatales la CPEUM no prevé un procedimiento específico, como en el caso del Instituto, y se limita a delinear las bases para la selección de comisionados. Por ejemplo, se establece que se conformará con un número impar de integrantes, dejándole a los órganos estatales autonomía sobre cuántos deben de ser.

Aunque con variantes, en general, estos ordenamientos siguen el ejemplo de la CPEUM, pero reducen el número de comisionados a tres o cinco.

De conformidad con el artículo 38 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en la designación de los comisionados (tanto los de INAI, como lo de los órganos estatales) se debe privilegiar aquellos que cuenten con experiencia en materia de acceso a la información pública o protección de datos personales. Este dispositivo busca dar contenido material al principio de especialización establecido en la CPEUM. Junto con lo anterior, la especialización permite que los comisionados puedan realizar sus funciones de manera individual, sin tener que recurrir al conocimiento experto de terceros.[249]

Finalmente, los comisionados, tanto del INAI como de los estados, solo pueden ser removidos de su cargo en los términos del título cuarto de la CPEUM y serán sujetos de juicio político.[250] Este procedimiento constituye otro mecanismo orientado a garantizar su independencia e imparcialidad.

La CPEUM establece que el comisionado presidente del INAI será designado por los propios comisionados mediante voto secreto, por un periodo de tres años y con posibilidad de ser reelecto por un periodo igual. Este tendrá la responsabilidad de representar legalmente al INAI, de presidir el Pleno y estará obligado a rendir un informe anual ante el Senado.[251] El mecanismo de designación entre pares es de nuevo una garantía de la autonomía e independencia del INAI, pues limita la injerencia de otros poderes en la conducción de la institución.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), además de las facultades que los comisionados del INAI ejercen como órgano colegiado, les otorga atribuciones individuales, como son: 1) someter, participar, proporcionar información y votar asuntos en el Pleno; 2) participar en foros, reuniones, eventos, convenciones y congresos de temas que les competen; 3) remover y nombrar al personal que tienen asignado; 4) solicitar información a las unidades correspondientes sobre el estado de los asuntos; 5) solicitar al comisionado presidente la solicitud de recursos para ejercer sus funciones; 6) coadyuvar en la integración del programa anual y los informes y 7) excusarse de conocer asuntos en los que exista conflicto de interés.[252]

En síntesis, los requisitos, procedimientos y facultades de los comisionados están diseñados para garantizar que puedan ejercer sus funciones de manera autónoma, experta e independiente.

248 Artículo 38 de la Ley General de Transparencia y Acceso a la Información Pública.

249 Ugalde, F. (2010). "Órganos constitucionales autónomos". *Revista del Instituto de la Judicatura Federal Escuela Judicial*. No. 29. UNAM. Disponible en: https://revistas-colaboracion.juridicas.unam.mx/index.php/judicatura/article/view/32280/29277. Fecha de consulta: 5 de junio 2019.

250 Artículo 39 de la Ley General de Transparencia y Acceso a la Información Pública.

251 Artículo 30 de la Ley Federal de Transparencia y Acceso a la Información Pública.

252 Artículo 29 de la Ley Federal de Transparencia y Acceso a la Información Pública.

Comité de transparencia

María Marván Laborde

El comité de transparencia es un órgano colegiado, integrado por un número impar de servidores públicos que se formará de manera obligatoria al interior de cada sujeto obligado de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). Al igual que con los órganos garantes, el comité desarrollará, de manera concomitante, las funciones propias del acceso a la información y de la protección de datos personales.

En materia de acceso a la información, los comités tienen como función principal determinar la clasificación de la información de su propia institución para poder desempeñar sus funciones. La ley establece que todos los miembros del comité podrán tener acceso a la información que van a clasificar. En razón de lo anterior, los miembros del comité deberán guardar el debido sigilo sobre la información reservada ya que son responsables de la secrecía que amerita el manejo de la información reservada y la información confidencial que incluye a los datos personales.

Para el buen funcionamiento de los comités de transparencia, la LGTAIP establece que sus miembros no podrán depender jerárquicamente entre sí y nunca podrá alguno de los miembros tener una doble representación.

Con base en el artículo 6 constitucional, la interpretación de estas leyes siempre deberá favorecer la publicidad de la información gubernamental, en razón de ello este cuerpo colegiado debe ser, antes que nada, un cuerpo deliberativo que determine las reservas solo cuando se consideren indispensables y siempre con estricto apego a derecho y partiendo de la lógica de máxima publicidad.

La ley establece que el número de sus integrantes sea impar con el propósito de evitar que las votaciones queden empatadas cuando, debido a una ausencia temporal, se produzca un empate, la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) le concede al presidente del comité voto de calidad. El comité de transparencia revisa la clasificación de la información que haya hecho la unidad administrativa responsable de la información solicitada.

Cuando el comité lo juzgue pertinente podrán llamar como invitados a los responsables de la información que pretenden clasificar con el fin de escuchar sus puntos de vista y determinar, a través de la deliberación y la votación, si se justifica o no la reserva. Los invitados participarán con voz pero sin voto.

Entre las funciones del comité de transparencia se encuentra la de garantizar la gestión administrativa de las solicitudes de información, pues es clave para el buen funcionamiento del acceso a la información y la protección de datos personales. Los miembros del comité necesitan conocer su institución y el aparato normativo (las tres leyes mencionadas en este artículo y los lineamientos, reglas, recomendaciones y criterios que de ellas se derivan), ya que son el primer cuerpo colegiado que debe deliberar para garantizar la entrega de la información pública y proteger el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).[253]

253 Derechos de acceso, rectificación, cancelación y oposición a que se refieren las leyes de protección de datos personales.

Los comités tienen la función (LGTAIP, art.44, fracción II) de "confirmar, modificar o revocar las determinaciones que, en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas de los sujetos obligados".

Cuando una institución recibe una solicitud, la unidad de transparencia debe turnarla a las áreas correspondientes donde hay servidores públicos habilitados para encontrar la información y ofrecer la respuesta. Cuando esta respuesta no favorece al solicitante por cualquier razón (inexistencia, incompetencia o reserva) debe ser revisada por el comité de transparencia.

La legislación anterior a la LGTAIP no obligaba al comité a revisar las ampliaciones de plazo, sin embargo, la experiencia demostró que en muchas ocasiones había dilaciones injustificadas. En caso de las declaraciones de inexistencia, clasificación de la información o incompetencia, los comités deben revisar que se justifique la respuesta ofrecida al solicitante y sobre todo, que esté debidamente fundamentada y motivada.

Otra novedad de la LGTAIP es que en los casos en los que la unidad administrativa declare la inexistencia de la información, pero que por sus facultades se determine a través de la deliberación del comité que dicha inexistencia es injustificada, pueden ordenarle generar esa información. Cuando el área acredite fehacientemente la imposibilidad de producir la información deberá de justificarlo para entregar al solicitante una respuesta debidamente fundada y motivada. (LGTAIP, artículo 44, fracción III).

Los comités son una de las muchas instancias señaladas por la ley para diseñar políticas públicas que garanticen cabalmente el acceso y la obtención de la información. Los comités también deberán promover la capacitación de los servidores públicos tanto en acceso a la información como en protección de datos personales.

Debido a que todos los miembros del comité están autorizados para ver la información susceptible de ser reservada, la LGTAIP exceptuó a las instancias de seguridad nacional de tener un comité. Caben dentro de esta excepción el Centro de Investigación y Seguridad Nacional; el Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia; el Centro Federal de Protección a Personas; la Dirección de Coordinación de Inteligencia de la Comisión Nacional de Seguridad; la Subprocuraduría Especializada en Investigación de Delincuencia Organizada; la Unidad de Inteligencia Financiera; el Estado Mayor Presidencial, el Estado Mayor de la Defensa Nacional, el Estado Mayor General de la Armada, la Autoridad Investigadora de la Comisión Federal de Competencia Económica y la del Instituto Federal de Telecomunicaciones (IFT). En todas estas instituciones, las decisiones correspondientes al comité deberá tomarlas el titular de la entidad administrativa. Huelga decir que no están exentas de cumplir con las disposiciones y principios de la ley, a saber, el principio de máxima publicidad y la obligación de fundamentar y motivar las respuestas conforme a derecho. Las reservas aprobadas por el titular deberán justificar el probable daño causado a la nación si la información solicitada se hiciese pública.

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) añade en su artículo 84 las siguientes funciones a los comités de transparencia: asegurarse de garantizar efectivamente este derecho a los particulares, hacerse responsable de instituir los procedimientos internos que sean necesarios para la gestión de las solicitudes hechas por los particulares para el ejercicio de los derechos ARCO, al igual que en materia de transparencia podrá confirmar, modificar o revocar las determinaciones de las unidades administrativas, cuando se declare la inexistencia o se niegue el ejercicio de sus derechos a quién lo haya solicitado, recae sobre los comités la obligación de supervisar

a todas las áreas de la dependencia o entidad el cumplimiento de las medidas de control y acciones previstas en los documentos de seguridad para la mejor protección de las bases de datos personales, dar seguimiento a las resoluciones del Instituto y de los órganos garantes y se reitera su obligación de establecer programas de capacitación en la materia y en caso necesario, deberá dar vista al órgano interno de control cuando tenga conocimiento de presuntas irregularidades en el tratamiento de los datos personales.

Para establecer un marco de exigencia mayor, los Lineamientos Generales de Protección de Datos Personales para el Sector Público establecen que la negativa de atención de derechos ARCO deberá notificarse al comité de transparencia (artículo 105).[254]

Cómputo en la nube

Isabel Davara Fernández de Marcos,[255]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El cómputo en la nube, también conocido por su denominación en inglés *"cloud computing"* se refiere, entre otras cosas, al almacenamiento y tratamiento de información —no solo personal— mediante una serie de tecnologías y modelos de servicio que se centran en el uso de internet y la prestación de aplicaciones informáticas, capacidad de tratamiento, espacio de memoria y almacenamiento.[256]

El cómputo en la nube ha sido definido de diversas formas, sin embargo, una de las definiciones que gozan de mayor aceptación en la práctica es la proporcionada por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés) que ha definido al cómputo en la nube[257] de la siguiente forma:

> El cómputo en la nube es un modelo que permite el acceso ubicuo, conveniente y bajo demanda de red a un conjunto de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que puedan ser rápidamente proveídos con esfuerzos mínimos de administración o interacción con el proveedor de servicios. Este modelo en la nube promueve la disponibilidad y se compone de cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación.[258]

En la práctica, el cómputo en la nube se concibe como una nueva forma de prestación de los servicios de tratamiento de la información, válida tanto para una empresa como para un particular y, también, para la administración pública.[259] Por lo tanto, la expresión

254 Véase: http://inicio.ifai.org.mx/AcuerdosDelPleno/ACT-PUB-19-12-2017.10.pdf

255 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

256 Grupo de Trabajo del Artículo 29, WP 196, Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012.

257 "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models." Extraído de: Mell, P. y Grance T. (2011, septiembre). The NIST Definition of Cloud Computing. NIST. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-145/final

258 Ver Téllez, J. (2013). *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México*. México. Universidad Nacional Autónoma de México-Instituto de Investigaciones Jurídicas. Recuperado de: https://www.microsoftmexicopoliticaspublicas.com/docs/c-julio-tellez-lex-cloud-computing.pdf

259 Agencia Española de Protección de Datos. (2013). *Guía para clientes que contraten servicios de cloud computing*. España. Disponible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf Fecha de consulta: 4 de septiembre de 2018.

"cómputo en la nube" involucra una amplia gama de servicios que van desde sistemas de tratamiento virtual (que sustituyen o trabajan junto con servidores convencionales bajo el control directo del responsable del tratamiento) hasta servicios de apoyo al desarrollo de aplicaciones avanzadas y alojamiento avanzado, o hasta programas informáticos basados en la web que pueden sustituir a las aplicaciones instaladas convencionalmente en las computadoras personales de los usuarios finales.[260]

Es decir, los servicios de cómputo en la nube ofrecen acceso a las organizaciones a un amplio rango de tecnologías y modelos de servicios típicamente entregados a través de internet, siendo por tanto esencial en el concepto el acceso a recursos de cómputo bajo demanda a través de una red.[261]

En cuanto a su definición normativa, conviene precisar que la normatividad de protección de datos personales en México —tanto para el sector privado como para el público— ha sido pionera en la definición de lo que se denomina cómputo en la nube. En primer lugar, fue el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) el que aportó, en el año 2011, la primera definición de cómputo en la nube al indicar en su artículo 52 lo siguiente:

> Para fines del presente RLFPDPPP, por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o *software,* que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.

La definición anterior es un referente normativo importante en la protección de datos personales y retoma aspectos relacionados con la definición elaborada por el NIST como son la provisión de servicios bajo demanda mediante la facilitación de diversos modelos de servicio (infraestructura, plataforma o *software*).

Por otra parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) del 26 de enero de 2017 en la fracción VI de su artículo 3 definiría al cómputo en la nube de una forma bastante cercana a lo que hizo el RLFPDPPP al establecer lo siguiente:

> VI. Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente.

Del contenido de las definiciones normativas anteriores se puede entender que el cómputo en la nube hace referencia a un esquema de presentación de servicios bajo demanda que puede implicar la facilitación de servicios de infraestructura, plataforma o software, distribuidos de forma flexible mediante procedimientos virtuales, en recursos compartidos dinámicamente.

El cómputo en la nube —bajo cualquiera de sus modalidades de servicio— representa una nueva forma de utilizar las tecnologías de la información y las comunicaciones que se basa en el empleo de técnicas ya existentes, pero de una forma innovadora y, sobre todo, a una nueva escala.[262] La gran magnitud a la que se prestan es una de las características que los distingue de otros modelos de provisión de servicios ya que es a través de éstos que se permite el uso de recursos de *hardware, software,* almacenamiento, y comunicacio-

260 Grupo de Trabajo del Artículo 29, WP 196, Dictamen 05/2012 sobre la computación en nube, adoptado el 1 de julio de 2012.

261 ICO. (2012). *Guidance on the use of cloud computing*. Reino Unido. Disponible en: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf Fecha de consulta: 4 de septiembre de 2018.

262 Agencia Española de Protección de Datos. (2013). *Guía para clientes que contraten servicios de cloud computing*. España. Disponible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf Fecha de consulta: 4 de septiembre de 2018.

nes geográficamente distribuidos y a los que se accede de forma dinámica por internet y en ocasiones mediante el pago de una contraprestación, facilitando así un servicio bajo demanda.[263]

1. Características esenciales

El cómputo en la nube es un modelo de provisión de servicios con características particulares. El NIST[264] indica que sus características esenciales son las siguientes:

a) Autoservicio por demanda: un consumidor puede abastecerse unilateralmente de capacidades de computación, como tiempo de servidor y almacenamiento en red, según sus necesidades de forma automática, sin requerir la interacción humana con cada proveedor de servicios.[265]

b) Acceso amplio desde la red: las capacidades están disponibles sobre la red y se accede a ellas a través de mecanismos estándar que promueven el uso de plataformas heterogéneas tanto pesadas como ligeras (por ejemplo, teléfonos móviles, computadoras portátiles y otros dispositivos).

c) Reservas de recursos en común: los recursos computacionales del proveedor proponen servir en común a varios usuarios que utilicen un modelo de multiposesión (*multi-tenant model*), con diferentes recursos físicos y virtuales dinámicos y reasignados de acuerdo con la demanda de los consumidores.

d) Rápida elasticidad: las capacidades pueden suministrarse de manera rápida y elástica (en algunos casos de manera automática) para poder hacer un reajuste de forma. En cuanto al consumidor, las capacidades disponibles para abastecerse a menudo aparecen ilimitadas y se pueden adquirir en cualquier cantidad y en momento.

e) Servicio medido: los sistemas de nube controlan y optimizan el uso de los recursos de manera automática utilizando una capacidad de medición en un cierto nivel de abstracción adecuado para el tipo de servicio (por ejemplo, almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de recursos puede ser monitoreado, controlado y reportado, de esta manera suministra transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

En cuanto a las ventajas de este modelo de prestación de servicios, cabe citar que permite al usuario optimizar la asignación y el coste de los recursos asociados a sus necesidades de tratamiento de información, de forma tal que el usuario no tiene necesidad de realizar inversiones en infraestructura sino que utiliza la que pone a su disposición el prestador del servicio, quien garantiza que no se generarán situaciones de falta o exceso de recursos, así como el sobrecoste asociado a dichas situaciones.[266]

No obstante, pueden existir dificultades derivadas del uso de este tipo de servicios, entre ellas, la garantía de los derechos de privacidad por parte de los terceros proveedores de

263 AEPD. (2013). *Guía para clientes que contraten servicios de cloud computing*. España. Disponible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf

264 Mell, P. y Grance, Tim. (2011, septiembre). *The NIST Definition of Cloud Computing*. NIST. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-145/final

265 La relación que aquí se presenta de de características esenciales se encuentra en el texto Téllez, J. (2013). Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México. México. Universidad Nacional Autónoma de México-Instituto de Investigaciones Jurídicas, p. 7. Disponible en: https://www.microsoftmexicopoliticaspublicas.com/docs/c-julio-tellez-lex-cloud-computing.pdf

266 AEPD. (2013). *Guía para clientes que contraten servicios de cloud computing*. España. Disponible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf

este servicio, la determinación de la jurisdicción aplicable, la disponibilidad de la información y la falta de control de los recursos, aunque no son las únicas.

2. Modelos de servicio

Según el NIST[267] el cómputo en la nube puede tener los siguientes modelos de servicio:

a) Software como servicio *(software as a service o "SaaS")*: se proporciona al consumidor la capacidad de usar las aplicaciones suministradas por el proveedor que se ejecutan en una infraestructura de la nube mediante una interfaz que muestra la aplicación desde los distintos dispositivos del cliente. El consumidor no gestiona la infraestructura de la nube subyacente que incluye la red, servidores, sistemas operativos, almacenamiento o incluso capacidades de aplicaciones individuales —con la posible excepción de unos parámetros de configuración de la aplicación específica del usuario.[268]

b) Plataforma como servicio *(plataform as a service o "PaaS")*: en la plataforma como servicio, la capacidad proporcionada al consumidor es para desplegar en la infraestructura de la nube las aplicaciones adquiridas o creadas por el consumidor, utilizando lenguajes y herramientas de programación soportadas por el proveedor. En ese tipo de modelo, según el NIST, el consumidor no administra ni controla la infraestructura de la nube subyacente que incluye la red, servidores, sistemas operativos o de almacenamiento, pero tiene el control sobre las aplicaciones desplegadas y la posibilidad de controlar las configuraciones de entorno del *hosting* de aplicaciones.[269]

c) Infraestructura como servicio *(infrastructure as a service o "IaaS")*: en la infraestructura como servicio se suministra al consumidor la capacidad de procesamiento, almacenamiento, redes y otros recursos computacionales fundamentales, de tal forma que el consumidor puede desplegar y ejecutar el *software* de su elección, el cual puede incluir sistemas operativos y aplicaciones. El consumidor no administra la infraestructura de la nube subyacente, pero tiene control sobre los sistemas operativos, almacenamiento, aplicaciones desplegadas y la posibilidad de tener un control limitado de los componentes de la red seleccionados (por ejemplo, hospedar *firewalls*).[270]

3. Modelos de despliegue

Se pueden dar diversas modalidades de implementación,[271] entre las cuales se suele encontrar las siguientes:

a) Nube Privada: la infraestructura de cómputo en la nube puede ser administrada por la organización o por un tercero —de manera local o no. Los servicios relacionados con

267 Cfr., Peter Mell y Tim Grance, "The NIST Definition of Cloud Computing", https://csrc.nist.gov/publications/detail/sp/800-145/final

268 Téllez, J. (2013). *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México*. México. Universidad Nacional Autónoma de México-Instituto de Investigaciones Jurídicas, p. 7.

269 Téllez, J. (2013). *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México*. México. Universidad Nacional Autónoma de México-Instituto de Investigaciones Jurídicas, p. 7. Disponible en: https://www.microsoftmexicopoliticas-publicas.com/docs/c-julio-tellez-lex-cloud-computing.pdf

270 Téllez, J. (2013). *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México*. México. Universidad Nacional Autónoma de México-Instituto de Investigaciones Jurídicas, p. 7. Disponible en: https://www.microsoftmexicopoliticas-publicas.com/docs/c-julio-tellez-lex-cloud-computing.pdf

271 Para realizar la distinción entre los modelos de despliegue de cómputo en la nube, nuevamente se toman como referencia las aportaciones del NIST. Ídem.

esta modalidad de servicio se presentan cuando una entidad realiza la gestión y administración de sus servicios de cómputo en la nube para las partes que la forman, sin que en la misma puedan participar entidades externas y mantiene el control sobre ella.[272]

b) Nube comunitaria: la infraestructura de cómputo en la nube es compartida por diversas organizaciones y apoya a una comunidad específica que ha compartido sus preocupaciones y puede ser administrada por éstas o por terceros, ya sea de forma local o no.

c) Nube pública: la infraestructura de nube es provisionada para el uso de comunidades específicas de consumidores de distintas organizaciones que tienen objetivos compartidos. Puede ser administrada, operada y pertenecer a una o más organizaciones en la comunidad, por terceras partes o una combinación de las anteriores. En este tipo de servicios, el proveedor proporciona sus recursos de forma abierta a entidades heterogéneas, sin más relación entre sí que el contrato con el mismo proveedor de servicio.[273]

d) Nube híbrida: en este tipo de modelo, la infraestructura de cómputo en la nube es una composición de dos o más nubes (privadas, comunitarias y/o públicas) que permanecen como entidades únicas pero que están unidas por tecnología estandarizada o por tecnología propietaria[274] que permite la portabilidad de datos y aplicaciones.

De forma adicional, se suelen encontrar en esta categoría las denominadas nubes privadas virtuales. Esto ocurre cuando se implementan garantías adicionales de seguridad sobre nubes públicas.[275]

4. Figura del encargado del tratamiento y cómputo en la nube

El proveedor de servicios de cómputo en la nube es, en términos de la legislación nacional en materia de protección de datos personales, un encargado del tratamiento,[276] es decir, sin perjuicio de remitirnos a la definición del mismo presente en esta obra, un tercero que trata datos personales por cuenta del responsable como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Así lo especifica el artículo 52 del RLFPDPPP, los artículos 63 y 64 de la LGPDPPSO y el 111 de los Lineamientos Generales.

De manera general, el proveedor de servicios de cómputo en la nube asumirá en consecuencia las obligaciones aplicables al encargado del tratamiento y que están previstas, tanto en la normatividad del sector público[277] como en aquella del sector privado, dependiendo del ámbito en el que nos encontremos.[278]

272 Agencia Española de Protección de Datos (AEPD). (2013). *Guía para clientes que contraten servicios de cloud computing*. España. Disponible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf Fecha de consulta: 4 de septiembre de 2018.

273 AEPD. (2013). *Guía para clientes que contraten servicios de cloud computing*. España. Disponible en: https://www.aepd.es/media/guias/guia-cloud-prestadores.pdf Fecha de consulta: 4 de septiembre de 2018.

274 La tecnología propietaria (*proprietary technology*) es aquel tipo de tecnología desarrollada por una empresa, la cual la mantiene para su uso restringido, privado o privativo mientras que la tecnología abierta (*open technology*) es aquella disponible en el mercado para las empresas. Cfr., Fernández del Hoyo, A. (2013). *Innovación y gestión de nuevos productos*. Madrid. Pirámide, p. 463.

275 Agencia Española de Protección de Datos. (2013). *Op. cit*.

276 Artículo 111 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

277 Véase el artículo 59 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

278 Véase, entre otros, el artículo 50 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Asimismo, en el supuesto de incumplimiento a las instrucciones del responsable (según se dispone en el artículo 53 del RLFPDPPP y en el artículo 60 de la LGPDPPSO) podrá considerarse al proveedor de servicios de cómputo en la nube responsable ilícito del tratamiento y en consecuencia asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.

5. Condiciones para el tratamiento de datos personales en cómputo en la nube

La normatividad nacional en materia de protección de datos personales ha sido pionera en el desarrollo de obligaciones específicas para los proveedores de servicios en cómputo en la nube, de tal suerte que, con la emisión del RLFPDPPP el 21 de diciembre de 2011 se establecieron las obligaciones que el responsable deberá cumplir de forma previa a la contratación de servicios, aplicaciones e infraestructura en cómputo en la nube.

El artículo 52 del RLFPDPPP precisó que, de forma previa a la adhesión y/o contratación de servicios que impliquen el tratamiento de datos personales en el denominado cómputo en la nube por parte del responsable, éste deberá verificar que los terceros que faciliten dicho servicio cumplan con obligaciones específicas y cuenten con determinados mecanismos para garantizar la protección de los datos y, en consecuencia, con el cumplimiento del principio de responsabilidad respecto de la obligación de tutelar que el encargado realice un tratamiento conforme a lo que dispone la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

En particular, la fracción I del citado artículo 52 del RLFPDPPP indica que el responsable que contrate o se adhiera a servicios de cómputo en la nube podrá contratarlos siempre que el proveedor de los mismos cumpla con las siguientes condiciones:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la LFPDPPP y el RLFPDPPP.
b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio.
c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio.
d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.

La fracción II del citado artículo 52 refiere, además, que se deberá comprobar que el tercero que proporcione estos servicios al responsable cuenta con mecanismos para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta.
b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio.
c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio.
d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos.
e) Impedir el acceso a datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En el último párrafo del citado artículo 52 del RLFPDPPP se puntualiza, además, que el responsable no podrá adherirse a servicios que no garanticen la debida protección de datos personales.

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) dispone en su artículo 63 (con una redacción bastante similar a la prevista por el RLFPDPPP) lo siguiente:

> El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.
>
> En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.

En este mismo orden de ideas, el artículo 64 de la LGPDPPSO precisa, en idénticos términos a los de las fracciones I y II artículo 52 del RLFPDPPP, la obligación del responsable de adherirse a servicios, aplicaciones e infraestructura de cómputo en la nube que garanticen condiciones y mecanismos adecuados para la protección de datos personales.

> Artículo 64. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, solo podrá utilizar aquellos servicios en los que el proveedor:
>
> I. Cumpla, al menos, con lo siguiente:
>
> a) tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;
>
> b) transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
>
> c) abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y
>
> d) guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio.
>
> II. Cuente con mecanismos, al menos, para:
>
> a) dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
>
> b) permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
>
> c) establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;
>
> d) garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, y
>
> e) impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.
>
> En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la presente Ley y demás disposiciones que resulten aplicables en la materia.

Además, el artículo 111[279] de los Lineamientos Generales previene que el cumplimiento de lo previsto por los artículos 63 y 64 de la LGPDPPSO con relación a la contratación de servicios

279 Artículo 111 de los Lineamientos Generales de Protección de Datos personales para el Sector Público.

de cómputo en la nube y otras materias afines deberá prever, en el instrumento contractual que firme con el proveedor de servicios, al menos las cláusulas generales a que se refieren los artículos 59 de la LGPDPPSO[280] y 109 de los referidos Lineamientos Generales.[281]

También en la esfera pública, la Ley General de Archivos regula la provisión de servicios de cómputo en la nube en su artículo 62 y dispone que los sujetos obligados podrán gestionar los documentos de archivo electrónicos —no solo información personal— en un servicio de nube y que este servicio deberá permitir:

a) Establecer las condiciones de uso concretas en cuanto a la gestión de los documentos y responsabilidad sobre los sistemas.
b) Establecer altos controles de seguridad y privacidad de la información conforme a la normatividad mexicana aplicable y los estándares internacionales.
c) Conocer la ubicación de los servidores y de la información.
d) Establecer las condiciones de uso de la información de acuerdo con la normativa vigente.
e) Utilizar infraestructura de uso y acceso privado, bajo el control de personal autorizado.
f) Custodiar la información sensible y mitigar los riesgos de seguridad mediante políticas de seguridad de la información.
g) Establecer el uso de estándares y de adaptación a normas de calidad para gestionar los documentos de archivo electrónicos.
h) Posibilitar la interoperabilidad con aplicaciones y sistemas internos, intranets, portales electrónicos y otras redes.
i) Reflejar en el sistema, de manera coherente y auditable, la política de gestión documental de los sujetos obligados.

En definitiva, cuando el servicio de cómputo en la nube involucra el tratamiento de datos personales, tanto en el ámbito privado como en el público habrá que atender a lo siguiente:

a) El prestador de servicios de cómputo en la nube será considerado encargado del tratamiento conforme a la definición prevista en la normatividad.
b) El responsable del tratamiento solo podrá escoger encargados que cumplan con las condiciones exigidas por la normatividad, entre ellas:

   I. Contrato que especifique el alcance del encargado concedido.

   II. Sujeción a la legislación mexicana y a la competencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como autoridad de acuerdo con lo previsto por el artículo 4 del RLFPDPPP.

   III. Seguimiento de las instrucciones del responsable.

   IV. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

   V. Establecimiento de medidas de seguridad físicas, técnicas y administrativas para garantizar la protección de los datos.

   VI. Guardar confidencialidad respecto de los datos personales tratados.

   VII. Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación o cuando así lo requiera la autoridad competente.

280 Artículo 59 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

281 Artículo 109 de los Lineamientos Generales de Protección de Datos personales para el Sector Público.

c) Si el prestador de servicios de cómputo en la nube (o cualquier otro encargado del tratamiento) incumple las instrucciones, será considerado responsable del tratamiento y responderá como tal de conformidad con las disposiciones legalmente aplicables para tal efecto.

Comunicaciones privadas

José Soto Galindo

Las comunicaciones privadas son el intercambio de informaciones, opiniones o datos entre dos o más personas en una interlocución con carácter confidencial o privado. Las comunicaciones privadas comprenden todo el proceso comunicativo, lo que incluye el contenido, los datos de tráfico de una comunicación (como la identidad de los interlocutores, el origen y el destino de las llamadas telefónicas, su duración y fecha) y la localización geográfica del aparato tecnológico utilizado para el acto comunicativo y vinculado a una persona determinada (véase geolocalización).

La privacidad de las comunicaciones está garantizada en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), que también impone barreras contra molestias, intromisiones o injerencias arbitrarias a la persona, la familia, el domicilio, los papeles, las posesiones y la correspondencia. Sin mencionarlo explícitamente como un derecho, los párrafos 12 y 13 del artículo 16 constitucional sugieren el deber de confidencialidad de las comunicaciones privadas, con excepción de cuando se trata de una intervención autorizada con fines de investigación judicial o cuando una de las partes la aporte voluntariamente:

> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.
>
> Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público (MP) de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando, además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Todas las formas existentes de comunicación —y las que resulten de la evolución tecnológica— están protegidas por el derecho a la inviolabilidad de las comunicaciones privadas. Los avances tecnológicos han permitido la multiplicación de soportes y formatos para documentar comunicaciones privadas, así que éstas abarcan el contenido de la correspondencia, las comunicaciones telefónicas alámbricas o inalámbricas, correos electrónicos, mensajería sincrónica (*chat*), en tiempo real o instantánea asincrónica, intercambio de archivos en línea, redes sociales en internet, informaciones en formato de texto, audio, video o fotografías.

La "Constitución no limita los medios a través de los cuales se puede producir la comunicación objeto de protección del derecho fundamental en estudio. Esto resulta acorde con la finalidad de la norma, que no es otra que la libertad de las comunicaciones, siendo que

ésta puede ser conculcada por cualquier medio o artificio técnico desarrollado a la luz de las nuevas tecnologías", según ha dictado la Suprema Corte de Justicia de la Nación (SCJN).

1. Relación con la vida privada

Las comunicaciones privadas pueden revelar aspectos íntimos o privados de sus participantes, por lo que las leyes garantizan su confidencialidad sin importar por cuál medio o sistema de comunicación, análogo o digital, fueron expresadas o manifestadas ni el soporte o formato en que se encuentren. Se trata de proteger la esfera de libertad más íntima de las personas, donde éstas pueden expresar libremente su identidad, ya sea en sus relaciones con los demás o en lo individual.

Las comunicaciones privadas pueden comprender, desde conversaciones sobre situaciones de la vida cotidiana hasta la manifestación sobre malestares de salud, problemas económicos u opiniones de cualquier índole que las personas quieran mantener en secreto o compartir solo con terceros de su confianza, además de los datos que identifican dicha comunicación en la red o sistema de comunicaciones donde se produjo y la geolocalización del equipo de comunicación utilizado.

La jurisprudencia en México relaciona las comunicaciones privadas con los derechos a la vida privada y a la intimidad, a la protección de datos personales, a la inviolabilidad del domicilio, a la autodeterminación informativa y de libertad de expresión. Las personas pueden "elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede utilizar esa información".[282]

El derecho a las comunicaciones privadas es una garantía formal, pues implica que todas las comunicaciones privadas están protegidas con independencia de su contenido: "No se necesita en modo alguno analizar el contenido de la comunicación, o de sus circunstancias, para determinar su protección por el derecho fundamental".[283]

2. Antecedentes

La primera ley que castigó la intervención de comunicaciones privadas, en su modalidad de correspondencia postal, fue instaurada en Prusia en 1794: "Quien abre la carta de otro sin su voluntad y sin un permiso especial enfrenta de 3 a 14 días de prisión", decía el artículo 1370 de las Leyes Generales para los Estados Prusianos. Se trató de un dispositivo jurídico diseñado e implementado en plena Ilustración, como una medida de defensa de los ciudadanos contra intromisiones e injerencias y arbitrarias de parte del Estado.

El régimen jurídico mexicano contempló por primera vez la protección de la confidencialidad de las comunicaciones privadas en la Constitución de 1857. El artículo 16, diseñado por el liberal Ponciano Arriaga Leija, preveía la intervención legal de las comunicaciones privadas solo en casos excepcionales, con un control de excepcionalidad de la medida y la exigencia de fundar y motivar por escrito su aplicación con la descripción del procedimiento y las manifestaciones de al menos un testigo:

> Todos los habitantes de la República, así en su persona y familias, como en su domicilio, papeles y posesiones, están a cubierto de todo atropellamiento, examen o cateo, embargo o secuestro de cualquier persona o cosa, excepto en los casos prefijados por las leyes y con las indispensables condi-

282 Tribunales Colegiados de Circuito. Novena época. Semanario Judicial de la Federación y su Gaceta. Tomo XXVIII, septiembre de 2008, Pág. 1253

283 Tribunales Colegiados de Circuito. Novena época. Semanario Judicial de la Federación y su Gaceta Tomo XXXIV, agosto de 2011, Pág. 221

ciones de que se procederá racionalmente y de que la autoridad competente exprese en su mandato escrito la causa probable del procedimiento, sostenida por la afirmación al menos de un testigo, y señale y describa el lugar que debe ser registrado o la cosa o persona que debe ser secuestrada.

La Constitución de 1917, resultado de la Revolución Mexicana, recuperó prácticamente la totalidad de la redacción original de Arriaga Leija sobre la inviolabilidad de las comunicaciones privadas hasta 1996, cuando se incluyeron dos nuevos párrafos al artículo 16 constitucional para actualizar la norma ante el avance de las tecnologías de la información y la comunicación.

3. Derecho internacional

En el derecho internacional, del que México forma parte, las comunicaciones privadas están protegidas por los siguientes dispositivos:

Artículo 12 de la Declaración Universal de Derechos Humanos de la Organización de las Naciones Unidas de 1948: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Artículo 17 fracción 1 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por los países miembros de la ONU en 1966: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación".

Artículo 11 fracción 2 de la Convención Interamericana sobre Derechos Humanos, también conocida como el Pacto de San José, suscrita por los integrantes de la Organización de los Estados Americanos (OEA) en 1969: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación".

La relación del derecho a mantener comunicaciones privadas se relaciona también con la libertad de expresión, en tanto que la intromisión o injerencia por terceros puede tener efectos intimidatorios contra "la libre expresión del pensamiento, búsqueda y difusión de información en los países de la región", como expresó la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, emitida en 2013 por el Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. "La vulneración de la privacidad de las comunicaciones tiene un efecto inhibitorio y afecta el pleno ejercicio del derecho a comunicarse", advierte la declaración de la ONU y la OEA.

Conciliación dentro del Procedimiento de Protección de Derechos

Isabel Davara Fernández de Marcos,[284]
Gregorio Barco Vega y
Alexis Cervantes Padilla

Es un medio alternativo de solución de controversias en virtud del cual el titular de los datos personales y el responsable del tratamiento, en presencia del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) o un organismo garante, dirimen un conflicto jurídico derivado de la interposición por parte de un titular de una solicitud de protección de derechos.[285]

La conciliación está regulada en la normatividad de datos personales, en específico, dentro de las disposiciones que regulan el Procedimiento de Protección de Derechos (PPD) y la atención de un recurso de revisión (RR).[286] Es decir, no es una vía independiente y tampoco se presenta en todos los procedimientos regulados en la normatividad.

En este sentido, podemos afirmar que la figura de la conciliación se presenta dentro de dos procedimientos específicos: el PPD, regulado en la normatividad del sector privado, y el recurso de revisión RR, regulado en la normatividad de datos personales de sector público.

La conciliación es una figura de gran relevancia en la normatividad de datos personales, ya que en caso de que las partes lleguen a un acuerdo, dicho acuerdo tendrá efectos vinculantes, lo que significa que lo acordado entre las partes será de observancia obligatoria para cada una de ellas. En caso de que las partes logren conciliar, el procedimiento del cual traiga a causa la conciliación se dará por terminado mediante una resolución que concrete el sobreseimiento por haber quedado sin materia.

1. Conciliación dentro del PPD

La conciliación resulta procedente una vez que es admitida la solicitud de protección de datos[287] interpuesta por el titular ante la Dirección General de Protección de Derechos y Sanción (DGPDS) del INAI. Es decir, la conciliación forma parte del PPD y se da como una alternativa procesal para dirimir la *litis* objeto del procedimiento.[288]

---

284 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

285 En este sentido deben tenerse en consideración los supuestos de procedencia del PPD (artículo 45 de la LFPDPPP y 19 de los Lineamientos de los Procedimientos) y del RR que, aunque son coincidentes en aspectos relativos al ejercicio ARCO, en el RR se señalan supuestos mucho más específicos para la procedencia de éste (artículo 104 de la LGPDPPSO).

286 Sobre este tema se puede consultar en el volumen 4 de las *Guías para Titulares de Datos Personales* publicadas por el INAI el texto "Procedimientos de datos personales ante el INAI". Disponible en: http://inicio.ifai.org.mx/Guias/Guia%20Titulares-04_PDF.pdf

287 *Vid* definición de "solicitud de protección de datos dentro del procedimiento de protección de derechos" en este diccionario.

288 En este sentido, conviene precisar los supuestos de procedencia del PPD, mismos que se señalan con claridad en el artículo 19 de los Lineamientos de los Procedimientos:
"El Procedimiento de Protección de Derechos procederá cuando exista una inconformidad por parte del Titular, derivada de acciones u omisiones del responsable con motivo del ejercicio de los derechos ARCO cuando:
I. El Titular no haya recibido respuesta por parte del responsable;
II. El Responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
III. El Responsable se niegue a efectuar las rectificaciones a los datos personales;
IV. El Titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;
V. El responsable se niegue a cancelar los datos personales;
VI. El Responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición
VII. El Responsable se niegue a atender la solicitud de oposición, y
VIII. Por otras causas que a juicio del Instituto sean procedentes conforme a la Ley o al Reglamento.

Respecto del momento procesal en que debe concretarse la conciliación, el artículo 54 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el artículo 25 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de los Procedimientos)[289] disponen que la misma podrá presentarse en cualquier momento dentro del PPD.[290]

Las reglas específicas que regulan la figura de la conciliación en la normatividad de datos personales aplicables al sector privado pueden encontrarse en el artículo 120 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP),[291] el cual, entre otras cosas, señala lo siguiente:

A. El INAI requerirá a las partes en el acuerdo de admisión[292] de la solicitud de protección de derechos para que en un plazo no mayor a 10 días manifiesten su voluntad de conciliar.[293]

B. La conciliación podrá celebrarse de forma presencial (con la presencia física del titular y el responsable), por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el INAI siempre que sea posible acreditar su existencia.[294]

C. Dentro de los veinte días siguientes en que se haya recibido la manifestación de las partes para conciliar, el INAI señalará el lugar o medio, día y hora para la celebración de la audiencia de conciliación. Dentro de esta etapa, se deberán de observar las siguientes formalidades:

   I. En un plazo máximo de cinco días el conciliador podrá requerir a las partes que presenten los elementos de convicción que estime necesarios para la conciliación.[295]

   II. La audiencia de conciliación podrá suspenderse hasta en dos ocasiones cuando el conciliador lo juzgue pertinente o a instancia de ambas partes. En el supuesto de que se decrete la suspensión de la audiencia de conciliación, se deberá señalar día y hora para su reanudación.[296]

---

289 Artículo 25. "El Instituto podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos o su representante y el responsable".

290 Artículo 54.- El Instituto podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable.

291 No obstante, el último párrafo del artículo 120 del RLFPDPP indica que, la previsión del procedimiento de conciliación ahí previsto no obsta para que, en términos del artículo 54 de la LFPDPPP, el INAI pueda buscar la conciliación en cualquier momento del PPD.

292 Al respecto detalla la fracción I del artículo 120 del RLFPDPPP que el acuerdo de admisión contendrá un resumen de la solicitud de protección de datos personales y de la respuesta del responsable si la hubiere, señalando los elementos comunes y los puntos de controversia.

293 No obstante lo anterior, es importante notar que el referido artículo 120 del RLFPDPPP señala que la conciliación no procederá cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con la LFPDPPP y el RLFPDPPP, salvo que cuente con representación legal debidamente acreditada.

294 En este mismo sentido se pronuncia el artículo 28 de los Lineamientos de los Procedimientos:
"La conciliación podrá celebrarse presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el Instituto".

295 El artículo 30 de los Lineamientos de los Procedimientos señala lo mismo:
"El conciliador, podrá requerir a las partes que presenten en un plazo máximo de cinco días hábiles, los elementos de convicción que estime necesarios para la conciliación".

296 En este contexto, los Lineamientos de los Procedimientos refieren:
"Artículo 31. El conciliador podrá suspender la audiencia hasta en dos ocasiones cuando lo estime pertinente o a instancia de ambas partes, en cuyo caso señalará día y hora para su reanudación".

III. En el supuesto de que la audiencia de conciliación tenga lugar, se deberá levantar el acta[297] en la que conste el resultado de la misma.[298]

D. La audiencia de conciliación podrá posponerse[299] en el supuesto de que alguna de las partes no acuda a la misma, pero justifique su ausencia en un plazo de tres días. En este caso, el INAI convocará a las partes una segunda audiencia de conciliación. En el supuesto de que la parte que justificó su ausencia no acuda a esta segunda audiencia de conciliación se continuará con la substanciación del PPD. Lo mismo sucederá cuando alguna de las partes se ausente de forma injustificada de la audiencia de conciliación.[300]

E. Una vez celebrada la audiencia de conciliación, si no existe acuerdo entre las partes, se continuará con la tramitación del PPD.

F. Cuando exista acuerdo de las partes en la audiencia de conciliación, el mismo se hará constar por escrito, tendrá efectos vinculantes y señalará el plazo de su cumplimiento.[301]

G. El PPD se dará por concluido cuando se hayan cumplido los compromisos previstos en el acuerdo derivado de la audiencia de conciliación entre las partes. No obstante, en el supuesto de que los acuerdos asumidos en la audiencia de conciliación no hayan sido observados, se reanudará el PPD.[302]

En definitiva, el acuerdo entre las partes de dirimir la controversia planteada por el titular de los datos personales a través de la conciliación tendrá como consecuencia la conclusión del procedimiento de protección de derechos instaurado en contra del responsable del tratamiento. Por obvias razones, la materialización de un acuerdo de conciliación entre las partes tendrá el efecto de suspender el plazo de 50 días previsto en el artículo 47 de la LFPDPPP[303] para que se dicte la resolución del PPD (artículo 120, último párrafo del RLFPDPPP y artículo 33, último párrafo, de los Lineamientos de los Procedimientos).[304]

297 Al respecto señala la fracción II del artículo 120 del RLFPDPPP que en caso de que el responsable o el titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa.

298 En este mismo sentido se pronuncia el artículo 29 de los Lineamientos de los Procedimientos:
"De toda audiencia de conciliación se levantará el acta respectiva, en la que conste el resultado de esta. En caso de que el Responsable o el Titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa".

299 "Audiencia:
Artículo 121. Para los efectos del penúltimo párrafo del artículo 45 de la Ley, el Instituto determinará, en su caso, el lugar o medio, fecha y hora para la celebración de la audiencia, la cual podrá posponerse solo por causa justificada. En dicha audiencia se desahogarán las pruebas que por su naturaleza así lo requieran y se levantará el acta correspondiente".

300 En este mismo sentido, los Lineamientos de los Procedimientos señalan lo siguiente:
"Artículo 32. Si alguna de las partes no acude a la audiencia y justifica su ausencia en un plazo de tres días hábiles, será convocado a una segunda audiencia; en caso de que no acuda a esta última, se continuará con el procedimiento. Cuando alguna de las partes no acuda a la audiencia de conciliación sin justificación alguna, se continuará con el procedimiento".

301 Nuevamente, encontramos los Lineamientos de los Procedimientos en un sentido idéntico prevén lo siguiente:
"Artículo 33. En caso de que en la audiencia se logre la conciliación, el acuerdo deberá constar por escrito y tendrá efectos vinculantes y señalará, en su caso, el plazo de su cumplimiento".

302 En este mismo contexto, los Lineamientos de los Procedimientos previenen:
"Artículo 34. De no existir acuerdo en la audiencia de conciliación, se continuará con el Procedimiento de Protección de Derechos emitiéndose el acuerdo correspondiente".

303 "Artículo 47. El plazo máximo para dictar la resolución en el procedimiento de protección de derechos será de cincuenta días, contados a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo".

304 "Artículo 33. En caso de que en la audiencia se logre la conciliación, el acuerdo deberá constar por escrito y tendrá efectos vinculantes y señalará, en su caso, el plazo de su cumplimiento.
El plazo al que se refiere el artículo 47 de la Ley será suspendido durante el periodo de cumplimiento del acuerdo de conciliación".

2. Conciliación dentro del RR

La conciliación, de acuerdo con lo previsto por el artículo 106 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[305] se presenta una vez admitido el RR,[306] ya sea por el INAI y/o los organismos garantes.[307]

La etapa de conciliación[308] prevista en la LGPDPPSO, de acuerdo con los Lineamientos de Protección de Datos Personales para el Sector Público (Lineamientos Generales) además de sujetarse a las reglas previstas en dicha norma, deberá observar los principios de voluntariedad, confidencialidad, neutralidad, imparcialidad, equidad, flexibilidad y economía.[309]

Respecto de la etapa conciliatoria del RR, la citada Ley General en su artículo 107 destaca las siguientes reglas específicas sobre su sustanciación:

---

305 "Artículo 106. Una vez admitido el recurso de revisión, el Instituto o, en su caso, los Organismos garantes podrán buscar una conciliación entre el titular y el responsable.
De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto, o en su caso, los Organismos garantes, deberán verificar el cumplimiento del acuerdo respectivo".

306 En relación con este tema, recomendamos la lectura de la voz de "Recurso de Revisión" que figura en esta obra como parte de los procedimientos de protección de datos personales aplicables al sector público.

307 La tramitación del RR obedece a los supuestos de procedencia identificados concretamente en el artículo 104 de la LGPDPPSO:
"El recurso de revisión procederá en los siguientes supuestos:
I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
II. Se declare la inexistencia de los datos personales;
III. Se declare la incompetencia por el responsable;
IV. Se entreguen datos personales incompletos;
V. Se entreguen datos personales que no correspondan con lo solicitado;
VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales;
VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia;
VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;
IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;
X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de estos;
XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y
XII. En los demás casos que dispongan las leyes".

308 De acuerdo con el contenido del párrafo tercero de la fracción I del artículo 107 de la LGPDPPSO "Queda exceptuado de la etapa de conciliación, cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con la Ley y el Reglamento, salvo que cuente con representación legal debidamente acreditada".
En este mismo sentido, los Lineamientos de Protección de Datos Personales disponen lo siguiente:
"Conciliación en recursos de revisión de menores de edad.
Artículo 145. De conformidad con el artículo 107, fracción I de la Ley General y el artículo anterior, la conciliación no será procedente cuando el titular sea menor de edad y se hubiere vulnerado alguno de los derechos contemplados en la Ley General de los Derechos de Niñas, Niños y Adolescentes vinculados con la Ley General, salvo que el menor cuente con representación legal debidamente acreditada".

309 "Etapa de conciliación
Artículo 144. El Comisionado ponente deberá promover, privilegiar y buscar la conciliación entre el titular y responsable. La etapa de conciliación solo será posible cuando el titular y el responsable acuerden someterse a dicho procedimiento, la cual, de acuerdo con el artículo 17, fracción I de la Ley General, podrá celebrarse por cualquiera de los siguientes medios:
I. Presencialmente
II. Por medios remotos o locales de comunicación electrónica, o
III. Cualquier otro medio que determine el Comisionado ponente.
En cualquiera de los medios señalados en las fracciones anteriores del presente artículo, el Comisionado ponente deberá dejar constancia de la existencia de la conciliación para efectos de acreditación.
En la etapa de conciliación deberán observarse los principios de voluntariedad, confidencialidad, neutralidad, imparcialidad, equidad, flexibilidad y economía".

A. En un plazo no mayor a siete días, contados a partir de la notificación del acuerdo de invitación a las partes para conciliar, la autoridad garante correspondiente requerirá a las partes que manifiesten su voluntad de conciliar por cualquier medio.[310] Esto quiere decir, que la conciliación puede celebrarse presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine la autoridad garante. En este sentido, los Lineamientos de Protección de Datos Personales añaden la precisión de que, cuando la audiencia de conciliación se realice por medios remotos, el conciliador hará del conocimiento de las partes que la misma será grabada por el medio que a juicio del conciliador se considere conveniente para el único efecto de acreditar su existencia.[311]

B. Dentro de los 10 días siguientes en que la autoridad garante correspondiente haya recibido la manifestación de la voluntad de conciliar de ambas partes, se procederá a señalar el lugar o medio, día y hora para la celebración de la audiencia de conciliación. Al respecto, el artículo 107 indica también que, durante la audiencia de conciliación, se podrá requerir a las partes que presenten en un plazo máximo de cinco días, los elementos de convicción que estime necesarios para la conciliación.[312]

C. La audiencia de conciliación podrá suspenderse por una sola ocasión cuando el conciliador lo estime pertinente o a instancia de ambas partes. En el supuesto de que ocurra la suspensión de la audiencia de conciliación, el conciliador señalará día y hora para su reanudación dentro de los cinco días siguientes.

D. El resultado de la audiencia de conciliación se hará constar a través de un acta de conciliación que, según el artículo 149 de los Lineamientos de Protección de Datos Personales, deberá de contener al menos los siguientes elementos:

- El número de expediente del recurso de revisión

310 El citado artículo 107 dispone lo siguiente:
"La conciliación podrá celebrarse presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el Instituto o los organismos garantes, según corresponda. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia".
En este mismo sentido, los Lineamientos de Protección de Datos Personales señalan:
"Etapa de conciliación
Artículo 144. El comisionado ponente deberá promover, privilegiar y buscar la conciliación entre el titular y responsable. La etapa de conciliación solo será posible cuando el titular y el responsable acuerden someterse a dicho procedimiento, la cual, de acuerdo con el artículo 17, fracción de la Ley General, podrá celebrarse por cualquiera de los siguientes medios:
I. Presencialmente
II. Por medios remotos o locales de comunicación electrónica, o
III. Cualquier otro medio que determine el Comisionado ponente.
En cualquiera de los medios señalados en las fracciones anteriores del presente artículo, el comisionado ponente deberá dejar constancia de la existencia de la conciliación para efectos de acreditación.
En la etapa de conciliación deberán observarse los principios de voluntariedad, confidencialidad, neutralidad, imparcialidad, equidad, flexibilidad y economía".

311 *Vid*, último párrafo del artículo 149 de los Lineamientos de Protección de Datos Personales.

312 En este sentido, el artículo 146 de los Lineamientos de Protección de Datos Personales indica lo siguiente:
"Audiencia de conciliación
Artículo 146. Aceptada la conciliación por el titular y el responsable, en términos del artículo 107 de la Ley General, el Comisionado ponente deberá emitir un acuerdo a través del cual señale el lugar o medio, día y hora para la celebración de la audiencia de conciliación y solicite a éstos los elementos de convicción que consideren pertinentes presentar durante el desarrollo de la audiencia, dentro de los tres días siguientes contados a partir del día siguiente que tenga conocimiento de que el titular y el responsable aceptan someterse a la etapa de conciliación.
La audiencia de conciliación deberá realizarse en un plazo máximo de diez días siguientes en que el Comisionado ponente recibió la manifestación de voluntad del titular y el responsable para conciliar.
La audiencia de conciliación podrá llevarse a cabo con el representante del titular, siempre y cuando, el titular haya manifestado su voluntad para tales efectos".

- El lugar, fecha y hora de celebración de la audiencia de conciliación
- Los fundamentos legales para llevar a cabo la audiencia
- El nombre completo del titular o su representante, ambos debidamente acreditados
- La denominación del responsable y el servidor público que haya designado como su representante, este último debidamente acreditado
- El nombre o los nombres de los servidores públicos del Instituto que asistieron a la audiencia de conciliación
- La manifestación de la voluntad del titular y responsables de dirimir sus controversias mediante la celebración de un acuerdo de conciliación
- La narración circunstanciada de los hechos ocurridos durante la audiencia de conciliación
- Los acuerdos adoptados por las partes, en su caso
- El plazo para el cumplimiento de los acuerdos, en su caso
- El nombre y firma de del conciliador, servidores públicos designados por el Comisionado ponente, titular o su representante, representante del responsable y de todas aquellas personas que intervinieron en la audiencia de conciliación

En relación con los requisitos del acta, tanto el artículo 107 de la LGPDPPSO como el artículo 149 de los Lineamientos Generales coinciden en que la falta de forma de la misma por parte del titular y/o su representante legal, no afecta la validez de la misma ni el carácter vinculante de los acuerdos adoptados en ella.

E. En el supuesto de que alguna de las partes no acuda a la audiencia de conciliación pero justifique su ausencia a la misma en un plazo de tres días, se procederá a convocar a una segunda audiencia de conciliación, en el plazo de cinco días.[313] Por otro lado, de acuerdo con el referido artículo 107, cuando la persona que haya solicitado que se difiera la audiencia, no acuda a esta última, se continuará con el RR.[314] Lo mismo sucederá cuando alguna de las partes no acuda a la audiencia de conciliación sin justificación alguna.

F. En el supuesto de que las partes no hayan alcanzado un acuerdo en la etapa de conciliación se procederá a continuar con la sustanciación del RR.

G. Cuando exista acuerdo de las partes en la audiencia de conciliación, el mismo se hará constar por escrito, tendrá efectos vinculantes y señalará el plazo de su cumplimiento.[315] Respecto del cumplimiento del acuerdo de conciliación se debe destacar que

313 En este sentido, el artículo 147 de los Lineamientos de Protección de Datos Personales precisa:
"Ausencia de alguna de las partes a la audiencia de conciliación con justificación
Artículo 147. De conformidad con el artículo 107, fracción III de la Ley General, si el titular o el responsable no acuden a la audiencia de conciliación y justifican su ausencia dentro de los tres días, contados a partir del día siguiente de la fecha señalada para la celebración de la audiencia de conciliación, serán convocados por el Comisionado ponente a una segunda audiencia en el plazo de cinco días, contados a partir del día siguiente de la recepción de su justificación.
En caso de que el titular o el responsable no acudan a esta segunda audiencia, el Comisionado ponente deberá continuar con la siguiente etapa de sustanciación del procedimiento del recurso de revisión conforme lo dispuesto en la Ley General y los presentes Lineamientos generales".

314 En este sentido, el artículo 148 de los Lineamientos de Protección de Datos Personales indica lo siguiente:
"Ausencia de alguna de las partes a la audiencia de conciliación sin justificación
Artículo 148. De conformidad con el artículo 107, fracción III de la Ley General, cuando el titular o el responsable no acudan a la audiencia de conciliación y no justifiquen su ausencia, el Comisionado ponente deberá continuar con la siguiente etapa de sustanciación del procedimiento del recurso de revisión en términos de la Ley General y los presentes lineamientos generales".

315 Al respecto, los Lineamientos de Protección de Datos Personales señalan lo siguiente:
"Acuerdo de conciliación
Artículo 150. En términos de los artículos 106 y 107, fracción V de la Ley General, si el titular y el responsable

de acuerdo con el contenido de los Lineamientos de Protección de Datos Personales, el cumplimiento al acuerdo de conciliación se definirá en función de los derechos ARCO a ejercer y de la complejidad técnica, operativa o demás cuestiones involucradas para hacer efectivo el derecho que se trate.[316]

H. El RR se dará por concluido cuando se hayan cumplido los compromisos previstos en el acuerdo derivado de la audiencia de conciliación entre las partes y en caso de que los mismos no hay sido observados, se reanudará el RR.

Un aspecto particular de la conciliación en el sector público es que el responsable se encuentra obligado a hacer del conocimiento del comisionado ponente el cumplimiento del acuerdo de conciliación a más tardar al día siguiente de que concluya el plazo fijado para cumplir el acuerdo de conciliación, pues en caso contrario se continuará con la sustanciación del RR.[317]

Finalmente, para acreditar el cumplimiento de las disposiciones convenidas en el acuerdo de conciliación, el comisionado ponente emitirá un acuerdo de cumplimiento sobre la observancia de lo dispuesto en el acuerdo de conciliación.[318] Así, la materialización de los acuerdos que emanen de la conciliación, tendrá como consecuencia la conclusión del RR para que el comisionado ponente someta a consideración del Pleno del INAI el proyecto de resolución en la que se proponga el sobreseimiento del RR.

Confidencialidad de la información

Christian Paredes González

La confidencialidad es un atributo de la información y al mismo tiempo un principio de seguridad que hace referencia a la obligación de que las personas que tienen acceso a ésta apliquen y respeten determinadas reglas y procedimientos a fin de que sea protegida de su divulgación no autorizada a terceros y se garantice que solo el personal autorizado pueda acceder a la misma. El atributo de confidencialidad obliga a que se establezcan condicio-

llegan a un acuerdo en la etapa de conciliación, éste deberá constar por escrito en el acta de la audiencia de conciliación y tendrá efectos vinculantes".

316 Cumplimiento del acuerdo conciliación
"Artículo 151. El responsable deberá cumplir el acuerdo de conciliación en el plazo establecido en el acta, el cual se definirá en función del derecho ARCO a ejercer y de la complejidad técnica, operativa o demás cuestiones involucradas para hacer efectivo el derecho que se trate.
Para tal efecto, el responsable deberá hacer del conocimiento del Comisionado ponente el cumplimiento del acuerdo a que se refiere el párrafo anterior del presente artículo a más tardar al día siguiente de que concluya el plazo fijado para cumplir el acuerdo de conciliación […]".

317 "Cumplimiento del acuerdo conciliación
Artículo 151. El responsable deberá cumplir el acuerdo de conciliación en el plazo establecido en el acta, el cual se definirá en función del derecho ARCO a ejercer y de la complejidad técnica, operativa o demás cuestiones involucradas para hacer efectivo el derecho que se trate.
Para tal efecto, el responsable deberá hacer del conocimiento del Comisionado ponente el cumplimiento del acuerdo a que se refiere el párrafo anterior del presente artículo a más tardar al día siguiente de que concluya el plazo fijado para cumplir el acuerdo de conciliación.
En caso de que el responsable no informe sobre el cumplimiento del acuerdo de conciliación en el plazo establecido en el párrafo anterior, se tendrá por incumplido y se reanudará la sustanciación del recurso de revisión".

318 "Efecto del cumplimiento del acuerdo de conciliación
Artículo 152. Cuando el responsable cumpla con el acuerdo de conciliación, el Comisionado ponente deberá emitir un acuerdo de cumplimiento, dentro de los tres días siguientes contados a partir del día siguiente de la recepción de la notificación del responsable sobre el cumplimiento del acuerdo de conciliación.
El cumplimiento del acuerdo de conciliación dará por concluida la sustanciación del recurso de revisión y el Comisionado ponente deberá someter a consideración del Pleno del Instituto el proyecto de resolución en la que se proponga el sobreseimiento del recurso de revisión, en términos de lo dispuesto en el artículo 113, fracción V de la Ley General".

nes específicas de protección que impidan que la información sea empleada para fines no autorizados por parte de quien es su legítimo propietario o tiene control sobre la misma.

En otras palabras, debemos comprender que la confidencialidad considera a aquella información que se pone libremente a disposición pero que trae aparejado un halo de reserva y la salvaguarda de que esa información está segura en aquellas personas en que se está depositando y encargando.

La Organización Internacional de Estandarización (ISO), en la norma ISO/IEC 27002, define a la confidencialidad de la información de la siguiente forma: "Garantizar que la información es accesible solo para aquellos autorizados a tener acceso".

Por otra parte, las Recomendaciones de Seguridad de Datos Personales para el Sector Privado (Recomendaciones de Seguridad),[319] la *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales* publicada en 2015[320] (GISGSDP) y las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales[321] definen confidencialidad de la información en idénticos términos y señalan que "se trata de la propiedad de la información para evitar su acceso, divulgación o revelación, no autorizados".

El atributo de confidencialidad de la información se relaciona con los deberes de seguridad y confidencialidad previstos en la normatividad de datos personales (remitimos a lector a la consulta de las voces respectivas en esta obra) ya que la clasificación de la información contenida en los sistemas de tratamiento bajo esta categoría permitirá al responsable determinar entre otras cosas, las medidas de seguridad aplicables, prevenir riesgos y atender incidentes de seguridad en caso de que estos se presenten.

En definitiva, la confidencialidad de la información consiste en la propiedad de la información para evitar que sea materia de un tratamiento no autorizado, determinándose reglas específicas de secreto profesional y/o laboral para su acceso bajo determinadas condiciones. La confidencialidad siempre buscará ser la manera para que el titular conserve sus datos y lo que esto conlleva bajo su completa administración y fiscalización.

Consejero consultivo del INAI

Denise Guillén Lara

El consejero honorífico del Consejo Consultivo del Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales (consejero honorífico del INAI o consejero) es la persona física proveniente de la sociedad civil y/o la academia elegida conforme al procedimiento descrito en la fracción VIII, apartado A del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), el artículo 47 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), y los artículos 53 y 55 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP).

El consejero honorífico del Consejo Consultivo del INAI es una persona elegida por el Senado de la República para conformar, junto con otros nueve consejeros honoríficos, el Consejo Consultivo del INAI. En su asignación, el Senado deberá garantizar la igualdad

319 *Diario Oficial de la Federación*. 30 de octubre de 2013.

320 INAI. (2015). *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

321 INAI. (2018). *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

de género y la inclusión. Deberá tener experiencia en derechos humanos y provenir de organizaciones de la sociedad civil y la academia. Su asignación se llevará a cabo después de una convocatoria pública dirigida a instituciones académicas, de investigación, asociaciones, colegios de profesionales y la sociedad en general[322] para integrar el Consejo Consultivo del INAI por un plazo que no exceda a siete años y participar de forma conjunta y coordinada, junto con los demás consejeros honoríficos, en la promoción de los derechos de acceso a la información pública y de protección de datos personales, fortaleciendo las funciones del INAI y su relación con la sociedad.[323]

1. Requisitos para ser consejero del Consejo Consultivo del INAI

La LFTAIP, en su artículo 55, menciona como requisitos para ser consejero ser ciudadano mexicano por nacimiento en pleno ejercicio de sus derechos políticos y civiles, tener cuando menos 30 años cumplidos, contar con al menos cinco años de experiencia y reconocido prestigio en materia de acceso a la información, protección de datos, transparencia, rendición de cuentas y/o protección a los derechos humanos, gozar de buena reputación y no haber sido condenado por delito que amerite pena corporal de más de un año de prisión (pero si se tratare de robo, fraude, falsificación, abuso de confianza y otro que lastime seriamente la buena fama en el concepto público, inhabilitará para el cargo, cualquiera que haya sido la pena) y no haber sido secretario de Estado, fiscal general de la República, senador, diputado federal ni gobernador de algún estado o jefe de gobierno de la Ciudad de México, durante el año previo al día de su nombramiento.[324]

El organismo garante tendrá un consejo consultivo integrado por 10 consejeros, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.

2. Proceso de designación

El proceso de designación de los Consejeros del Consejo Consultivo del INAI se regula, en primer lugar, en el artículo 6 de la CPEUM que indica en la fracción VIII del apartado A, que dice que los consejeros honoríficos son elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores.[325] Asimismo, el proceso de

322 Micrositio del Consejo Consultivo del INAI. Disponible en: http://proyectos.inai.org.mx/consejoconsultivo/ Fecha de consulta: 24 de agosto de 2018

323 Micrositio del Consejo Consultivo del INAI, Definición disponible en: http://proyectos.inai.org.mx/consejoconsultivo/ Fecha de consulta: 25 de julio de 2018.

324 "Artículo 55. Para ser consejero se requiere:
I. Ser ciudadano mexicano por nacimiento, en pleno ejercicio de sus derechos políticos y civiles;
II. Tener cuando menos treinta años cumplidos el día de la designación;
III. Contar con al menos cinco años de experiencia y reconocido prestigio en materia de acceso a la información, protección de datos, transparencia, rendición de cuentas y/o protección a los derechos humanos;
IV. Gozar de buena reputación y no haber sido condenado por delito que amerite pena corporal de más de un año de prisión; pero si se tratare de robo, fraude, falsificación, abuso de confianza y otro que lastime seriamente la buena fama en el concepto público, inhabilitará para el cargo, cualquiera que haya sido la pena, y
V. No haber sido Secretario de Estado, Fiscal General de la República, Senador, Diputado Federal ni Gobernador de algún Estado o Jefe de Gobierno de la Ciudad de México, durante el año previo al día de su nombramiento".

325 "El organismo garante tendrá un consejo consultivo, integrado por 10 consejeros, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a

designación aparece regulado principalmente en el artículo 47 de la LGTAIP y los artículos 53 y 55 de la LFTAIP que disponen las siguientes reglas:

- Para su nombramiento, la Cámara de Senadores realizará una amplia consulta a la sociedad y con el voto de las dos terceras partes de sus miembros presentes, nombrará al consejero que deba cubrir la vacante.
- El Senado de la República determinará los métodos internos de proposición de nombramiento de los consejeros a los órganos competentes de dicho Poder Legislativo.
- En la integración del Consejo Consultivo se deberá garantizar la igualdad de género[326] y la inclusión de personas con experiencia en las materias de esta Ley y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia.
- La Cámara de Senadores establecerá el procedimiento para que el nombramiento de los consejeros se realice considerando, que el método de proposición y designación sea transparente.
- El procedimiento para el nombramiento de los consejeros deberá contemplar la realización de una amplia consulta a la sociedad mediante una convocatoria pública dirigida a instituciones académicas, de investigación, asociaciones, colegios de profesionales y la sociedad en general, para que ciudadanas y ciudadanos mexicanos sean propuestos para ocupar alguno de los cargos honoríficos de consejero.

Derivado de lo anterior, el artículo 20 de la LFTAIP indica que el Senado de la República deberá acordar el procedimiento de designación, los plazos que se deban cumplir y en general todos los pormenores del proceso de selección considerando al menos las siguientes características:

- Acordar el método de registro y evaluación de los aspirantes
- Hacer pública la lista de las y los aspirantes comisionado
- Hacer públicos los documentos que hayan sido entregados para su inscripción en versiones públicas
- Hacer público el cronograma de audiencias
- Podrán efectuarse audiencias públicas en las que se invitará a participar a investigadores, académicos y a organizaciones de la sociedad civil, especialistas en las materias de acceso a la información, transparencia, datos personales, fiscalización y rendición de cuentas
- El dictamen que se presente al Pleno a propuesta de los grupos parlamentarios, deberá hacerse público al menos un día antes de su votación

Finalmente, debe tenerse en consideración que la persona que aspire a ser consejero del INAI deberá de cumplir con los requisitos de elegibilidad previstos en el artículo 55 de la LFTAIP referidos con anterioridad.

3. Atribuciones

Los consejeros tendrán las facultades que corresponden al Consejo Consultivo y que se señalan en los artículos 48 de la LGTAIP y 54 de la LFTAIP que se han mencionado en la

seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo".

326 Asimismo, según declara el segundo párrafo del artículo 47 de la LGTAIP, como regla para la integración del Consejo Consultivo, deberá garantizarse la igualdad de género y la inclusión de personas con experiencia en la materia y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia.

voz correspondiente a la figura del Consejo Consultivo. En sintonía con dichas facultades, legalmente reconocidas en favor del Consejo Consultivo, el artículo 8 de las Reglas de Operación del Consejo Consultivo del INAI dispone que sus consejeros cuenten con las siguientes atribuciones específicas: participar en los trabajos del Consejo Consultivo, así como resolver colegiadamente los asuntos de su competencia, de manera presencial o mediante asistencia remota; asistir presencial o de manera remota, participar en las deliberaciones y votar los proyectos de acuerdo o dictamen que se sometan a la consideración del Pleno; conocer la información necesaria para el ejercicio de las atribuciones establecidas en el artículo 54 de la LFTAIP; proponer la realización de requerimientos de información al Pleno del INAI; sugerir la invitación en las sesiones del Consejo Consultivo de autoridades y particulares, para informar o responder preguntas relacionadas con asuntos de su competencia, especialidad y/o conocimiento, así como el personal administrativo y técnico del INAI; solicitar la inclusión de asuntos en el orden del día; solicitar, de conformidad con las reglas de operación, se convoque a sesión ordinaria y/o extraordinaria; suscribir los acuerdos, opiniones, actas y dictámenes que sean sometidos a la consideración del Consejo Consultivo; emitir opiniones y formular propuestas al seno del Consejo Consultivo, sobre la aplicación y orientación de la programación anual de trabajo del INAI; considerar y en su caso aprobar el calendario anual de sesiones y la integración de comisiones; participar en las comisiones que se integren; opinar sobre el presupuesto anual del Instituto; proponer programas o proyectos especiales para la promoción del derecho a la información pública, la transparencia o la cultura de la rendición de cuentas; solicitar la información que consideren necesaria al Instituto para el ejercicio de sus funciones; nombrar al secretario técnico a propuesta del presidente del Consejo Consultivo y las demás que les sean conferidas por la Ley y las Reglas de Operación del Consejo Consultivo.

4. Consejero presidente

De conformidad con las Reglas para la elección del presidente del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales emitidas por el Pleno del INAI[327] y con el artículo 57 de la LFTAIP, el aspirante debidamente registrado a consejero presidente del Consejo Consultivo que obtenga la mayoría simple del voto secreto de los presentes en una sesión de consejo extraordinaria que requerirá del quórum por lo menos de las dos terceras partes sus miembros sin ser válida la participación remota de los mismos, su encargo dura un periodo de tres años, renovable por una ocasión, siempre que su nombramiento le permita concluir a cabalidad el nuevo periodo.[328]

De acuerdo con lo previsto por el artículo 9 de las Reglas de Operación, el presidente del Consejo Consultivo tiene las siguientes atribuciones: presidir el Consejo Consultivo y conducir sus sesiones; representar oficialmente al Consejo Consultivo; fungir como vínculo entre el INAI y el Consejo Consultivo; convocar a las sesiones ordinarias y extraordinarias, con excepción de aquellas que sean convocadas de manera directa por cuatro consejeros en los términos previstos en la Regla 11, fracción II; [329] proponer, conforme a las reglas de

327 Reglas para le elección del presidente del Consejo Consultivo del INAI. Disponible en: http://proyectos.inai.org.mx/consejoconsultivo/images/docs/normativa/fundamentos/reglaseleccionpresidente.pdf

328 "Artículo 56. El consejo será presidido por el consejero electo por la mayoría de sus integrantes y durará en su encargo un periodo de tres años, renovable por una ocasión, siempre que su nombramiento le permita concluir a cabalidad el nuevo periodo".

329 "Artículo 11. Las sesiones del Consejo Consultivo podrán ser:
I. Ordinarias: aquellas que deban celebrarse periódicamente de acuerdo con la Ley, por lo menos una vez cada dos

operación, el orden del día de cada sesión; declarar la existencia del quórum legal, instalar y concluir las sesiones, además de decretar los recesos que fueren necesarios; conducir los trabajos, moderar los debates y tomar las medidas necesarias para el adecuado funcionamiento del Consejo Consultivo; conceder el uso de la palabra, de acuerdo con las Reglas; determinar, de acuerdo con las Reglas de Operación, si los temas del orden del día han sido suficientemente discutidos; ordenar al secretario técnico que someta a votación el orden del día propuesto, el acta de las sesiones anteriores, los proyectos de acuerdos y dictámenes; garantizar el orden de las sesiones; vigilar la correcta aplicación de las Reglas de Operación; rendir los informes y comunicados que deban ser del conocimiento de los integrantes del Consejo Consultivo, así como aquellos que considere pertinentes; instruir al secretario técnico para que notifique y publique los acuerdos y dictámenes del Consejo Consultivo; dirimir los empates que se produzcan en las votaciones con su voto de calidad; proponer al Consejo Consultivo la integración de comisiones que sean necesarias para el ejercicio de sus funciones; solicitarle al secretario técnico que prepare el proyecto del Informe Anual de Actividades del Consejo Consultivo y someterlo a la consideración de los consejeros; fungir de enlace con las instancias consultivas de otras instituciones públicas, cuando así lo decida el Consejo Consultivo, en el ejercicio de sus funciones; ser el vocero ante el Instituto y la sociedad de los acuerdos que tome el Consejo Consultivo o delegar esa responsabilidad en otro consejero y las demás que le otorguen la Ley y las Reglas de Operación.

5. Consejeros del Primer Consejo Consultivo del INAI

El 28 de abril de 2017 el Pleno del Senado aprobó el dictamen sobre el nombramiento de los 10 consejeros honoríficos integrantes del Consejo Consultivo del INAI mediante la aprobación con 80 votos a favor del dictamen.[330] Los integrantes del Primer Consejo Consultivo fueron Rafael Martínez Puón y José Pineda Ventura (quienes concluyeron sus funciones el 1 de septiembre de 2017) José Mario de la Garza Marroquín y Víctor Samuel Peña Mancilla (quienes concluyeron sus funciones el 1 de septiembre de 2018), Diana González Obregón y Denisse Guillén Lara (en funciones hasta el 1 de septiembre de 2019), Sofía Gómez Ruano y María Maqueo Ramírez (en funciones hasta el 1 de septiembre de 2020) y Fernando Nieto Morales y Khemvirg Puente Martínez (en funciones hasta el 1 de septiembre el 2021).

Los Consejeros que concluyeron sus funciones deberán ser sustituidos por nuevos consejeros siguiendo el procedimiento de los ordenamientos anteriormente mencionados.

meses de acuerdo con el calendario que acuerden los consejeros y que será publicado en el micrositio del Consejo Consultivo. Podrá determinarse un día diverso al señalado cuando exista causa justificada.
II. Extraordinarias: aquellas convocadas por el consejero presidente o por lo menos cuatro consejeros para tratar asuntos específicos cuando el caso lo amerite".

330 Senado de la República. (2017, abril 28). *Senado aprueba a 10 consejeros honoríficos del Consejo Consultivo del INAI*. Coordinación de comunicación social del Senado de la República. Disponible en: http://comunicacion.senado.gob.mx/index.php/informacion/boletines/36197-senado-aprueba-a-10-consejeros-honorificos-del-consejo-consultivo-del-inai.html Fecha de consulta: 24 de agosto de 2018.

Consejo Consultivo de los organismos garantes de las entidades federativas

Denise Guillén Lara

1. Antecedentes

La figura del Consejo Consultivo de los organismos garantes de las entidades federativas es de reciente incorporación en la legislación. La incursión de esta figura en la legislación nacional es el resultado de la reforma constitucional en materia de transparencia del 7 de febrero de 2014,[331] la cual creó un nuevo diseño institucional y un nuevo régimen jurídico sobre la transparencia, el acceso a la información y la protección de datos personales. Al igual que su homologo federal, el Consejo Consultivo del INAI, el Consejo Consultivo de los organismos garantes de las entidades federativas surge a partir de la necesidad de integrar a la sociedad civil en el proceso de toma de decisiones trascendentales sobre temas de interés nacional, siendo la transparencia uno de ellos.[332]

Los antecedentes normativos de la figura del Consejo Consultivo de los organismos garantes de las entidades federativas se encuentran, en primer lugar, en la reforma a la fracción VIII del apartado A del artículo 6 constitucional en cuyo párrafo décimo tercero se señaló que la Federación habría de contar con un Consejo Consultivo,[333] y en segundo lugar, en la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) del 4 de mayo de 2015, cuyo artículo 47 señaló que las entidades federativas del país habrían de contar con un órgano de esta naturaleza, integrado por consejeros honoríficos por un plazo no mayor a siete años.[334]

2. Definición

El Consejo Consultivo de los organismos garantes de las entidades federativas es una figura instituida por la LGTAIP de forma análoga a la figura a nivel federal. Es decir, el Consejo Consultivo del INAI, el cual es "un órgano plural, honorífico y ciudadano creado por disposición constitucional, que participa de forma conjunta y coordinada en la promoción de los derechos de acceso a la información pública y de protección de datos personales, fortaleciendo las funciones de los organismos garantes y su relación con la sociedad" tal como quedó definido por el propio Consejo Consultivo del INAI en su micrositio.

En las leyes de las entidades federativas pueden encontrarse distintas definiciones de la figura del consejo consultivo en el orden local. A manera de ejemplo, mencionamos el caso de la Ley de la Ciudad de México y la del estado de Jalisco, los cuales aportan claridad para la delimitación de este concepto.

La Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México indica, en la fracción VII de su artículo 6, que se entenderá por Consejo

331 Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en materia de transparencia. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&

332 Página del Consejo Consultivo del INAI. Definición disponible en: http://proyectos.inai.org.mx/consejoconsultivo/ Fecha de consulta: 25 de julio de 2018.

333 "[…] El organismo garante tendrá un consejo consultivo, integrado por 10 consejeros, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo".

334 "Artículo 47. Los organismos garantes contarán con un Consejo Consultivo, que estará integrado por consejeros que serán honoríficos y por un plazo que no exceda a siete años. La Ley Federal y la de las entidades federativas contemplarán lo relativo a la integración, funcionamiento, procedimientos transparentes de designación, temporalidad en el cargo y su renovación".

Consultivo o Ciudadano al órgano colegiado de la sociedad civil que realiza actividades de coordinación y planeación con el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.[335]

La Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus municipios, en la fracción III de su artículo 4, define que el consejo consultivo será un "órgano colegiado y plural, integrado por varios sectores de la sociedad civil que tiene como propósito proponer, analizar y opinar al Congreso del estado y al Instituto, en materia de transparencia y acceso a la información".[336]

3. Sustento legal

La figura del consejo consultivo de los organismos garantes de las entidades federativas se encuentra reconocida y regulada en la LGTAIP. Esta ley prevé la figura del consejo consultivo de los organismos garantes para que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las entidades federativas y los municipios.[337] De esta forma, las disposiciones de la LGTAIP referentes al establecimiento del Consejo Consultivo de los organismos garantes son la base para el funcionamiento y operación de estos últimos en cada una de las entidades federativas de la República Mexicana.

En particular, el sustento normativo de la figura del consejo consultivo de los organismos garantes son los artículos 47 y 48 de la LGTAIP, siendo el primero de ellos en el que se instituye su creación:

> Artículo 47. Los organismos garantes contarán con un consejo consultivo que estará integrado por consejeros que serán honoríficos y por un plazo que no exceda a siete años. La Ley Federal y la de las entidades federativas contemplarán lo relativo a la integración, funcionamiento, procedimientos transparentes de designación, temporalidad en el cargo y su renovación.
>
> En la integración del Consejo Consultivo se deberá garantizar la igualdad de género y la inclusión de personas con experiencia en la materia de esta Ley y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia.

A la fecha, cada una de las 32 entidades federativas cuentan con leyes propias de transparencia y acceso a la información. En cada una ellas se ha instituido la figura del consejo consultivo y, como lo dispone la LGTAIP, se regula su integración, funcionamiento, procedimientos, procesos de designación y temporalidad en el cargo y su renovación (el encargo no podrá ser inferior a siete años, según dispone el artículo 47 de la LGTAIP).

Para una pronta referencia sobre la normatividad aplicable a los consejos consultivos de los organismos garantes de las entidades federativas, se incluye una tabla que detalla el estado, su normatividad y los artículos aplicables:

---

335 "Artículo 6. Para los efectos de la presente Ley se entenderá por:
[...]
VII. Consejo Consultivo Ciudadano: Al órgano colegiado de la Sociedad Civil que realiza actividades de coordinación y planeación con el Instituto; [...]".

336 "Artículo 4. Ley-Glosario
1. Para efectos de esta ley se entiende por:
[...]
III. Consejo Consultivo: órgano colegiado y plural, integrado por varios sectores de la sociedad civil que tiene como propósito proponer, analizar y opinar al Congreso del Estado y al Instituto, en materia de transparencia y acceso a la información".

337 "Artículo 1. La presente Ley es de orden público y de observancia general en toda la República, es reglamentaria del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia y acceso a la información.
Tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las entidades federativas y los municipios".

Estado	Normatividad	Artículos aplicables
Aguascalientes	Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes y sus Municipios	Artículos 3, fracción cuarta, 30, 31, artículos 32 y 33
Baja california	Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California	Artículos 42, 43, 44, 45, 46, 47, 48 y 49
Baja California Sur	Ley de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur	Artículos 5, fracción tercera, 52, 53, 54, 55, 56, 57, 59 y 60
Campeche	Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche	Artículos 3, fracción séptima, 40, 41, 42 y 43
Ciudad De México	Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México	Artículos 6, fracción séptima, 95, 96, 97 y 98
Coahuila	Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila de Zaragoza	Artículos 222, 223 y 224
Colima	Ley de Transparencia y Acceso a la Información Pública del Estado de Colima	Artículos 6, fracción IV, 97, 98, 99, 100, 101 y 102
Chiapas	Ley de Transparencia y Acceso a la Información Pública del Estado Chiapas	Artículos 3, fracción séptima, 44, 45 y 46
Chihuahua	Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua	Artículos 5, fracción octava, 27, 28, 29, 30 y 31
Durango	Ley De Transparencia y Acceso a la Información Pública del Estado de Durango	Artículos 44, 45 y 46
Estado de México	Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios	Artículos 60, 61 y 62
Guerrero	Ley Número 207 de Transparencia y Acceso a la Información Pública del Estado de Guerrero	Artículos 58, 59, 60, 61 y 62
Jalisco y sus municipios	Ley de Transparencia y Acceso a la Información Pública del Estado de Jalisco y sus Municipios	Artículos 4, fracción tercera, 52, 53, 54, 55 y 57
Michoacán	Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de Michoacán de Ocampo	Artículos 3 fracción sexta, 120, 121, 122 y 123
Morelos	Ley de Transparencia y Acceso a la Información Pública del Estado de Morelos	Artículos 30 y 31
Nayarit	Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit	Artículos 2, fracción tercera, 113, 114, 115 y 116
Nuevo León	Ley de Transparencia y Acceso a la Información Pública de Nuevo León	Artículos 61, 62, 63, 127 y 128
Oaxaca	Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca	Artículos 6, fracción cuarta, 98, 100, 102, 103, 104, 105, 106 y107.

Puebla	Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla	Artículos 43, 44, 45, 46 y 47
Querétaro	Ley de Transparencia y Acceso a la Información Pública del Estado de Querétaro	Artículos 39 y 41
Quintana Roo	Ley de Transparencia y Acceso a la Información Pública para el Estado de Quintana Roo	Artículos 3, fracción quinta, 68, 69, 70, 71 y 72
San Luis Potosí	Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí	Artículos 3 fracción séptima, 42 y 43
Sinaloa	Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa	Artículos 70, 71, 72, 73, 74, 75, 76, 77 y 78
Sonora	Ley de Transparencia y Acceso a la Información Pública del Estado de Sonora	Artículos 3, fracción octava, 43, 44, 45, 46, art.47, 53, 54 y 55
Tabasco	Ley de Transparencia y Acceso a la Información Pública de Tabasco	Artículos 53, 54 y 55
Tlaxcala	Ley de Transparencia y Acceso a la Información Pública del Estado de Tlaxcala	Artículos 43 y 44
Veracruz	Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave	Artículo 126
Yucatán	Ley de Transparencia y Acceso a la Información Pública del Estado de Yucatán	Artículos 31, 32, 33 y 34
Zacatecas	Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas	Artículos 147 y 148

4. Facultades y atribuciones

De manera genérica, las facultades de los consejos consultivos de los organismos garantes de las entidades federativas se establecen en el artículo 48 de la LGTAIP. Las facultades de las que se dota a los consejos consultivos son: opinar sobre el programa anual de trabajo, su cumplimiento y sobre el proyecto de presupuesto para el ejercicio del año siguiente; conocer del informe de los organismos garantes sobre el presupuesto asignado a programas y el ejercicio presupuestal y emitir las observaciones correspondientes; emitir opiniones no vinculantes a petición de organismos garantes o por iniciativa propia sobre temas relevantes en materia de transparencia, acceso a la información, accesibilidad y protección de datos personales; emitir opiniones técnicas para la mejora continua en el ejercicio de las funciones sustantivas de los organismos garantes; opinar sobre la adopción de criterios generales en materia sustantiva y analizar y proponer la ejecución de programas, proyectos y acciones relacionadas con la materia de transparencia y acceso a la información y su accesibilidad.[338]

338 "Artículo 48. Los Consejos Consultivos contarán con las siguientes facultades:
I. Opinar sobre el programa anual de trabajo y su cumplimiento;
II. Opinar sobre el proyecto de presupuesto para el ejercicio del año siguiente;
III. Conocer el informe de los organismos garantes sobre el presupuesto asignado a programas y el ejercicio presupuestal y emitir las observaciones correspondientes;
IV. Emitir opiniones no vinculantes, a petición de los organismos garantes o por iniciativa propia, sobre temas relevantes en las materias de transparencia, acceso a la información, accesibilidad y protección de datos personales;

5. Integración y proceso de designación

El Consejo Consultivo de los organismos garantes se integra por consejeros honoríficos que durarán en su encargo un plazo que no exceda de siete años de conformidad con el artículo 47 de la LGTAIP. La integración de los consejos consultivos de los organismos garantes se regula en la LGTAIP de manera genérica y sin mayor detalle debido a que, para la concreción de aspectos relativos a su integración y designación, se remite a las leyes de las entidades federativas. De esta manera, el segundo párrafo del artículo 47 previene lo siguiente: "En la integración del Consejo Consultivo se deberá garantizar la igualdad de género y la inclusión de personas con experiencia en la materia de esta Ley y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia".

6. Funcionamiento

La operación de los consejos consultivos de los organismos garantes de las entidades federativas, al igual que su integración, funcionamiento, procedimientos transparentes de designación, temporalidad en el cargo y renovación de sus consejeros se sujeta a lo dispuesto en las leyes vigentes en las entidades federativas del país, por lo que habrán de consultarse para conocer en detalle las reglas aplicables a cada uno de los consejos consultivos de cada uno de los organismos garantes de las entidades federativas, lo anterior, en consonancia con el mandato previsto en el artículo 47 de la LGTAIP.[339]

De la misma forma que su homólogo federal, los consejos consultivos de los organismos garantes desempeñan un importante papel en el fortalecimiento de los órganos garantes de las entidades federativas y su relación con la sociedad.

Consejo Consultivo del INAI

Denise Guillén Lara

1. Antecedentes

El Consejo Consultivo del Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales (Consejo Consultivo del INAI o Consejo Consultivo) es un órgano de reciente creación en nuestro ordenamiento jurídico. Fue a partir de la reforma constitucional del 7 de febrero de 2014[340] (reforma de transparencia) cuando se instituyó su creación, junto con la del Organismo Garante Federal, el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales (INAI) modificándose sustancialmente la configuración de las instituciones, órganos y normas referentes a la transparencia, el acceso a la información pública y protección de datos personales en México. Es decir, de forma previa a la reforma de transparencia, dicha figura no había tenido ningún tipo de referencia ni regulación en el derecho nacional.

V. Emitir opiniones técnicas para la mejora continua en el ejercicio de las funciones sustantivas de los organismos garantes;
VI. Opinar sobre la adopción de criterios generales en materia sustantiva, y
VII. Analizar y proponer la ejecución de programas, proyectos y acciones relacionadas con la materia de transparencia y acceso a la información y su accesibilidad".

339 "Artículo 47. Los Organismos garantes contarán con un Consejo Consultivo, que estará integrado por consejeros que serán honoríficos y por un plazo que no exceda a siete años. La Ley Federal y la de las Entidades Federativas contemplarán lo relativo a la integración, funcionamiento, procedimientos transparentes de designación, temporalidad en el cargo y su renovación. En la integración del Consejo Consultivo se deberá garantizar la igualdad de género y la inclusión de personas con experiencia en la materia de esta Ley y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia".

340 Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en materia de transparencia. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&

El Consejo Consultivo entendido como un órgano de consulta abierto, surge a partir de la necesidad de integrar a la sociedad civil en el proceso de toma de decisiones trascendentales sobre temas de interés nacional, siendo la transparencia uno de ellos.[341] Como lo ha destacado la comisionada del INAI, María Patricia Kurczyn Villalobos, dicho órgano es fundamental para perfeccionar la función del INAI porque aporta ideas, contribuye a perfilar temas de interés ciudadano y avala las decisiones del Instituto.[342]

No obstante, aunque la figura del Consejo Consultivo es novedosa en nuestro entorno legal, ya había sido adoptada en otras latitudes. Por ejemplo, en España, el artículo 38 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (LOPD)[343] destaca que el director de la Agencia Española de Protección de Datos (AEPD) estará asesorado por un consejo consultivo heterogéneo en su composición y que informará sobre todas las cuestiones que someta a su consideración el director de la AEPD, pudiendo formular propuestas en materia de protección de datos.

La existencia de un órgano de consulta que represente a la sociedad civil sobre la base de los principios de independencia, igualdad, pluralidad y representatividad, entre otros, para la toma de decisiones de transcendencia general ha sido una idea que también ha sido recibida en órganos constitucionales autónomos como el Instituto Federal de Telecomunicaciones (IFT), que en términos de lo dispuesto por la Constitución Política de los Estados Unidos Mexicanos (CPEUM), cuenta con un consejo ciudadano[344] que asesora al IFT respecto de las funciones que tiene encomendadas por mandato constitucional y legal.[345] Dicho órgano, análogo al Consejo Consultivo del INAI se caracteriza por ser un órgano asesor respecto de los principios establecidos en los artículos 2, 6 y 7 de la CPEUM y cuyos integrantes son especialistas de reconocido prestigio en las materias que son competencia del IFT.[346]

En respuesta a lo ordenado por la reforma de transparencia, el Congreso Federal aprobó, el 4 de mayo de 2015, la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), ordenamiento que establecería, en su artículo 47, y por vez primera, la obligación de que los organismos garantes (a nivel federal y local) contaran con un consejo

341 Página del Consejo Consultivo del INAI Definición disponible en: http://proyectos.inai.org.mx/consejoconsultivo/ Fecha de consulta: 25 de julio de 2018,

342 INAI. (2018, agosto 20). *Reconoce INAI Labor de José Mario de la Garza y Víctor Peña como integrantes del Consejo Consultivo del Instituto*. Comunicado 229/18. Disponible en: http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-229-18.pdf Fecha de consulta: 25 de julio de 2018.

343 "Artículo 38. Consejo Consultivo
El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:
Un Diputado, propuesto por el Congreso de los Diputados.
Un Senador, propuesto por el Senado.
Un representante de la Administración Central, designado por el Gobierno.
Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
Un miembro de la Real Academia de la Historia, propuesto por la misma.
Un experto en la materia, propuesto por el Consejo Superior de Universidades.
Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.
Un representante de cada Comunidad Autónoma que haya creado una Agencia de Protección de Datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.
Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.
El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan".

344 http://consejoconsultivo.ift.org.mx/miembros.php

345 http://consejoconsultivo.ift.org.mx/miembros.php

346 http://consejoconsultivo.ift.org.mx/miembros.php

consultivo. Posteriormente, la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), publicada el 9 de mayo de 2016 en el *Diario Oficial de la Federación*, pasaría a regular en los artículos 35, 53, 54, 55, 56, 57, 58, 59, 60 y séptimo transitorio todo lo relativo al Consejo Consultivo del INAI.

Como lo declara el propio Consejo Consultivo del INAI, en su primer informe de labores, el trabajo de este órgano, desde su diseño, fue más amplio que solo dar seguimiento a las funciones del INAI extendiéndose a objetivos tales como analizar y proponer, desde un enfoque ciudadano, la ejecución de programas, proyectos y acciones en las materias de transparencia, acceso a la información pública y protección de datos personales, así como opinar sobre temas relevantes en relativos a esos temas y para que se adopten criterios generales acerca de ellas, además de conocer y pronunciarse sobre el desempeño y el presupuesto ejercido por el INAI, a efecto de promover la mejora continua de sus funciones sustantivas.[347]

Es de notar que el Consejo Consultivo no cuenta con un patrimonio propio, por lo que el desempeño de sus funciones será sin presupuesto asignado, asimismo, el encargo es honorífico, por lo mismo los consejeros honoríficos no reciben remuneración alguna. Asimismo, los consejeros invierten incontables horas en el desempeño de sus funciones en beneficio de un fortalecimiento del INAI.

El Pleno del INAI ha respondido a este compromiso desinteresado apoyando con recursos materiales y técnicos para la creación y mantenimiento periódico del micrositio del Consejo Consultivo, asignando a un secretario técnico, tal como lo disponen sus reglas de operación, así como con la asignación de una sala de sesiones del Consejo Consultivo del INAI para su uso particular. Por otro lado, los comisionados del Pleno ponen a disposición del Consejo Consultivo en sus sesiones ordinarias y extraordinarias el equipo estenográfico, fotógrafos y video para transmitir sus sesiones en vivo.

2. Definición

El Consejo Consultivo del INAI, según se describe en su propio micrositio ubicado dentro del portal de internet del Instituto, "es un órgano plural, honorífico y ciudadano creado por disposición constitucional, que participa de forma conjunta y coordinada en la promoción de los derechos de acceso a la información pública y de protección de datos personales, fortaleciendo las funciones del INAI y su relación con la sociedad".[348]

Desde la perspectiva normativa, encontramos la definición de Consejo Consultivo en la fracción VIII del artículo 2 de las Reglas de Operación del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales al tenor siguiente:

> VIII. Consejo Consultivo: el órgano colegiado del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos al que aluden los artículos 47 de la Ley General de Transparencia y Acceso a la Información, 53 de la Ley Federal de Transparencia y Acceso a la Información Pública y artículo 88 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

El Consejo Consultivo es el órgano colegiado y plural, integrado por la sociedad civil que tiene como propósito proponer, analizar y opinar ante el INAI, en materia de transparencia y ac-

347 INAI. (Del 14 de junio de 2017 al 13 de junio de 2018). *Primer Informe de Actividades del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a Información y Protección de Datos Personales*. Micrositio del Consejo Consultivo del INAI. Recuperado de: http://proyectos.inai.org.mx/consejoconsultivo/images/docs/informesanuales/2017-2018.pdf

348 Fecha de consulta: 25 de julio de 2018.

ceso a la información, así como también en su ámbito administrativo para el correcto funcionamiento y debida protección de los principios fundamentales en materia de transparencia.[349]

3. Sustento legal

El Consejo Consultivo tiene notoria relevancia debido a que su creación responde a un mandato constitucional. Específicamente, es el artículo 6 de la CPEUM, fracción VIII, apartado A, el que instituye la creación de este importante órgano colegiado al precisar que el organismo garante federal contará con un consejo consultivo, remitiendo a la legislación secundaria las reglas de su actuación.

> El organismo garante tendrá un Consejo Consultivo, integrado por diez consejeros, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.

Además, con motivo de la reforma de transparencia del 7 de febrero de 2014 se emitieron distintas disposiciones que dan sustento a la figura del Consejo Consultivo a saber:

- LGTAIP (artículos 47 y 48).
- LFTAIP (artículos 35, 53, 54, 55, 56, 57, 58, 59, 60 y séptimo transitorio).
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) (artículo 88).
- Estatuto Orgánico del INAI (último párrafo del artículo 5).
- Reglas de Operación del Consejo Consultivo del INAI.
- Reglas para la Elección del Presidente del Consejo Consultivo del INAI.
- Código de Ética del Consejo Consultivo del INAI.

La LGTAIP destaca por ser la primera disposición secundaria que refiere la creación del Consejo Consultivo, al señalar en sus artículos 47 y 48 la obligación de los entes garantes de contar con dicho órgano y detallar sus funciones.

La LFTAIP dispone sobre la creación del Consejo Consultivo y regula su composición, proceso de designación y actuar general en los artículos 53, 54, 55, 56, 57, 58, 59 y 60.

Por su lado, la LGPDPPSO, en su artículo 88, refiere que en lo que concierne a la integración, procedimiento de designación y funcionamiento del Consejo Consultivo se estará a lo dispuesto por la LGTAIP, La LFTAIP y demás disposiciones conducentes:

> Artículo 88. En la integración, procedimiento de designación y funcionamiento del Instituto y del Consejo Consultivo se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

Por otra parte, el último párrafo del artículo 5 del Estatuto Orgánico del INAI que, dentro de su estructura el INAI contará con un Consejo Consultivo de acuerdo con las siguientes bases:

> El Instituto contará con un consejo consultivo que se integrará en la forma y términos que establece el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, la Ley General y la Ley Federal; así como con un órgano interno de control cuyo titular será designado en términos del artículo 74, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos y demás normatividad aplicable.

349 Micrositio del Consejo Consultivo del INAI. Disponible en: http://proyectos.inai.org.mx/consejoconsultivo/ Fecha de consulta: 24 de agosto de 2018.

Finalmente, como se señaló, debe destacarse la importante labor que ha realizado el Primer Consejo Consultivo del INAI mediante la emisión de las Reglas de Operación del Consejo Consultivo, y el propio órgano garante federal, mediante el Pleno del INAI, en la emisión de las Reglas para la elección del Presidente del Consejo Consultivo del Instituto.

Recientemente, el Consejo Consultivo expidió también su código de ética,[350] esto como una buena práctica, pues el Consejo, sin ser una institución pública, tiene una función de interés público, que debe regirse por principios y valores esenciales para su mejor funcionamiento.[351]

4. Integración y proceso de designación

La integración del Consejo Consultivo se refiere, en primer lugar, en el artículo 6 de la CPEUM que indica que el INAI (organismo garante federal) contará con el Consejo Consultivo integrado por 10 consejeros con carácter honorífico, que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores, después de una convocatoria pública dirigida a instituciones académicas, de investigación, asociaciones, colegios de profesionales y la sociedad en general. Los consejeros provendrán de organizaciones de la sociedad civil y la academia.[352 y 353]

Con base en lo anterior, el artículo 47 de la LGTAIP[354] dispone que el Consejo Consultivo estará compuesto por consejeros que serán honoríficos y por un plazo que no excederá siete años. No obstante, en lo referente a la integración, funcionamiento, procedimientos transparentes de designación, temporalidad en el cargo y renovación se remite a la LFTAIP, por lo que será en esta última donde se encontrarán las reglas específicas.

Respecto de la integración del Consejo Consultivo, el artículo 53 de la LFTAIP dispone las siguientes reglas:

- El Consejo Consultivo estará integrado por 10 consejeros honoríficos que durarán en su encargo siete años
- Para su nombramiento, la Cámara de Senadores realizará una amplia consulta a la sociedad y con el voto de las dos terceras partes de sus miembros presentes, nombrará al consejero que deba cubrir la vacante
- Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.

350 INAI. (2017). *Código de Ética del Consejo Consultivo del INAI*. Disponible en: http://proyectos.inai.org.mx/consejoconsultivo/images/docs/normativa/fundamentos/codigodeetica.pdf Fecha de consulta: 27 de agosto de 2918,

351 INAI. (Del 14 de junio de 2017 al 13 de junio de 2018). *Primer Informe de Actividades del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a Información y Protección de Datos Personales*. Micrositio del Consejo Consultivo del INAI. Recuperado de: http://proyectos.inai.org.mx/consejoconsultivo/images/docs/informesanuales/2017-2018.pdf

352 El organismo garante tendrá un consejo consultivo integrado por 10 consejeros que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. La ley determinará los procedimientos a seguir para la presentación de las propuestas por la propia Cámara. Anualmente serán sustituidos los dos consejeros de mayor antigüedad en el cargo, salvo que fuesen propuestos y ratificados para un segundo periodo.

353 Micrositio del Consejo Consultivo del INAI. Disponible en: http://proyectos.inai.org.mx/consejoconsultivo/ Fecha de consulta: 24 de agosto de 2018,

354 "Artículo 47. Los organismos garantes contarán con un consejo consultivo que estará integrado por consejeros que serán honoríficos y por un plazo que no exceda a siete años. La Ley Federal y la de las Entidades Federativas contemplarán lo relativo a la integración, funcionamiento, procedimientos transparentes de designación, temporalidad en el cargo y su renovación. En la integración del Consejo Consultivo se deberá garantizar la igualdad de género y la inclusión de personas con experiencia en la materia de esta Ley y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia".

- El Senado de la República determinará los métodos internos de proposición de nombramiento de los consejeros a los órganos competentes del Poder Legislativo
- En la integración del Consejo Consultivo se deberá garantizar la igualdad de género[355] y la inclusión de personas con experiencia en las materias de esta Ley y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia
- La Cámara de Senadores establecerá el procedimiento para que el nombramiento de los consejeros se realice considerando, además que el método de proposición y designación sea transparente.
- El procedimiento para el nombramiento de los consejeros deberá contemplar la realización de una amplia consulta a la sociedad a través de una convocatoria pública dirigida a instituciones académicas, de investigación, asociaciones, colegios de profesionales y la sociedad en general, para que ciudadanas y ciudadanos mexicanos sean propuestos para ocupar alguno de los cargos honoríficos de consejero y se realizará en los términos del artículo 20 de la LFTAIP

En sintonía con lo anterior, el artículo 20 de la LFTAIP, aplicable al proceso de designación de los consejeros del Consejo Consultivo, indica que el Senado de la República deberá acordar el procedimiento de designación, los plazos que se deban cumplir y en general todos los pormenores del proceso de selección considerando al menos las siguientes características:

- Acordar el método de registro y evaluación de los aspirantes.
- Hacer pública la lista de las y los aspirantes a comisionada o comisionado.
- Hacer públicos los documentos que hayan sido entregados para su inscripción en versiones públicas.
- Hacer público el cronograma de audiencias.
- Podrán efectuarse audiencias públicas en las que se invitará a participar a investigadores, académicos y a organizaciones de la sociedad civil, especialistas en las materias de acceso a la información, transparencia, datos personales, fiscalización y rendición de cuentas.
- El dictamen que se presente al Pleno a propuesta de los grupos parlamentarios, deberá hacerse público al menos un día antes de su votación.

Finalmente, debe tenerse en consideración que la persona que aspire a ser consejero del INAI (ver la voz correspondiente en este diccionario) deberá cumplir con los requisitos de elegibilidad previstos en el artículo 55 de la LFTAIP.

A partir del 28 de abril de 2017 quedó constituido el primer Consejo Consultivo mediante la aprobación del Pleno del Senado con 80 votos a favor del dictamen sobre el nombramiento de10 consejeros honoríficos, integrantes del Consejo Consultivo.[356]

Los integrantes del Primer Consejo Consultivo fueron el Rafael Martínez Puón y José Pineda Ventura (sustituidos el 1 de septiembre de 2017), José Mario de la Garza Marroquín y Víctor Samuel Peña Mancilla (sustituidos el 1 de septiembre de 2018), Diana González Obregón y Denisse Guillén Lara (en función hasta el 1 de septiembre de 2019), Sofía

355 Asimismo, según declara el segundo párrafo del artículo 47 de la LGTAIP, como regla para la integración del Consejo Consultivo, deberá garantizarse la igualdad de género y la inclusión de personas con experiencia en la materia y en derechos humanos, provenientes de organizaciones de la sociedad civil y la academia.

356 Senado de la República. Disponible en: http://comunicacion.senado.gob.mx/index.php/informacion/boletines/36197-senado-aprueba-a-10-consejeros-honorificos-del-consejo-consultivo-del-inai.html Fecha de consulta: 24 de agosto de 2018.

Gómez Ruano y María Maqueo Ramírez (en función hasta el 1 de septiembre de 2020) y Fernando Nieto Morales y Khemvirg Puente Martínez (en función hasta el 1 de septiembre el 2021).

Los consejeros honoríficos habrán de ser sustituidos por nuevos consejeros siguiendo el procedimiento descrito anteriormente.

5. Facultades y atribuciones

El Consejo Consultivo del órgano garante federal cuenta con importantes facultades para la realización de sus funciones. De acuerdo con el artículo 48 de la LGTAIP, el Consejo Consultivo cuenta (al igual que sus homólogos locales) con facultades para opinar sobre el programa anual de trabajo y su cumplimiento, sobre el proyecto de presupuesto para el ejercicio del año siguiente, conocer el informe de los organismos garantes sobre el presupuesto asignado a programas, proyectos y acciones relacionadas con la materia de transparencia y acceso a la información y su accesibilidad.[357]

De acuerdo con lo previsto por el artículo 54 de la LFTAIP, el Consejo Consultivo cuenta con las siguientes atribuciones: aprobar sus reglas de operación, presentar al Pleno su informe anual de actividades, opinar sobre el programa anual de trabajo del instituto y su cumplimiento, emitir un informe anual sobre el desempeño del INAI, opinar sobre el proyecto de presupuesto para el ejercicio del año siguiente, conocer el informe del INAI sobre el presupuesto asignado a programas y el ejercicio presupuestal y emitir las observaciones correspondientes, emitir opiniones no vinculantes al INAI sobre temas relevantes en las materias de transparencia, acceso a la información, accesibilidad y protección de datos personales, emitir opiniones técnicas para la mejora continua en el ejercicio de las funciones sustantivas del Instituto, opinar sobre la adopción de criterios generales en materia sustantiva, proponer mejores prácticas de participación ciudadana y colaboración en la implementación y evaluación de la regulación en materia de datos abiertos, analizar y proponer la ejecución de programas, proyectos y acciones relacionadas con la materia de transparencia y acceso a la información y su accesibilidad, y aquellas que deriven de la LGTAIP y la propia LFTAIP.

Según destaca el propio Consejo Consultivo en su primer informe de labores,[358] la principal actividad que realiza dicho órgano colegiado consiste en la toma de decisiones, sea por mayoría o por unanimidad de los consejeros honoríficos que se reúnen en sesión. Dichas

357 "Artículo 48. Los Consejos Consultivos contarán con las siguientes facultades:
I. Opinar sobre el programa anual de trabajo y su cumplimiento;
II. Opinar sobre el proyecto de presupuesto para el ejercicio del año siguiente;
III. Conocer el informe de los Organismos garantes sobre el presupuesto asignado a programas y el ejercicio presupuestal y emitir las observaciones correspondientes;
IV. Emitir opiniones no vinculantes, a petición de los Organismos garantes o por iniciativa propia, sobre temas relevantes en las materias de transparencia, acceso a la información, accesibilidad y protección de datos personales;
V. Emitir opiniones técnicas para la mejora continua en el ejercicio de las funciones sustantivas de los Organismos garantes;
VI. Opinar sobre la adopción de criterios generales en materia sustantiva, y
VII. Analizar y proponer la ejecución de programas, proyectos y acciones relacionadas con la materia de transparencia y acceso a la información y su accesibilidad".

358 La labor de este Consejo Consultivo ha sido reconocida ya por la comisionada María Patricia Kurczyn, quien funge como "enlace" entre el Pleno del INAI y el Pleno del Consejo Consultivo del INAI y quien en agosto de 2018 reconoció la labor de los consejeros honoríficos José Mario de la Garza Marroquín y Víctor Samuel Peña Mancilla que terminaban su encargo, destacando lo siguiente: "Siempre es importante estudiar y analizar para mejorar, para perfeccionar, entonces un Consejo Consultivo es un apoyo muy importante por dos razones: la primera, para aportar ideas y tratar de centrar en un momento determinado; la segunda, para avalar, en lo personal y ahora como comisionada lo diría, me siento avalada en las resoluciones, en las decisiones porque tenemos un consejo de diez expertos, de diez personas de una entrega importante, que sin ningún interés económico o político aportan a la sociedad". INAI, Comunicado 229/18. Disponible en: http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-229-18.pdf Fecha de consulta: 25 de julio de 2018.

decisiones pueden reflejarse en un dictamen, acuerdo o resolución sobre los asuntos que someten a consideración del Pleno del Consejo sus miembros, mediante la conformación previa del orden del día.[359]

Aun cuando las opiniones que emite el Consejo Consultivo no son vinculantes, el artículo 35 de la LFTAIP establece que, en el ejercicio de las atribuciones del Pleno, deberá atender las opiniones correspondientes que el Consejo Consultivo emita de conformidad con lo dispuesto en la propia LFTAIP.

6. Funcionamiento

En lo que concierne al funcionamiento del Consejo Consultivo, el artículo 59 de la LFTAIP indica que este órgano colegiado habrá de funcionar de acuerdo con las disposiciones del Estatuto Orgánico del INAI, en sesiones ordinarias y extraordinarias tomando sus decisiones por mayoría de votos.

Las sesiones del Consejo Consultivo podrán ser ordinarias o extraordinarias. De acuerdo con el artículo 60 de la LFTAIP, sesiones ordinarias deberán convocarse cuando menos, una vez cada dos meses, mientras que las sesiones extraordinarias deberán convocarse únicamente cuando existan asuntos de importancia que deben resolverse de inmediato por el Presidente del Consejo y mediante convocatoria que formulen cuatro de los consejeros. En los artículos 11[360] y 12[361] de las Reglas de Operación del Consejo Consultivo se establece que se entenderá por sesiones ordinarias y extraordinarias, así como el proceso aplicable en caso de suspensión de la sesión por falta de quórum.

Un aspecto importante sobre la operación del Consejo Consultivo es su organización en comisiones. De acuerdo con lo dispuesto por el artículo 41 de las Reglas de Operación del Consejo Consultivo, las comisiones tienen por objeto realizar estudios, investigaciones y análisis, para dar cumplimiento a lo establecido en el artículo 48 de la Ley General y 54 de la Ley Federal, siendo cada una de las comisiones con base en su área de especialidad las responsables de elaborar los proyectos de opiniones que deberán de someter para la aprobación final del Consejo Consultivo en sesión ordinaria o extraordinaria, según sea el caso.

Según el citado artículo 41, las comisiones estarán integradas por el número de consejeros que deseen participar en cada una. Además, en el artículo 41 de las referidas Reglas de Operación se dispone que el Consejo Consultivo decidirá el número y ámbito de sus comisiones, pero cuando menos se conformarán las siguientes comisiones:

- Comisión de Presupuesto: encargada de elaborar los estudios pertinentes para expresar opinión sobre el presupuesto del Instituto, así como la proyección y gestión de los recursos propios del Consejo Consultivo para satisfacer las necesidades materiales del mismo.

359 INAI. (Del 14 de junio de 2017 al 13 de junio de 2018). *Primer Informe de Actividades del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a Información y Protección de Datos Personales*. Micrositio del Consejo Consultivo del INAI. Recuperado de: http://proyectos.inai.org.mx/consejoconsultivo/images/docs/informesanuales/2017-2018.pdf

360 "Artículo 11. Las sesiones del Consejo Consultivo podrán ser:
I. Ordinarias: aquellas que deban celebrarse periódicamente de acuerdo con la Ley, por lo menos una vez cada dos meses de acuerdo al calendario que acuerden los Consejeros y que será publicado en el micrositio del Consejo Consultivo. Podrá determinarse un día diverso al señalado cuando exista causa justificada.
II. Extraordinarias: aquellas convocadas por el Consejero Presidente o por lo menos cuatro consejeros para tratar asuntos específicos cuando el caso lo amerite".

361 "Artículo 12. El presidente podrá suspender la sesión cuando no haya quórum o cuando así lo acuerden la mayoría de los asistentes. En ese mismo momento se deberá fijar la hora y fecha de reanudación".

- Comisión de Organización y Desempeño: encargada de evaluar el desempeño de las actividades ordinarias y estratégicas del Instituto, así como la opinión sobre la programación de su trabajo anual y proponer al Consejo Consultivo la emisión de observaciones sobre la administración y profesionalización del Instituto.
- Comisión de Transparencia y Participación Ciudadana: encargada de promover la cultura del derecho a la información pública y la transparencia, así como la promoción de una mejor accesibilidad y participación ciudadana en las actividades del Instituto.
- Comisión de Protección de Datos Personales: encargada de promover la cultura de protección de datos personales, así como de hacer observaciones a las políticas y procedimientos del Instituto en este ámbito.

Las Comisiones se sujetarán a lo dispuesto por el artículo 43 de las Reglas de Operación del Consejo Consultivo que precisan que en éstas solo podrán participar los miembros del Consejo Consultivo, se llevarán a cabo con la frecuencia que sus integrantes establezcan para la realización de su programa de actividades pero no deberán transcurrir más de dos meses sin reunirse, sus opiniones y conclusiones no tendrán carácter definitivo en todos los casos sus proyectos o recomendaciones deberán ser sancionados por el Consejo Consultivo, los consejeros recibirán por escrito las propuestas y conclusiones de las comisiones con al menos una semana de anterioridad a la celebración de la sesión del Consejo Consultivo con la finalidad de que conozcan y estudien los temas que serán tratados y resueltos en la sesión, podrán recibir en el ejercicio de sus funciones la colaboración técnica de las unidades administrativas del INAI así como la solicitar el apoyo de otras instituciones o terceros cuando así lo defina el Consejo Consultivo, en las sesiones del Consejo Consultivo deberán informar, a través de su responsable sobre los avances y resultados de sus actividades.

Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Jorge Islas López

El camino de la transparencia en México estuvo marcado por mucho tiempo por una idea errónea del constitucionalismo, en la cual se pensaba que con la simple ampliación semántica de derechos fundamentales, era suficiente para garantizarlos y protegerlos efectivamente. Tal y como lo mencionaron Madison y Hamilton en *El Federalista*, la realidad es que "los derechos no se protegen con meras declaraciones sino con las propias estructuras de un gobierno constitucional".[362] En este sentido, los derechos se protegen con estructuras de gobierno sólidas y eficaces que los garanticen por medio de un diseño general protector. Es por esta razón que, en un sistema democrático constitucional es de vital importancia un buen diseño institucional que brinde protección con las obligaciones que el gobierno tiene que cumplir, conforme a lo que la ley mandata. En esta línea, el derecho de acceso a la información pública,[363] el cual está establecido en el artículo 6 de la

362 Sartori, G. (1996). *Ingeniería Constitucional Comparada.* Segunda edición. Trad. de Roberto Reyes, México. Fondo de Cultura Económica, p. 211.

363 "Un derecho fundamental que comprende la libertad de: difundir, investigar y recabar información pública" Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. 2014. México, p. 7.

Constitución Política de los Estados Unidos Mexicanos (CPEUM) y regulado por la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), requiere un marco institucional y procedimental que garantice el buen funcionamiento y la protección de este derecho. De ahí la importancia del Consejo Nacional de Transparencia, Acceso a la Información y Datos Personales (Consejo Nacional).

En la búsqueda de protección al derecho de acceso a la información pública, los legisladores optaron por crear un organismo institucional capaz de armonizar, integrar y mejorar el funcionamiento de los distintos actores del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (SNT). De esta manera, el Consejo Nacional funciona como la estructura institucional capaz de organizar, promover, difundir y coordinar las facultades asignadas al SNT.

1. Definición

De acuerdo con el artículo 32 de la LGTAIP, el SNT cuenta con un consejo nacional. Este Consejo Nacional funciona, conforme a lo establecido en la exposición de motivos, como "la instancia rectora del SNT, el cual tendrá por objeto la organización efectiva y eficaz de los esfuerzos de coordinación, cooperación, colaboración, promoción y difusión en materia de transparencia y acceso a la información".[364] En otras palabras, este órgano rector funciona como el eje central en materia de transparencia, mismo que permite que el derecho de acceso a la información pública se garantice por medio de su instrumentación como parte del SNT.

2. Características y beneficios

El Consejo Nacional está conformado por los integrantes del SNT y está presidido por el presidente del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI). De esta forma, las funciones del Consejo Nacional no se mantienen solo en el ámbito de la transparencia, sino que adicionalmente involucran temas relacionados con la rendición de cuentas. De lo anterior, se entiende que el legislador privilegió al INAI como la autoridad que preside el Consejo, con la cual respetó la preeminencia constitucional tal como se encuentra establecido en su artículo 6, apartado A.[365]

El objetivo central del Consejo Nacional es el de ejercer una función rectora para coordinar los esfuerzos institucionales en conjunto, así como institucionalizar los mecanismos garantes que protegen la transparencia, los derechos de acceso a la información y la protección de datos personales. De esta forma, al ser parte del SNT tiene la misma finalidad establecida en el artículo 28 de la LGTAIP el cual es "coordinar y evaluar las acciones relativas a la política pública transversal de transparencia, acceso a la información y protección de datos personales, así como establecer e implementar los criterios y lineamientos (...)". En este sentido, el Consejo Nacional se erige como la instancia que

364 Ibídem, p. 10.

365 "Artículo 6: (...)
A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
El organismo garante coordinará sus acciones con la Auditoría Superior de la Federación, con la entidad especializada en materia de archivos y con el organismo encargado de regular la captación, procesamiento y publicación de la información estadística y geográfica, así como con los organismos garantes de las entidades federativas, con el objeto de fortalecer la rendición de cuentas del Estado Mexicano".
Constitución Política de los Estados Unidos Mexicanos (1917). México.

articula la política y las acciones en materia de transparencia a través de la coordinación entre diferentes órganos de gobierno. Por ello el Consejo se integra por los mismos organismos establecidos en el artículo 30 de la LGTAIP,[366] para así llevar a cabo una adecuada protección de estos derechos.

Es por ello que el compromiso con la transparencia no solo está encomendado a todas aquellas dependencias, entidades, organizaciones, individuos y sujetos obligados que precisa la ley para el adecuado trabajo del SNT, sino también para aquellos que necesite el Consejo Nacional. En este rubro, el Consejo Nacional puede extender una invitación institucional cuando la naturaleza de los asuntos concernientes así lo requieran (artículo 33, Ley General de Acceso a la Información Pública y Datos Personales). Estas instancias pueden participar en las reuniones en las que se discute la Política Nacional de Transparencia, y de esta forma mantener en alto las voces de los sujetos obligados para que así puedan ser parte de la discusión.

Aunque en un principio el funcionamiento del Consejo Nacional se previó que trabajaría en sesiones ordinarias y extraordinaria,[367]finalmente la Ley mandata que el funcionamiento del Consejo Nacional no tendrá diferentes tipos de sesiones. Lo anterior, se entiende al estar articulado en Pleno o en comisiones. El Pleno debe reunirse, como mínimo, una vez cada seis meses y para convocar a una asamblea se necesita de una solicitud presentada ya sea por el presidente o por la mayoría absoluta de los miembros, contando, en cualquier caso, con el proyecto de orden del día. Respecto a las comisiones, resulta de gran relevancia que el legislador haya establecido esta posibilidad, debido a que por la especialización de los temas en materia de transparencia este tipo de comisiones permiten que se recurra a especialistas con amplios conocimientos en diversas áreas que participen en la elaboración de los acuerdos.[368]

3. Interpretación literal de la Ley

A. Funcionamiento

El Consejo Nacional está compuesto por organismos e institutos, de los cuales tiene 32 representantes, más cuatro entidades públicas (el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el Instituto Nacional de Estadística y Geografía, la Auditoría Superior de la Federación y Archivo General de la Nación), por lo que para formar el quórum necesario se necesitan 18 miembros y se aprueban los acuerdos con 10 de sus integrantes. Asimismo, el Consejo tiene la opción de establecer comisiones de trabajo, lo cual es un criterio acertado del legislador, ya que existen en la materia ciertos asuntos que necesitan de especialización y experiencia que solo pueden realizarse a través de una instancia colegiada y altamente calificada.

La articulación del Consejo Nacional, su funcionamiento y requerimientos formales, se realiza ya sea en Pleno o en comisiones. El presidente del órgano tiene la facultad de coordinar, armonizar y asegurar el adecuado funcionamiento del Sistema. Sin embargo, aunque esta obligación pareciera solo del Consejo, los distintos miembros del Consejo Nacional también tienen el deber de mejorar el funcionamiento del Sistema Nacional a

366 El Instituto Nacional de Acceso a la Información, los organismos garantes de las entidades federativas, la Auditoría Superior de la Federación, el Archivo General de la Nación y el Instituto Nacional de Estadística y Geografía.

367 Iniciativa con proyecto de decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. 2014. México, p. 11

368 Los acuerdos a que establezcan deben ser avalados por la mitad más uno de los integrantes presentes.

través de la creación y propuesta de proyectos de reglamentos internos o acuerdos. Se puede decir, que solo cuando el que convoca a una sesión de Pleno del Consejo Nacional es el presidente del INAI, es cuando se necesita de una mayoría para convocar la sesión, en los demás casos cualquier miembro puede formular proyectos.

B. Atribuciones y facultades

El Consejo, como órgano colegiado y de conformidad con el artículo décimo del Reglamento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos, tiene como principales atribuciones y facultades el establecimiento de toda la reglamentación, compilación y emisión de normas necesarias para la consecución de los objetivos planteados por el SNT. Asimismo, podrá y deberá establecer programas a nivel nacional que promuevan, investiguen, difundan y *transversalicen* los derechos de transparencia, acceso a la información, protección de datos personales y apertura gubernamental en el país, además, deberán emitir una ruta crítica con los procesos, estrategias, indicadores y directrices, así como códigos de buenas prácticas que consideren necesarios para el cumplimiento de las metas en la agenda de trabajo del SNT.

El Reglamento del Consejo Nacional, en su artículo 5, define a dicho organismo como el órgano colegiado y máximo rector de coordinación y deliberación del SNT. Asimismo, tiene como valores centrales y núcleo institucional los principios de certeza, eficacia, independencia, legalidad, objetividad, profesionalismo, máxima publicidad y transparencia.[369] Por medio de la coordinación y evaluación de las acciones relativas a la política pública transversal de transparencia, acceso a la información y protección de datos personales, así como de la implementación de criterios y lineamiento es que el Consejo Nacional puede impulsar la transparencia y el fortalecimiento de la rendición de cuentas en México.

C. Jurisprudencia y convencionalidad

A pesar de que en la jurisprudencia dictada por cortes internacionales no se establece la existencia de una figura análoga al Consejo Nacional, este órgano es fundamental para la consecución, difusión, garantía y fiscalización de la transparencia, así como de los derechos al acceso a la información y a la protección de datos personales. El Consejo es la materialización e implementación institucional de las recomendaciones que la Corte emitió en el caso "Claude Reyes y otros vs. Chile",[370] en el cual se reconoce el derecho de acceso a la información como un derecho autónomo que debe ser vigilado y propiciado por el Estado. Asimismo, la sentencia decreta la importancia de la transversalización del derecho a la transparencia y acceso a la información como fundamento y núcleo de las democracias constitucionales.

D. Derecho comparado

a) España

En el derecho español, la regulación de los órganos de transparencia es, al igual que en México, a través de la Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno.

369 "Artículo 5. El Consejo Nacional es el órgano colegiado y máximo rector de coordinación y deliberación del Sistema Nacional. De acuerdo con lo establecido por el artículo 34 de la Ley, el Consejo Nacional podrá funcionar en Pleno o en comisiones. El Consejo Nacional regirá su funcionamiento bajo los principios de certeza, eficacia, independencia, legalidad, objetividad, profesionalismo, máxima publicidad y transparencia". Reglamento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. 2015. México.

370 Corte IDH. *Caso "Claude Reyes y otros Vs. Chile"*. Fondo, reparaciones y costas. Sentencia de 19 de septiembre de 2006. Serie C. No. 151. Chile.

En este sentido, en el artículo 33 de esta Ley, se establece el Consejo de Transparencia y Buen Gobierno, el cual es un organismo público encargado de garantizar el derecho de acceso a la información. Si bien, en el derecho español no existe un sistema nacional que integre a los organismos y las instancias garantes en materia de transparencia, establece que el Consejo de Transparencia y Buen Gobierno es el organismo público que tiene como objeto la promoción de la transparencia de la actividad pública, la vigilancia del cumplimiento de las obligaciones de publicidad, la salvaguarda del ejercicio de derecho de acceso a la información pública y la garantía de observancia y materialización de las condiciones de buen gobierno (Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, artículo 34). Dicho órgano se compone por la Comisión de Transparencia y Buen Gobierno. Asimismo, el presidente del consejo será también presidente de la Comisión (Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, artículo 35).

b) Chile

El ordenamiento jurídico chileno tiene como organismo rector de la política en materia de transparencia y protección de datos personales al Consejo para la Transparencia. Dicho Consejo es una corporación autónoma de derecho público, con personalidad jurídica y patrimonio propio (Ley sobre Acceso a la Información Pública, artículo 31). Tiene como objeto la promoción de la función pública, la fiscalización y observancia del cumplimiento de la normatividad sobre publicación de información pública, acceso a la información y transparencia (Ley sobre acceso a la información pública, artículo 32). Asimismo, se le asignan funciones para asegurar la materialización, difusión, promoción y respeto de los derechos de transparencia, acceso a la información y transparencia.[371]

E. Conclusión

La importancia del Consejo Nacional, dentro del ordenamiento jurídico mexicano, radica en la institucionalización de un nuevo arreglo político y jurídico que garantice la protección universal al derecho de acceso a la información pública. Por medio de esta instancia rectora del Sistema Nacional se amplió el alcance de garantía y respeto de este derecho a través del mejoramiento del funcionamiento de los distintos integrantes de dicho sistema.

371 "Artículo 33. El Consejo tendrá las siguientes funciones y atribuciones:
a) Fiscalizar el cumplimiento de las disposiciones de esta ley y aplicar las sanciones en caso de infracción a ellas
b) Resolver, fundadamente, los reclamos por denegación de acceso a la información que le sean formulados de conformidad a esta ley
c) Promover la transparencia de la función pública, la publicidad de la información de los órganos de la administración del Estado y el derecho de acceso a la información, por cualquier medio de publicación
d) Dictar instrucciones generales para el cumplimiento de la legislación sobre transparencia y acceso a la información por parte de los órganos de la administración del Estado, y requerir a éstos para que ajusten sus procedimientos y sistemas de atención de público a dicha legislación.
e) Formular recomendaciones a los órganos de la administración del Estado tendientes a perfeccionar la transparencia de su gestión y a facilitar el acceso a la información que posean
f) Proponer al presidente de la República y al Congreso Nacional, en su caso, las normas, instructivos y demás perfeccionamientos normativos para asegurar la transparencia y el acceso a la información
g) Realizar, directamente o a través de terceros, actividades de capacitación de funcionarios públicos en materias de transparencia y acceso a la información
h) Realizar actividades de difusión e información al público, sobre las materias de su competencia.
i) Efectuar estadísticas y reportes sobre transparencia y acceso a la información de los órganos de la Administración del Estado y sobre el cumplimiento de esta ley
j) Velar por la debida reserva de los datos e informaciones que conforme a la Constitución y a la ley tengan carácter secreto o reservado
k) Colaborar con y recibir cooperación de órganos públicos y personas jurídicas o naturales, nacionales o extranjeras, en el ámbito de su competencia
l) Celebrar los demás actos y contratos necesarios para el cumplimiento de sus funciones.
m) Velar por el adecuado cumplimiento de la ley Nº 19.628, de protección de datos de carácter personal, por parte de los órganos de la administración del Estado". Ley sobre Acceso a la Información Pública, 2008. Chile.

El Consejo es la instancia encargada de dar impulso y garantizar, al mismo tiempo, el cumplimiento y funcionamiento de los objetivos establecidos para el Sistema Nacional de Transparencia, toda vez que opera como un contrapeso democratizador y federalista dentro de la estructura administrativa en México. Su correcto funcionamiento permite la transición hacia un modelo institucional eficaz para la de rendición de cuentas, en el cual exista un sistema integral capaz de inhibir y reducir sensiblemente la corrupción y el mal gobierno a través de la mayor cooperación entre las instituciones en materia de transparencia.

El modelo institucional con el que contamos es un ejemplo de organización, comunicación, colaboración y complementación entre los poderes públicos para garantizar un derecho fundamental para los gobernados y, en consecuencia, para la democracia.

Consentimiento

Luis Manuel C. Meján

1. El concepto general del consentimiento

El consentimiento es un concepto que suele ser estudiado siempre a la luz de la doctrina de los contratos, pues constituye un elemento esencial de estos. Sin embargo, hay que entender que puede haber consentimiento para algún otro acto jurídico que no es propiamente un contrato, ni el acatamiento de una orden. Pueden existir decisiones de autoridades que, sin ser impositivas o coercitivas, pueden ser aceptadas por una persona (elegir una de las alternativas que plantea la ley o la autoridad, aceptar una oferta hecha por la autoridad, decidir ser albacea o tutor, por ejemplo). La expresión de esa conformidad puede darse para una variedad de actos jurídicos, pero toma su significado íntegro cuando se trata de un contrato. En efecto, la voluntad se puede expresar en otro acto jurídico unilateral del cual se derivarán efectos jurídicos, ahí habrá aquiescencia, aceptación, asunción de obligaciones, conformidad, pero no consentimiento.[372]

La Real Academia Española (RAE) lo define con significados, ya como término común, ya como término de derecho, de la siguiente manera: "Acción y efecto de consentir. En los contratos, conformidad que sobre su contenido expresan las partes. Der. Manifestación de voluntad, expresa o tácita, por la cual un sujeto se vincula jurídicamente".[373]

Se trata de un proceso propio de las facultades del ser humano pues intervienen dos facultades psicológicas: el conocimiento y la voluntad, por un lado y, por otro, las condiciones de libertad y de igualdad.

El consentimiento nace de una primera fase cognoscitiva del hombre en la que conjunta la información que será necesaria para la siguiente fase en la que interviene la voluntad inclinándose hacia la decisión de otorgar el consentimiento y celebrar un acto jurídico.

Justamente sobre esa información se ejerce la voluntad, es decir, la apetencia racional, que es la inclinación a hacer aquellas cosas que nuestra razón ha conocido (en oposición a la apetencia sensible o deseo que proviene de los instintos). *Voluntas est, quae quid cum ratione desiderat*. (Existe la voluntad, que es lo que un deseo racional).[374]

372 "La palabra consentimiento se comprende cuando el acto tiene varios autores; pero no es muy exacta cuando el acto depende de la voluntad de una sola persona". Planiol, M y Ripert, G. (2000). *Derecho Civil*. Primera Serie. Volumen 8. Editorial Oxford. México, p. 40.

373 http://dle.rae.es/?id=AP6QLrg

374 Cicerón, T. (2005) *Disputaciones Tusculanas* (B.C.G 332), México, Gredos, p. 3.

El otorgamiento del consentimiento supone también el concepto de igualdad de los seres humanos. Si los seres humanos no participan con igualdad, los contratos serían imposibles. La igualdad no significa un conocimiento, experiencia o posición cultural o económica idénticas, eso es imposible, todos tienen un bagaje cultural y de información diverso, la igualdad supone que, aunque hay diferencias en esas situaciones, ambas partes concurren con la misma dignidad y la misma presencia ante el derecho a la convención.

El ejercicio de la voluntad (apetito racional), en un plano de igualdad en lo esencial, es lo que constituye la libertad contractual y ayuda a decir sobre la medida, los límites y las condiciones de los efectos jurídicos que han de desencadenarse.[375]

2. La estructura jurídica del consentimiento

Consentimiento, del latín: *cum-sentire* "sentir con", supone la participación de más de una persona que expresan su voluntad. Por ello, el consentimiento forma parte de la esencia del contrato, si no concurren las voluntades de quienes celebran ese acto jurídico, podrán darse algunas consecuencias de derecho, pero no habrá contrato. La pluralidad de sujetos es esencial, lo tradicional es que sean dos partes, pero pueden concurrir muchas más como en los casos de obligaciones complejas (simple mancomunidad, solidaridad, indivisibilidad) o en los casos de contratos concurrentes (asociación, sociedad). Todos ellos "sienten juntos".[376] Incluso en el contrato de adhesión, en donde el objeto del contrato está definido por una sola de las partes, lo que hace el contratante es aceptar y concurrir con lo que el otro quiere.

El consentimiento recae sobre algo, es decir sobre un objeto (segundo elemento de esencia de los contratos) que debe ser lícito y posible (física y jurídicamente).[377] Las voluntades pueden ser sobre cosas disímbolas aunque concurrentes, pues la prestación que busca obtener una parte es distinta a la que busca la otra parte, pero en el fondo ambas partes quieren que cada una obtenga lo que se proponen en conjunto (el comprador quiere adquirir un artículo o servicio y el vendedor busca recibir el precio, pero ambos están de acuerdo en que ambos obtengan lo que quiere cada uno).

El resultado del otorgamiento del consentimiento genera la vinculación entre las partes al darse la producción de efectos jurídicos: creación, modificación, transmisión o extinción de derechos y obligaciones.[378] Estos efectos estarán protegidos por el sistema jurídico a fin de que cada parte cumpla y reciba lo convenido.

En el mapa de la formación del consentimiento hay tres zonas: a) la voluntad interna, es decir, lo que está en el interior de cada una de las partes al concluir su proceso psicológico de información y voluntad; b) La declaración o expresión de dicha voluntad interna. Esto

375 "Cada convención, cada contrato, es una muestra de la libertad del ser humano. Si la actuación de los hombres fuera impuesta, ya por una autoridad, ya por otra entidad superior capaz de imponerse, entonces no habría contrato. Habría Ley, habría sentencia, habría acto administrativo, habría acto de autoridad, habría actos jurídicos unilaterales, pero no existiría en el mundo del derecho el fenómeno contrato". Mejan, L. (2004). *Contratos Civiles. Ayuda de Memoria*. Editorial Oxford. México, pp. 200 y 201.

376 "El consentimiento es el acuerdo de voluntades constitutivos del Contrato. Dos o más personas, por tanto, dos voluntades, son necesarias, por lo menos, para que haya consentimiento y, por ende, contrato. Pero el contrato puede existir entre un mayor número de personas, como lo demuestran las sociedades." Bonnecase, J. (1997). *Tratado Elemental De Derecho Civil* (Parte B). Volumen 2. Editorial Harla. México, pp. 794.

377 "El consentimiento implica la expresión externa de las voluntades que coincidan en el objeto del acto, pues no basta la expresión de voluntad unilateral si no hay acuerdo sobre la materia o naturaleza del acto y sobre la identidad de la cosa (error obstáculo) o sobre el negocio y la cosa a realizar". Baqueiro, E. (2004). *Diccionarios Jurídicos Temáticos/ Derecho Civil.* Volumen I. Editorial Oxford. México, pp. 25-26.

378 "Acuerdo entre dos o más voluntades acerca de la producción o transformación de derechos y obligaciones". De Pina Vara, R. (2003). *Diccionario de Derecho*. Trigésima Primera Edición. Editorial Porrúa. México, p. 183.

es, ya que el derecho no puede operar sobre la psique de los sujetos, es necesario que los afectados manifiesten su voluntad. Dicha voluntad puede ser expresa (cuando es mediante signos inequívocos) o tácita (cuando la conducta del sujeto solo puede interpretarse como un consentimiento) y c) el acuerdo o voluntad común, en donde ambas declaraciones coinciden y cuando puede decirse que el contrato está celebrado.[379]

El camino del contrato sigue, usualmente, dos momentos: el de la policitación u oferta y el de la aceptación, que es cuando cada una de las partes expresa su voluntad en el sentido de obligarse en los términos que se proponen. Cuando ambas propuestas coinciden, se ha formado el contrato.[380] Esta formación del contrato por coincidencia de los consentimientos puede requerir una serie de ofertas entre las partes (que en el lenguaje común se conocen como "negociaciones") hasta llegar a la concurrencia.[381]

Este camino puede darse cuando ambas partes están presentes (ya sea en persona o comunicándose por un medio tecnológico que produce el mismo efecto de la presencia física en un solo lugar) o ausentes (usando un medio de comunicación que transporta la policitación y la aceptación). Las leyes regulan este proceso asignando tiempos y presunciones para determinar el momento en que han coincidido las voluntades y el consentimiento se ha formado. El Código Civil Federal Mexicano sigue el camino de la recepción, es decir, considera el consentimiento —y por ende, el contrato— formado, cuando el oferente recibe la aceptación de parte del aceptante.[382]

Respecto a la calidad del consentimiento, éste debe de ser expresado cuando se ha tenido la información correcta y cuando no ha habido una presión limitante de la voluntad, es decir, libre de vicios como errores, ya sea espontáneos, inducidos o tolerados, por dolo o mala fe; temores, por violencia ejercida o a sufrir una represalia si no se otorga; o abuso en el equilibrio de los valores de las prestaciones de cada una de las partes o por aprovechamiento de la necesidad, ignorancia o inexperiencia o miseria de una de las partes.

Al consentimiento, entendido, como se ha explicado, como la expresión de la voluntad de dos partes que convienen en un determinado objeto que les vincula jurídicamente, se le han añadido, en diversas legislaciones, algunas condiciones peculiares, por ejemplo, la nueva redacción introducida al código civil francés exige que la voluntad sea libre e íntgra;[383] mientras que el código civil de España adhiere la causa de constituir el contrato[384] y el código civil de Jalisco impone a las partes las mismas condiciones que apelan a un principio de ejecución del negocio.[385]

379 Véase en este sentido a Diez-Picazo, L. (2007). *Fundamentos del Derecho Civil Patrimonial.* Tomo I. Introducción Teoría del Contrato. Sexta edición. Thompson Reuters. Navarra, pp. 187 y siguientes; y a Robles, D. (2011). *Teoría General de las Obligaciones*. Editorial Oxford. México, p. 155.

380 "Oferta y aceptación. Uno de los futuros contratantes propone a otro las condiciones de un contrato; esto es lo que se llama oferta o policitación. Si el otro se muestra conforme con ellas, les da su aceptación queda formado el consentimiento". Borja, M. (2012). *Teoría General de las Obligaciones*. Editorial Porrúa. México, p. 121.

381 Bejarano cita a Joaquín Martínez Alfaro quien afirma: "El consentimiento se puede formar de un modo instantáneo o de un modo progresivo… será progresivo cuando el aceptante discute la oferta imponiendo condiciones o pidiendo que se modifiquen los términos de la oferta". Bejarano, M. (2010). *Obligaciones Civiles*. Editorial Oxford. México, pp. 51-56.

382 Código Civil Federal: Artículo 1807. El contrato se forma en el momento en que el proponente reciba la aceptación, estando ligado por su oferta, según los artículos precedentes.

383 El Artículo 1112-1 del Código Civil de Francia impone la obligación a las partes de darse toda la información relevante para que la otra parte pueda otorgar su consentimiento de manera informada, "Las partes no pueden ni limitar ni excluir este deber". Véase Benabent, A. (2017). *Droit des Obligations.* LGDJ Lextenso. Paris, pp. 67. El Código Civil de Jalisco consagra como vicio del consentimiento una figura similar a la que llama "reticencia". Artículo 1289 de dicho código.

384 El artículo 1266 indica: "El consentimiento se manifiesta por el concurso de la oferta y la aceptación de la cosa y la casusa que han de constituir el contrato". Editorial Civitas. 24 edición. Madrid 2001. "Requisito básico para el perfeccionamiento del Contrato que consiste en la manifestación de la voluntad de celebrarlo y de conformidad con su objeto y causa" *CC, Arts. 1254, 1261 y 1262. RAE. (2016). *Diccionario del Español Jurídico*. Primera Edición, pp. 480. (Énfasis añadido).

385 Artículo 1271 "…convienen en un mismo objeto y unas mismas condiciones y además en la conducta de ellas existe un principio de ejecución del negocio…". Código Civil de Jalisco. Edición del Congreso del Estado de Jalisco. Guadalajara, 1995.

Una vez expresado el consentimiento sobre un objeto, el contrato está formado y ordinariamente no es posible deshacerlo o revocarlo por la voluntad de una sola de las partes. El vínculo jurídico que han creado requiere, para su revocación, de nuevo el consentimiento de ambas partes o la decisión judicial que resuelve el conflicto. Existen algunas excepciones específicas en las legislaciones, especialmente en el caso de contratos *intuitus personae*, en donde es posible que la relación jurídica concluya por la voluntad de una sola de las partes, pero aún en esos casos pueden aparecer obligaciones de indemnización o de reparación de daños y perjuicios.

3. El consentimiento en materia de manejo de datos personales

El régimen de tratamiento de los datos personales está regulado por una ley aplicable a los datos que recaban, usan y conservan los particulares, la Ley Federal de Protección de Datos en Posesión de los Particulares (LFPDPPP), por otra ley relativa a cuando el responsable es una entidad pública, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) así como por la adhesión de México a algunos cuerpos internacionales como La Red Iberoamericana de Protección de Datos (RIPD)[386] que han emitido diversos instrumentos orientadores para las legislaciones nacionales de las jurisdicciones y organizaciónes que forman parte, por ejemplo los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos).

En todas estas estructuras jurídicas se advierte la necesidad de que los titulares de los datos personales que obran en poder de una entidad, privada o pública, que los usará, conservará y tratará acepten el manejo que de ellos hará el responsable (persona física o moral de carácter privado que decide sobre el tratamiento de datos personales). Esas normas requieren que el responsable que los recaba tenga la obligación de informar a través del aviso de privacidad el uso que hará de los mismos.

Es prácticamente un contrato de adhesión en el que el responsable se obliga a recabar, conservar y usar los datos de determinada manera y el titular de los mismo acepta que se haga así. Cuando la relación entre el titular y el responsable supone el ofrecimiento de un bien o servicio, el pacto de datos personales puede considerarse como un contrato o cláusula accesorios al contrato principal.

Ninguna operación será posible si el titular no manifiesta previamente estar enterado de ese aviso. En operaciones por internet, y algo similar sucede en algunos contratos escritos, la posibilidad de acordar la adquisición de un bien o servicio no puede continuar si no se ha manifestado el consentimiento con los términos fijados. El manifestar conocerlos ¿supone consentimiento? Sí, es la manera de exteriorizar la conformidad con tales términos.

Las normas referidas incluyen una definición de "consentimiento". La LFPDPPP dice: "Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos" (artículo 3, fracción IV); la LGPDPPSO dice a su vez: "Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos" y los Estándares Iberoamericanos dicen: "Manifestación de la voluntad, libre, específica, inequívoca e informada del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen". (artículo 2.1 b).

386 Red Iberoamericana de Protección de Datos (RIPD o Red): organización integrada por autoridades reguladoras del manejo y protección de datos de 10 países que cuenta, además, con instituciones observadoras de otras 13 jurisdicciones. Surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, dando cumplimiento a uno de los acuerdos adoptados en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada el 28 y 29 de octubre de 2016 en Colombia.

Como puede verse, los tres coinciden en que:

a) es una manifestación de voluntad
b) el emisor de tal manifestación es el titular de los datos
c) el objeto de la voluntad es el tratamiento de los datos

Es interesante que los dos últimos cuerpos normativos califican la expresión de la voluntad exigiendo que sea libre (sin vicios), específica (sobre el objeto del tratamiento de los datos), informada (una vez conocido cómo los piensa tratar el responsable) e inequívoca (que no haya duda).

En suma, puede decirse que el consentimiento debe, como en cualquier caso, estar libre de vicios, pero requiere además dos requisitos: a) que sea informado, esto es, que el otorgante haya tenido oportunidad de conocer el contenido del tratamiento que el responsable dará a los datos personales, ordinariamente a través del aviso de privacidad y b) que quede clara la finalidad del acopio y uso de los datos personales pues fuera de esta finalidad no pueden ser usados tales datos.

Otorgar tal consentimiento es imperativo para todo tratamiento de datos personales, tanto para el prestador de bienes o servicios o responsable, como para el que con él contrata o tiene alguna otra relación jurídica (LFPDPPP artículo 8).

Los Estándares admiten que conforme al derecho interno de cada jurisdicción puedan establecerse excepciones a la obligatoriedad de obtener el consentimiento de los titulares (Estándares 4.4). En tal sentido se expresan la LFPDPPP (artículos 10 y 37) y la LGPDPPSO (artículos 11 y 12) que contienen excepciones específicamente establecidas las cuales deben interpretarse *numerus clausus*.

Las excepciones refieren a aquellos casos en donde sean ya públicos, así lo permita la ley, se trate de grupos de sociedades, sean necesarios para desahogar una función pública, para defensa de los derechos del titular ante autoridad, para ejecutar un contrato con el titular, cuando la ley lo ordene, en casos de interés público y en casos de satisfacción de intereses legítimos, como es el caso de tratamientos médicos o de localización de personas físicas y otras razones similares.

Aun cuando se regula que el consentimiento puede ser expreso o tácito, en el caso de datos personales sensibles,[387] el consentimiento debe ser otorgado de forma expresa y por escrito en forma autógrafa o con alguno de los medios tecnológicos de formación del consentimiento.

Este consentimiento, a diferencia de lo que sucede en la contratación ordinaria, es esencialmente revocable pues supone el total dominio de la persona sobre los datos de los que es titular. La revocación debe estar prevista justamente en las políticas del responsable y formar parte del Aviso de Privacidad, con lo cual el camino de la revocación es parte del consentimiento otorgado.

En la Unión Europea, en mayo de 2018, entró en vigor el nuevo Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés),[388] que reemplazó la Directiva de Protección de Datos 95/46/ CE. El RGPD arroja una luz adicional y una ratificación a lo establecido en otros cuerpos legales como los aquí citados. Además, añade algunos conceptos interesantes.

387 Véase el concepto de datos personales sensibles en los artículos 3, fracción VI de la LFPDPPP, 3 Fracción X de la LGPDPPSO y en el 2.1 d) de los Estándares.

388 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0&tab=2

Al reproducir en los considerandos el concepto de consentimiento, se prevé que tiene que ser libre, informado e inequívoco y añade que el silencio o la inacción del titular no deben ser considerados como consentimiento. Ratifica la obligación imperativa de obtener el consentimiento del titular y menciona también casos en donde esta obligación puede ser obviada.

Los considerandos dan normas sobre lo que significa que el consentimiento sea informado, libre y lícito.

Para que el consentimiento sea informado, el GDPR requiere que se "proporcione un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas". Deberá incluirse, además, la identidad del responsable y los fines de la recaudación de datos personales. (Párrafo 42).

Para que sea libre, "no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento". (Párrafo 43).

El tratamiento debe ser lícito "cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato". (Párrafo 44).

El texto del reglamento tiene una definición de consentimiento del interesado que incluye la necesidad de ser expreso y admite una clara acción, como un camino tácito: "Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". (artículo 4).

Posteriormente dedica el artículo 7 para hablar de las condiciones para el consentimiento, el cual requiere que el responsable sea capaz de probar que cuenta con él y establece los formatos de solicitud en lenguaje claro y sencillo, sostiene la revocabilidad esencial del mismo y que el servicio o bien brindado no supedite su otorgamiento a obtener el consentimiento sobre datos que no son necesarios para dicho bien o servicio.

El reglamento europeo incluye normas especiales relativas al consentimiento en casos de niños o de diversas categorías, en donde aparecen, entre otras, los llamados "datos sensibles" y los fines de interés público.

Puede decirse, en suma, que el concepto "consentimiento", aunque parte de su tratamiento tradicional como figura jurídica, toma dimensiones especiales cuando es aplicado a la obtención, conservación y tratamiento de datos personales.

Consentimiento expreso

Isabel Davara Fernández de Marcos,[389]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El consentimiento[390] para el tratamiento de los datos personales es definido —tanto en la normatividad aplicable para el sector privado que es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), como para la del sector público que es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)— como la manifestación de la voluntad del titular mediante la cual acepta que sus datos personales sean tratados por el responsable en términos del aviso de privacidad que le fue puesto a su disposición.[391]

El consentimiento tiene que ser libre, específico, inequívoco e informado (como se ha visto en la voz referida a consentimiento), revistiendo diferentes formas. El consentimiento se puede manifestar de manera tácita o de forma expresa, según se actualicen de unos u otros elementos específicos. El consentimiento tácito es aquél que, en pocas palabras, se consigue del titular mientras —una vez informado sobre sus alcances— no manifieste su oposición. El consentimiento expreso, por su parte, requiere ser patente, especificado,[392] lo que significa que requiere de una acción afirmativa por parte del titular.

El consentimiento expreso puede manifestarse verbalmente, ya sea por escrito, por medios electrónicos, ópticos, por cualquier otra tecnología, o por signos inequívocos.[393] Sin embargo, en el caso de datos personales sensibles, se exige la forma escrita, ya sea mediante firma autógrafa, firma electrónica o mecanismo de autenticación equivalente.[394]

La manifestación verbal del consentimiento es aquélla en la que el titular estipula su otorgamiento mediante su propia palabra y no de forma escrita.[395] El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) disponen así que el consentimiento expreso se otorga de forma verbal cuando el titular lo externa oralmente de manera presencial o mediante el uso de cualquier tecnología,[396] ya sea física o electrónica, que permita el registro de cualquier locución acústica por conducto de la cual se pueda acreditar una manifestación de la voluntad del titular de los datos o de su representante legal debidamente acreditado.

Por otro lado, se considera que el consentimiento expreso se ha otorgado por escrito en el momento en el que el titular externa su voluntad mediante un documento que contiene su firma autógrafa, huella dactilar, firma electrónica, firma electrónica avanzada[397] o

389 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

390 Para una ulterior referencia se recomienda consultar las voces "consentimiento", "consentimiento tácito", "consentimiento expreso y por escrito", y "principio de consentimiento" presentes en este Diccionario de Protección de Datos Personales.

391 *Vid*, artículo 3, fracción IV de la LFPDPPP y artículo 3, fracción VIII de la LGPDPPSO.

392 RAE. (2018). "Expreso". En *Diccionario de la Lengua Española*. Disponible en: http://dle.rae.es/?id=HL8veMX

393 *Vid*, artículo 8, segundo párrafo de la LFPDPPP y artículo 21 de la LGPDPPSO.

394 *Vid*, artículo 9 de la LFPDPPP y artículo 21 de la LGPDPPSO.

395 RAE. (2018). "Verbal". En *Diccionario de la Lengua Española*. Disponible en: http://dle.rae.es/?id=bazFRtf

396 Artículo 18 del RLFPDPPP y artículo 17 de los Lineamientos Generales.

397 Recomendamos consultar las definiciones de firma electrónica y firma electrónica avanzada presentes en este *Diccionario de Protección de Datos Personales*.

cualquier otro mecanismo o procedimiento de autenticación equivalente que al efecto se establezca y permita identificar al titular y recabar su consentimiento de forma lícita.[398]

En consecuencia, para que el consentimiento se considere expreso es requerida una acción afirmativa clara o mediante una declaración verbal o escrita por parte del titular de los datos,[399] a través de la cual se pueda acreditar que éste, de manera libre, específica e informada ha aceptado que se lleve a cabo el tratamiento de sus datos personales para fines explícitos y determinados.[400] Es decir, el consentimiento debe ser inequívoco, requisito que se cumple cuando existen elementos que de manera indubitable demuestran que el mismo ha sido lícitamente otorgado por el titular.

Como adelantábamos en la primera parte de la definición, el consentimiento expreso debe ser libre, especifico, inequívoco e informado.[401] De acuerdo con la normatividad de datos personales, dichas características del consentimiento expreso consisten en lo siguiente:

- Libre: cuando el consentimiento expreso es obtenido sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular.
- Específico: cuando el consentimiento expreso se refiere de forma concreta, explícita y lícita a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales. Este requisito se cumple cuando la solicitud del consentimiento va relacionada con las finalidades concretas del tratamiento que se informan en el aviso de privacidad. Es decir, con base en esta característica, el consentimiento se debe solicitar para tratar los datos personales para finalidades específicas, no en lo general.[402]
- Informado: cuando de forma previa al otorgamiento del consentimiento, se hace del conocimiento del titular de los datos personales, el aviso de privacidad en virtud del cual se informa sobre el tratamiento al que serán sometidos los datos personales y las consecuencias de otorgar su consentimiento.

En ausencia de cualquiera de las mencionadas características, el consentimiento no puede considerarse válido.

Además de lo anterior, el consentimiento es revocable, de modo que el titular tiene la posibilidad de revocarlo en cualquier momento y el responsable, la correlativa obligación de establecer mecanismos sencillos y gratuitos que le permitan al titular ejercer dicho de-

398 Artículo 19 del RLFPDPPP y artículo 17 de los Lineamientos Generales.

399 En este sentido, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos disponen:
"12. Condiciones para el consentimiento
12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará, de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara".

400 De esta manera, encontramos que el Reglamento General de Protección de Datos dispone en su considerando 32 lo siguiente: "32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se da a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta [...]".

401 De acuerdo con lo previsto por el artículo 12 del RLFPDPPP y el artículo 20 de la LGPDPPSO.

402 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 18. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf Fecha de consulta: 30 de noviembre de 2018.

recho (al menos por el mismo medio por el que lo otorgó) siempre y cuando no lo impida una disposición legal.[403]

En cuanto a los supuestos en los que es obligatorio obtener un consentimiento expreso, y no así uno tácito, podemos señalar los siguientes:

- Lo exija una ley o reglamento
- Se trate de datos financieros o patrimoniales
- Se trate de datos sensibles
- Lo solicite el responsable para acreditar el mismo
- Lo acuerden así el titular y el responsable

Para la obtención del consentimiento expreso, el responsable se encuentra obligado a facilitar al titular un medio sencillo y gratuito para el otorgamiento del mismo y que le permita acreditar y documentar, de manera indubitable, que el consentimiento fue otorgado, ya sea a través de una declaración o una acción afirmativa clara.[404] En el sector público, de forma análoga a lo que dispone el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés), en su considerando 32,[405] se indica, además, que no constituyen consentimiento expreso las casillas previamente marcadas, la inacción o cualquier otra conducta similar.[406]

En consecuencia, para legitimar el tratamiento de datos personales mediante el consentimiento expreso es necesario que el titular señale expresamente que consiente el tratamiento de sus datos personales, pues si no existe dicha manifestación expresa, el responsable no podrá tratar los datos personales. Es decir, es necesario que el titular diga que sí explícitamente.[407]

En este contexto, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) indica que el consentimiento expreso se puede obtener a través del aviso de privacidad o de cualquier otro documento físico o electrónico que determine el responsable. Es decir, no se considera necesario que el consentimiento se obtenga por medio del aviso de privacidad, por lo que podrá recabarse, por ejemplo, a través de una grabación telefónica o de una casilla en formato electrónico.[408]

---

403 Artículo 21 del RLFPPP y artículo 20 de los Lineamientos Generales.

404 Artículo 19 del RLFPDPPP y artículo 16 de los Lineamientos Generales.

405 En este sentido, encontramos que el Reglamento General de Protección de Datos dispone, en su considerando 32, lo siguiente: "32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta [...]".

406 Artículo 16 de los Lineamientos Generales.

407 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 18. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf Fecha de consulta: 30 de noviembre de 2018.

408 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 21.

Otro aspecto que conviene considerar es el de la carga de la prueba[409] de la obtención del consentimiento, pues la obligación de demostrar su lícita obtención recae, en todos los casos, en el responsable del tratamiento,[410] por lo que dependiendo de la modalidad del consentimiento que se involucre, el responsable deberá generar las pruebas válidas en derecho que le permitan acreditar ante la autoridad, en caso de ser requerido, la lícita obtención del consentimiento.[411] En relación con esta carga probatoria, es fundamental tener presente que el responsable podrá valerse de pruebas electrónicas, ya que éstas tienen plena validez en términos de la legislación civil,[412] misma que es supletoria a la normatividad de protección de datos personales.

Finalmente, no debe perderse de vista que al igual que el resto de las modalidades del consentimiento, el consentimiento expreso también es susceptible de estar excepcionado, es decir, no será necesario, bajo los supuestos previstos en los artículos 10 y 37 de la LFPDPPP y artículos 22 y 70 de la LGPDPPSO.

El hecho de que no se requiera el consentimiento para el tratamiento, no implica que no se deban cumplir los otros principios (licitud, calidad, lealtad, finalidad, información, proporcionalidad y responsabilidad), lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.[413]

409 Los Estándares de Protección de Protección de Datos Personales para los Estados Iberoamericanos coinciden al señalar: "12. Condiciones para el consentimiento
12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara".
De la misma forma, el Reglamento General de Protección de Datos en el apartado 1 de su artículo 7 indica lo siguiente: 1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales […]".

410 Artículo 20 del RLFPDPPP y último párrafo del artículo 16 de los Lineamientos Generales.

411 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 23. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

412 "Artículo 210-A. Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta".

413 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 23.

Consentimiento expreso y por escrito

Isabel Davara Fernández de Marcos,[414]
Gregorio Barco Vega y
Alexis Cervantes Padilla

En función de la naturaleza de los datos personales, el consentimiento puede ser tácito, expreso y expreso y por escrito.[415]

De forma general,[416] el consentimiento es definido en la normatividad de datos personales como "la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos".[417]

El consentimiento tiene que ser libre, específico, inequívoco e informado (como se ha visto en la voz referida a consentimiento), revistiendo diferentes formas. El consentimiento se puede manifestar de manera tácita o de forma expresa, según se actualicen de unos u otros elementos específicos. El consentimiento tácito es aquél que se obtiene del titular mientras éste, una vez informado sobre su alcance, no manifieste su oposición. El consentimiento expreso, por su parte, requiere ser claro, patente y especificado,[418] lo que significa que requiere de una acción afirmativa por parte del titular. Es decir, si la voluntad del titular de los datos no es clara o específica, no se cumple con dicho requisito como base para la legitimación del tratamiento de los datos personales. Al añadir el elemento "escrito", lo que se incorpora es la obligación de que el consentimiento conste en cualquier documento (incluyendo también el denominado mensaje de datos o documento electrónico).[419]

El consentimiento expreso y por escrito, con firma autógrafa, firma electrónica o mecanismo de autenticación equivalente es obligatorio en los siguientes casos:

- Se trate de datos sensibles[420]
- Lo exija una ley o reglamento[421]
- Lo solicite el responsable para acreditar el mismo
- Lo acuerden así el titular y el responsable

Así, se considera que el consentimiento expreso se ha otorgado por escrito en el momento que el titular externa su voluntad mediante un documento que contiene su firma autógrafa, huella dactilar, firma electrónica, firma electrónica avanzada[422] o cualquier otro

---

414 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

415 *Vid*, artículo 9 de la LFPDPPP y artículo 21 de la LGPDPPSO.

416 Para una ulterior referencia, se recomienda consultar las voces "consentimiento", "consentimiento tácito", "consentimiento expreso" y "principio de consentimiento" presentes en este *Diccionario de Protección de Datos Personales*.

417 *Vid*, artículo 3, fracción IV de la LFPDPPP y artículo 3, fracción VIII de la LGPDPPSO.

418 RAE. (2018). "Expreso". En *Diccionario de la Lengua Española.* Disponible en: http://dle.rae.es/?id=HL8veMX

419 RAE. (2018). "Escrito". En *Diccionario de la Lengua Española.* Disponible en: http://dle.rae.es/?id=HL8veMX ttp://dle.rae.es/?id=GKRIYhs

420 Artículo 9 de la LFPDPPP y último párrafo del artículo 21 de la LGPDPPSO.

421 En este contexto, el INAI precisa que es importante tomar en cuenta que si una ley o reglamento, en lo particular, exige el consentimiento expreso o expreso y por escrito para el tratamiento, el responsable deberá solicitarlo de esa forma, aunque no se trate de datos financieros, patrimoniales o sensibles. INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 18. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf Fecha de consulta: 30 de noviembre de 2018.

422 Recomendamos consultar las definiciones "firma electrónica" y "firma electrónica avanzada" presentes en este *Diccionario de Protección de Datos Personales.*

mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento de forma lícita.[423]

En este punto, es importante señalar que el artículo 1803 del Código Civil Federal (CCF)[424] considera consentimiento expreso a aquel manifestado por medios electrónicos, ópticos, o de cualquier otra tecnología. Del mismo modo, el artículo 1834 bis del CCF[425] y los artículos 93 y 93 bis del Código de Comercio [426] establecen que el requisito de escrito para los contratos que incluyan la manifestación de voluntad en la que consiste el consentimiento, se cumple mediante el uso de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información sea íntegra, atribuible a las personas obligadas y accesible para su ulterior consulta. En este orden de ideas, es importante recordar que la carga de la prueba[427] recae en el responsable del tratamiento, quien[428] deberá generar las pruebas válidas en derecho que le permitan acreditar, ante la autoridad, en caso de ser requerido, la lícita obtención del consentimiento. [429] En relación con esta carga probatoria, es fundamental tener presente que el responsable podrá valerse de pruebas electrónicas (ya tienen plena validez en términos de la legislación civil)[430] y que es supletoria a la normatividad de protección de datos personales.

---

423 Artículo 19 del RLFPDPPP y artículo 17 de los Lineamientos Generales.

424 "Artículo 1803. El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
1. Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos (…)".

425 "Artículo 1834 Bis. Los supuestos previstos por el artículo anterior se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta".

426 "Artículo 93. Cuando la ley exija la forma escrita para los actos, convenios o contratos, este supuesto se tendrá por cumplido tratándose de Mensaje de Datos, siempre que la información en él contenida se mantenga íntegra y sea accesible para su ulterior consulta, sin importar el formato en el que se encuentre o represente. Cuando adicionalmente la ley exija la firma de las partes, dicho requisito se tendrá por cumplido tratándose de mensaje de datos, siempre que éste sea atribuible a dichas partes.
Artículo 93 bis. Sin perjuicio de lo dispuesto en el artículo 49 de este Código, cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho respecto a un Mensaje de Datos: Si existe garantía confiable de que se ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como Mensaje de Datos o en alguna otra forma, y De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar. Para efectos de este artículo, se considerará que el contenido de un Mensaje de Datos es íntegro, si éste ha permanecido completo e inalterado independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación. El grado de confiabilidad requerido será determinado conforme a los fines para los que se generó la información y de todas las circunstancias relevantes del caso".

427 Los Estándares de Protección de Protección de Datos Personales para los Estados Iberoamericanos coinciden al señalar:
"12. Condiciones para el consentimiento
12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara".
De la misma forma, el Reglamento General de Protección de Datos en el apartado 1) de su artículo 7 indica lo siguiente:
"1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales […]".

428 Artículo 20 del RLFPDPPP y último párrafo del artículo 16 de los Lineamientos Generales.

429 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 23.

430 "Artículo 210-A. Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta". (Énfasis agregado).

Para la obtención del consentimiento expreso y por escrito, el responsable se encuentra obligado a facilitar al titular un medio sencillo y gratuito para su otorgamiento. Así, el consentimiento expreso y por escrito puede ser recabado a través del aviso de privacidad o de cualquier otro documento físico o electrónico que determine el responsable. Es decir, no es obligatorio que el consentimiento se obtenga por medio del aviso de privacidad, sino que se puede obtener a través de un formato o contrato, o de una casilla en formato electrónico, por ejemplo, habiendo puesto siempre de manera previa a disposición el aviso de privacidad.[431]

En consecuencia, para que el consentimiento se considere expreso y por escrito es requerida una declaración escrita por parte del titular de los datos o el uso de cualquier otro mecanismo de autenticación equivalente[432] a través de la cual se pueda acreditar que éste, de manera libre, específica e informada ha aceptado que se lleve a cabo el tratamiento de sus datos personales para fines explícitos y determinados.[433]

En cuanto a sus características, el consentimiento expreso y por escrito debe ser libre, inequívoco, específico e informado.[434] De acuerdo con la normatividad de datos personales dichas características consisten en lo siguiente:

- Libre: cuando el consentimiento es obtenido sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular.
- Específico: cuando el consentimiento se refiere de forma concreta, explícita y lícita a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales. Es decir, como lo indica el INAI, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.[435]
- Informado: cuando de forma previa al otorgamiento del consentimiento, se hace del conocimiento del titular de los datos personales el aviso de privacidad en virtud del cual se informa sobre el tratamiento al que serán sometidos los datos personales y las consecuencias de otorgar su consentimiento.
- Inequívoco: el consentimiento es inequívoco cuando existen elementos que, de manera indubitable, demuestran que ha sido lícitamente otorgado por el titular.

En ausencia de dichas características, el consentimiento no puede considerarse como lícitamente otorgado.

---

431 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 23. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

432 En este sentido, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos disponen:
"12. Condiciones para el consentimiento
12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara".

433 En este sentido, encontramos que el Reglamento General de Protección de Datos dispone lo siguiente:
"[…] 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento […]".

434 Según lo previsto por el artículo 12 del RLFPDPPP y el artículo 20 de la LGPDPPSO.

435 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 23. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Además, el consentimiento es revocable, de modo que el titular tiene la posibilidad de revocarlo en cualquier momento y el responsable la correlativa obligación de establecer mecanismos sencillos y gratuitos, que permitan al titular ejercer dicho derecho al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.[436]

Sobre este particular, debe destacarse también que, como cualquier modalidad del consentimiento, el consentimiento expreso y por escrito también es susceptible de estar excepcionado bajo los supuestos previstos en los artículos 10 y 37 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), y los respectivos 22 y 70 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), por lo que cuando el consentimiento pueda ampararse en cualquiera de dichos presupuestos lógicos, no será necesario solicitarlo al titular para tratar o transferir sus datos personales. No obstante, el hecho de que no se requiera el consentimiento para el tratamiento, no implica que no se deberán cumplir los otros principios, lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.[437]

Consentimiento otorgado por medios electrónicos

Jonathan Gabriel Garzón Galván

El consentimiento es uno de los elementos base y esenciales para la existencia de cualquier contrato o convenio, sin él no sería posible vincular a una persona con las obligaciones y compromisos descritos en un documento. El consentimiento consiste en el acuerdo de dos o más voluntades sobre la producción o transmisión de obligaciones y derechos, siendo necesario que estas voluntades tengan una manifestación exterior.[438] La Real Academia Española (RAE)[439] nos aporta las siguientes acepciones:

> consentimiento
>
> 1. m. Acción y efecto de consentir.
>
> 2. m. En los contratos, conformidad que sobre su contenido expresan las partes.
>
> 3. m. Der. Manifestación de voluntad, expresa o tácita, por la cual un sujeto se vincula jurídicamente.
>
> consentir
>
> 1. tr. Permitir algo o condescender en que se haga.

Por su parte, Ricardo Treviño García define el consentimiento como:

> Un acuerdo de voluntades que implica la existencia de un interés jurídico: en el caso particular del contrato, ese interés consiste en la creación o transmisión de derechos reales o personales en la formación del consentimiento, nos encontramos siempre con una oferta o policitación, nombre que se le da a la proposición de celebrar un contrato, y con un asentamiento o conformidad a dicha oferta, que se denomina aceptación. A la persona que formula la oferta se le llama oferente, proponente o solicitante, y a la que otorga la aceptación, aceptante.[440]

436 Artículo 21 del RLFPDPPP y artículo 20 de los Lineamientos Generales.

437 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 23. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

438 Borja, M. (1998). *Teoría General de las Obligaciones*. Porrúa. México, p. 121.

439 RAE. (2017). *Diccionario de la Lengua Española.*Recuperado de: http://dle.rae.es/ Fecha de consulta: agosto 2018.

440 Treviño, R. (2003). *Contratos Civiles y sus Generalidades*. Mcgraw-Hill. México, p. 82.

Tomando en cuenta los puntos anteriores, los actos jurídicos (en especial los convenios o contratos) deben reunir ciertos elementos esenciales para que tengan existencia y algunos requisitos para su plena validez. En relación con los contratos y sus elementos esenciales, en el artículo 1794 del Código Civil Federal (CCF)[441] encontramos que son dos: a) el consentimiento y b) el objeto. Si falta alguno de los elementos mencionados, el contrato no tendrá existencia, es decir, carecerá de toda validez jurídica.

El consentimiento en materia de protección de datos personales se ha concebido como la premisa básica para contar con un tratamiento legítimo de los mismos. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), en su artículo 3, lo define como: "Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos".

A su vez, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP),[442] en su artículo 12, establece las características del consentimiento en materia de protección de datos:

> Artículo 12. La obtención del consentimiento tácito o expreso deberá ser:
>
> I. Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;
>
> II. Específica: referida a una o varias finalidades determinadas que justifiquen el tratamiento, y
>
> III. Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.
>
> El consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,[443] en su artículo 3, lo define como: "Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos".

Ahora bien, habiendo definido que el consentimiento debe entenderse como la voluntad de una persona para aceptar o rechazar su vinculación jurídica con algún acto jurídico, incluido el tratamiento a sus datos personales, adquiere relevancia la forma en que éste puede otorgarse, para ello, el artículo 1803 del CCF[444] y el artículo 8 de la LFPDPPP,[445] señalan que el consentimiento puede ser expreso o tácito.

El consentimiento expreso es aquella declaración que se realiza por medios que están naturalmente destinados a exteriorizarse como la voz, la escritura e incluso algún movimiento físico. El consentimiento tácito[446] omite alguna manifestación o expresión destina-

441 Código Civil Federal, última reforma DOF 09/03/2018. Véase: http://www.diputados.gob.mx/LeyesBiblio /pdf/2_090318.pdf

442 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. 21 de diciembre de 2011. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

443 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Diario Oficial de la Federación*. 26 de enero de 2017. Disponible en: http: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

444 Código Civil Federal, última reforma *Diario Oficial de la Federación*. 9 de marzo de 2018. Disponible en: http://www.diputados.gob.mx/LeyesBiblio /pdf/2_090318.pdf

445 Ley Federal de Protección de Datos Personales en Posesión de Particulares. *Diario Oficial de la Federación*. 5 de julio de 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

446 Para el concepto de consentimiento tácito como apoyo puede tomarse en cuenta el siguiente criterio publicado en la *Revista del Tribunal Electoral del Poder Judicial de la Federación*. Sup. 2, año 1998, p. 15: "CONSENTIMIENTO TÁCITO. NO SE DA SI SE INTERPONE UNO DE VARIOS MEDIOS DE IMPUGNACIÓN ALTERNATIVOS PARA COMBATIR EL ACTO.

da a exteriorizarse o mostrarse, siendo el silencio o inactividad sus ejemplos más claros, sin embargo, revela la voluntad de la persona.

El artículo 1803[447] antes referido y el artículo 8 de la LFPDPPP[448] establecen que cuando se hable de consentimiento expreso podrá realizarse por medios tecnológicos en general, sin establecer el uso de alguna tecnología en particular, aplicando correctamente el principio de neutralidad tecnológica.

Así mismo, tanto el artículo 1834 del CCF como el artículo 93 del Código de Comercio bis señalan que cuando deba celebrarse algún contrato por escrito, donde sea necesario incluir la expresión del consentimiento, este requisito se cumplirá, mediante la utilización de medios tecnológicos, siempre que la información sea íntegra, atribuible a las personas obligadas y accesible para su ulterior consulta.

Todo lo anterior fue incluido para adecuar la normativa mexicana a las formas modernas de expresar la voluntad y el avance de la tecnología, lo que inicialmente fue previsto en Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional de 1996, donde se estableció que:

a) la oferta y aceptación de un contrato puede ser a través de mensajes de datos[449] y que no deberá negarse validez o fuerza probatoria a un contrato por haberse utilizado los medios electrónicos para su formación. (Artículo 11).
b) no puede negarse efectos jurídicos o validez legal a una manifestación de voluntad o cualquier declaración por haberse realizado a través de medios electrónicos ópticos o cualquier tecnología. (Artículo 12).

La facultad de las personas de presentar como prueba ante las autoridades y juzgadores cualquier acto —incluido el consentimiento electrónico— está contenida en el artículo 210 A del Código Federal de Procedimientos Civiles (CFPC). Esta facultad y los puntos antes mencionados son suficientes para considerar que la manifestación de la voluntad realizada por medios electrónicos o mensajes de datos debe ser considerada una forma clara y determinante para expresar la voluntad de las personas, quienes quedarán vinculados jurídicamente a ella.[450]

El consentimiento tácito se forma con una presunción en la que se emplean los siguientes elementos: a) la existencia de un acto pernicioso para una persona; b) la fijación de un medio de impugnación para combatir ese acto, dentro de un plazo determinado, y c) la inactividad de la parte perjudicada durante el citado plazo. Esto en razón de que, cuando una persona está en posibilidad de combatir un acto que la perjudica, pero únicamente dentro de un plazo determinado, y no obstante se abstiene de hacerlo, resulta lógicamente admisible inferir que se conformó con el acto. Sin embargo, cuando el afectado dispone de dos o más medios para impugnar, indistintamente, un acto o resolución, el hecho de que no ocurra a uno de ellos no es elemento suficiente para formar la inferencia indicada, especialmente si expresa de manera clara y contundente su voluntad de combatirlo mediante la utilización del medio legal distinto, previsto para el mismo efecto".

447 Código Civil Federal, última reforma *Diario Oficial de la Federación.* 9 de marzo de 2018. Disponible en: http://www.diputados.gob.mx/LeyesBiblio /pdf/2_090318.pdf
"Artículo 1803. El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
I. Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y […]".

448 Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación* 5 de julio de 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
"Artículo 8.- […]
El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos […]".

449 Por mensaje de datos se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax. Artículo 2 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno. Disponible en: https://www. uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf.

450 Se debe hacer hincapié en que tanto el Código Civil Federal, como el Código Federal de Procedimientos Civiles son supletorios en la mayoría de las materias y regulaciones, por lo que dichas reformas impactan a la posibilidad de utilizar los

Los medios electrónicos o tecnológicos utilizados para expresar el consentimiento son abiertos, es decir la legislación no limita a alguna tecnología o metodología para realizarlo, siempre que se demuestre la voluntad en un sentido afirmativo o de rechazo a una información determinada.

Lo anterior se confirma en materia de protección de datos personales en los artículos 8 y 9 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), así como en el 14 y 19 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) y el 21 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), los cuales establecen las formas de otorgar el consentimiento, tanto tácito como expreso y por escrito. En el primer caso se establece la obligación previa al tratamiento de poner el aviso de privacidad en medios electrónicos y el segundo permite utilizar firma electrónica u otro mecanismo tecnológico.[451]

Uno de los principales métodos para expresar el consentimiento en medios electrónicos es la firma electrónica.[452] Sin embargo, agregamos aquí algunos ejemplos adicionales no limitativos. En todos los casos se requerirá poder tener acceso a la evidencia de su existencia y probar la integridad, fiabilidad y atribución de los mismos:[453]

a) Correo electrónico (entre ausentes). Requiere principalmente de la escritura y sistemas informáticos de comunicación bajo responsabilidad de cada uno de los contratantes. Es posible adjuntar imágenes, sonidos, videos y otros textos escritos en varios formatos. Si bien la tecnología de correo electrónico permite la comunicación bidireccional casi de manera instantánea, no es viable obtener una respuesta inmediata por lo que no puede ser considerado un acto entre presentes.

b) *Chat* (entre ausentes y presentes). Requiere principalmente escritura y un programa de cómputo único, a través del cual se intercambian mensajes de información de forma instantánea, como si fuera una charla entre dos o más personas. Dependiendo del tipo de chat es posible considerar el acto entre presentes o ausentes.

c) Botón o ventana emergente (entre presentes). Requiere que un usuario realice una selección entre uno o varios botones de distintas opciones desplegados en el sitio web o programa de cómputo. Estos botones pueden estar visibles directamente en una página del sitio o programa de cómputo, o pueden aparecer cuando se requiera el consentimiento del usuario del sistema o sitio. Las opciones comúnmente usadas son <ACEPTAR> y <CANCELAR>, sin embargo, estas pueden variar dependiendo de lo que se requiera (consentir o rechazar). Para lograr un consentimiento electrónico sin vicios deben ser claras las condiciones, información o acto del cual se requiere el consentimiento. Esta opción, al requerirse, de forma directa e inmediata para continuar en el sitio o continuar la acción seleccionada, es posible expresar la voluntad en ese momento, por lo que puede considerarse entre presentes.

---

medios electrónicos para expresar el consentimiento, celebrar actos jurídicos y para presentar la información soportada en ellos como medio probatorio en el ámbito público y también en el privado.

451 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. 21 de diciembre de 2011. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

452 En materia de protección de datos personales este punto es confirmado por el artículo 9 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* 5 de julio de 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

453 Este tipo de ejemplos son claramente aplicables a los consentimientos tácito y expreso contenidos en los artículos 14 y 19 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. 21 de diciembre de 2011. Disponible en: http://www.diputados.gob.mx/LeyesBiblio /regley/Reg_LFPDPPP.pdf

d) *Check box* (entre presentes). Requiere que un usuario de cómputo conectado a un sitio web realice la selección de un recuadro visible para continuar alguna acción determinada dentro del sitio. En este caso, al igual que el anterior, deben ser claras las condiciones, información o acto que debe autorizarse o rechazarse. Esta opción al requerirse de forma directa e inmediata para continuar en el sitio o continuar la acción seleccionada, es posible expresar la voluntad en ese momento, por lo que puede considerarse entre presentes.

e) Videoconferencia (presentes). Requiere de un sistema de cómputo único y compartido por las personas participantes en la comunicación. La expresión utilizada es la voz y el movimiento físico al permitir la transmisión o comunicación simultánea bidireccional de audio y video. Permite, en tiempo real, que los participantes expresen sus voluntades de forma directa, por lo que debe entenderse que es un acto entre presentes.

No debe perderse de vista que el consentimiento tácito no está excluido de los medios electrónicos o tecnológicos, sin embargo, como se mencionó anteriormente, al ser la inactividad o el silencio sus elementos característicos, no cobra relevancia el medio por el cual se realicen estos, toda vez que se trata precisamente de la no exteriorización de voluntad por actos positivos.

Al hablar de consentimiento a través de mensajes de datos, deben tomarse en cuenta los artículos del 13 al 15 de la Ley Modelo de Comercio Electrónico de la Comisión de las Naciones Unidad para el Derecho Mercantil Internacional y los artículos del 90 al 92 del Código de Comercio[454] en cuanto a la atribución, momento de envío y recepción de los mismos.

Consentimiento tácito

Isabel Davara Fernández de Marcos,[455]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La normatividad vigente previene que el consentimiento para el tratamiento de los datos personales pueda manifestarse de manera tácita o de forma expresa.[456] En ambos casos se prevén elementos y características específicos para que la manifestación del consentimiento sea lícita y pueda fungir como base para la legitimación del tratamiento de los datos personales.

Como decíamos, el consentimiento para el tratamiento de los datos personales se define de forma general como "la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos".[457]

El calificativo de "tácito" se refiere a que se trata de una manifestación de la voluntad que, según el *Diccionario de la Real Academia Española*, no se entiende, percibe, oye o dice formalmente, sino que se supone e infiere. Es decir, se trata de algo que no se expresa, pero se sobrentiende.[458]

454 Código de Comercio, última reforma *Diario Oficial de la Federación*. 28 de marzo de 2018. Disponible en: http://www.diputados.gob.mx/Leyes Biblio/pdf /3_280318.pdf

455 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

456 Para una ulterior referencia se recomienda consultar las voces "consentimiento", "consentimiento expreso", "consentimiento expreso y por escrito", y "principio de consentimiento" presentes en este *Diccionario de Protección de Datos Personales.*

457 *Vid*, artículo 8, párrafo tercero de la LFPDPPP y artículo 21, segundo párrafo de la LGPDPPSO.

458 RAE. (2017). "Tácito". *Diccionario de la Lengua Española.* Disponible en: http://dle.rae.es/?id=YvLgeeV

En relación con el consentimiento tácito, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) previenen que se entiende que el titular consciente tácitamente el tratamiento de sus datos cuando, habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.[459]

En esta tesitura, lo que la normatividad señala es que para que se actualice el consentimiento tácito será pertinente que, de forma previa al tratamiento de los datos personales, el responsable haya puesto a disposición del titular el aviso de privacidad (integral, simplificado[460] o corto)[461] y que este último no haya externado su negativa al tratamiento informado. Sobre este particular, debe recordarse que el aviso de privacidad puede ponerse a disposición del titular de forma directa[462] o personal:[463]

1. Obtención del consentimiento cuando los datos se recaban directa o personalmente del titular: De forma previa al tratamiento, el responsable debe poner a disposición del titular el aviso de privacidad, mismo que deberá contener un mecanismo para que, en su caso, el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular.
2. Obtención del consentimiento cuando los datos se recaban indirectamente del titular: En los casos en que los datos personales se obtengan de manera indirecta del titular y tenga lugar un cambio de las finalidades que fueron consentidas en la transferencia, el responsable deberá poner a disposición del titular el aviso de privacidad previo al aprovechamiento de los datos personales.

De esta manera, cumplido el requisito de puesta a disposición del aviso de privacidad sin haber recibido una específica oposición del titular de los datos para el tratamiento informado, se entenderá que el titular ha exteriorizado su voluntad para que sus datos personales sean sujetos al tratamiento informado en el aviso de privacidad. Con base en lo anterior, no es requerido que quede registrado que el titular autorizó el tratamiento de su información personal, sino que es suficiente con acreditar que éste no ha manifestado su oposición.[464]

Es decir, en caso de que el titular no manifieste su negativa para el tratamiento de sus datos de conformidad con lo anterior, se entenderá que ha otorgado su consentimiento para el tratamiento informado en el aviso de privacidad del responsable, salvo prueba en contra. En consecuencia, no es necesario que, de manera expresa, el titular indique que consiente el tratamiento de su información personal, sino que es suficiente con que no diga que no.[465]

459 *Vid*, artículo 8, segundo párrafo de la LFPDPPP y artículo 21 de la LGPDPPSO.

460 En el sector público únicamente resultan aplicables las modalidades de aviso de privacidad integral y simplificado.

461 En relación con lo anterior, recomendamos consultar la definición "aviso de privacidad" presente en este *Diccionario de Protección de Datos Personales.*

462 De acuerdo con los Lineamientos del Aviso de Privacidad, poner a disposición el aviso de privacidad de forma directa es el acto en el cual se hace del conocimiento del titular el aviso de privacidad por algún medio que permite su entrega directa, entre ellos, medios electrónicos, ópticos, sonoros, visuales o cualquier otra tecnología, como correo postal, internet o vía telefónica, entre otros.

463 De acuerdo con los Lineamientos del Aviso de Privacidad, poner a disposición el aviso de privacidad de forma personal es el acto en el cual el responsable o la persona física designada por el responsable para tal fin entrega o hace del conocimiento del titular el aviso de privacidad, con la presencia física de ambos.

464 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 18. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf Fecha de consulta: 30 de noviembre de 2018.

465 En otras legislaciones como el RGDP el consentimiento tácito no es válido, pues dicho instrumento señala que, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines.

En cuanto a sus características, el consentimiento tácito (de la misma forma que el consentimiento expreso y el expreso por escrito) debe ser libre, especifico, informado e inequívoco.[466] De acuerdo con la normatividad de datos personales, dichas características del consentimiento tácito consisten en lo siguiente:

- Libre: cuando el consentimiento expreso es obtenido sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular.
- Específico: cuando el consentimiento expreso se refiere de forma concreta, explícita y lícita a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales. Es decir, como lo indica el INAI, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, es decir, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas, no en lo general.[467]
- Informado: cuando de forma previa al otorgamiento del consentimiento, se hace del conocimiento del titular de los datos personales el aviso de privacidad en virtud del cual se informa sobre el tratamiento al que serán sometidos los datos personales y las consecuencias de otorgar su consentimiento.
- Inequívoco: de acuerdo con la normatividad, este requisito se cumple cuando existen elementos que de manera indubitable demuestran que el mismo ha sido lícitamente otorgado por el titular.

En ausencia de dichas características, el consentimiento no puede considerarse como lícitamente otorgado.

Además de lo anterior, el consentimiento es revocable, de modo que el titular tiene la posibilidad de revocarlo en cualquier momento y el responsable la correlativa obligación de establecer mecanismos sencillos y gratuitos que permitan al titular ejercer dicho derecho al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.[468]

Siguiendo con la exposición anterior, se debe señalar que el consentimiento tácito generalmente es válido para cualquier tipo de dato personal con excepción de aquellos datos que revistan el carácter de datos personales patrimoniales, financieros o sensibles pues en dicho caso se deberá contactar personal o directamente al titular para requerir el consentimiento respectivo.[469]

Por otro lado, debe destacarse que, como cualquier modalidad del consentimiento, el consentimiento tácito también es susceptible de estar excepcionado bajo los supuestos previstos en los artículos 10 y 37 de la LFPDPPP, 22 y 70 de la LGPDPPSO. No obstante, el hecho de que no se requiera el consentimiento para el tratamiento, no implica que no se deban cumplir los otros principios (licitud, calidad, lealtad, finalidad, información, proporcionalidad y responsabilidad), lo que incluye la obligación de poner a disposición del titular el aviso de privacidad.[470]

466 De acuerdo con lo previsto por el artículo 12 del RLFPDPPP y el artículo 20 de la LGPDPPSO.

467 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 18. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf Fecha de consulta: 30 de noviembre de 2018.

468 Artículo 21 del RLFDPPP y artículo 20 de los Lineamientos Generales.

469 Ídem.

470 Ídem.

Finalmente, el último aspecto que conviene considerar es el de la prueba de la obtención del consentimiento, pues como regla general la obligación de demostrar su lícita obtención corresponde al responsable que realiza el tratamiento[471] por lo que deberán generarse las pruebas que se resulten pertinentes.[472] En este caso, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) detalla que las pruebas podrán ser aquellas que permitan demostrar que el responsable puso a disposición de los titulares el aviso de privacidad, por ejemplo, tener disponible el aviso de privacidad en las ventanillas donde se recaban los datos personales de los titulares o la constancia de correos electrónicos donde se envía el aviso de privacidad.

Conservación de los datos

Isabel Davara Fernández de Marcos,[473]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La conservación hace referencia a la "acción consistente en mantener o cuidar de la permanencia o integridad de algo o de alguien".[474] De acuerdo con esta acepción genérica, en el ámbito específico de la protección de datos personales, el término "conservación" implica mantener la integridad de la información personal con base en criterios legales definidos.

Así, la conservación de datos personales es el tratamiento consistente en el almacenamiento, mantenimiento y resguardo de datos personales, ya sea en soportes físicos o electrónicos, en cumplimiento a los plazos legalmente establecidos o períodos de retención determinados por el responsable.

A pesar de que ni la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) ni la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) definen de forma precisa este término, lo emplean en diversas ocasiones, en específico para hacer referencia al cumplimiento del principio de calidad[475] y el establecimiento de procedimientos idóneos para garantizar que los datos personales se conservan, se bloquean o suprimen cumpliendo con las disposiciones legalmente aplicables.[476]

Los datos, por lo tanto, se pueden tratar mientras sean necesarios para la finalidad legítima del tratamiento. Después, deben ser cancelados. Además, la cancelación también puede provenir de una solicitud del titular. La cancelación da lugar al bloqueo y, pasado el plazo de bloqueo, procede la eliminación.

471 Artículo 20 del RLFPDPPP y último párrafo del artículo 16 de los Lineamientos Generales.

472 INAI. (2015) Principio y deberes en materia de Protección de Datos Personales, p. 8. Disponible en: http://metabase.uaem.mx/bitstream/handle/123456789/2525/3%20Principios%20y%20deberes%20en%20materia%20de%20Proteccio%CC%81n%20de%20Datos%20Personales.pdf?sequence=1

473 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

474 RAE. (2017). Conservar. *Diccionario de la Real Academia de la Lengua Española.* Disponible en: http://dle.rae.es/?id=APSYcwO

475 *Vid*, definición de "principio de calidad" en este *Diccionario de Protección de Datos Personales*.

476 No obstante, tratándose del ámbito del derecho público en la Ley General de Archivos podemos encontrar una definición de conservación de archivos:
"Artículo 4. Para los efectos de esta Ley se entenderá por: [...]
XVIII. Conservación de archivos: Al conjunto de procedimientos y medidas destinados a asegurar la prevención de alteraciones físicas de los documentos en papel y la preservación de los documentos digitales a largo plazo; [...]".

Así lo disponen la LFPDPPP y la LGPDPPSO al señalar que es obligación del responsable del tratamiento observar el principio de calidad, para lo cual, éste deberá cancelar[477] los datos personales cuando éstos hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables.[478] Es así que, el responsable estará compelido a conservar los datos personales durante el período que resulte necesario para dar cumplimiento a determinadas obligaciones legales así como en atención a las disposiciones aplicables en la materia de que se trate, que pueden ser de muy diversos aspectos (administrativos, contables, fiscales, etc.).[479]

Así también, la *Guía para el Borrado Seguro de Datos Personales* publicada por el INAI indica que "con independencia de que un titular de los datos personales ejerza su derecho de cancelación, el responsable del tratamiento está obligado a eliminar, de oficio, los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual se obtuvieron".[480] Como decíamos, la cancelación es procedente de oficio, aunque el titular no hubiera ejercido alguna de las prerrogativas que la normatividad le confiere.

De acuerdo con las precisiones antes detalladas, se puede decir que los plazos de conservación deberán tener en cuenta el tiempo requerido para llevar a cabo las finalidades del tratamiento, más los plazos legales de cualquier índole (administrativos, contables, fiscales, históricos, etc.) relacionados con el tratamiento específico.

Con base en el anterior sustento normativo, el responsable (ya sea de naturaleza pública o privada) tiene en ambas normatividades dos obligaciones concretas: 1) establecer procedimientos para la conservación, bloqueo y supresión de los datos personales y 2) demostrar el cumplimiento de los plazos de conservación previamente establecidos para dar cumplimiento al principio de calidad.

Así, la normatividad de datos personales conmina al responsable a establecer (primera obligación) y documentar (segunda obligación) procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales, que incluyan los periodos de conservación de los mismos.[481]

En la práctica, dicha obligación alcanza concreción cuando el responsable desarrolla y hace cumplir una política de cancelación, bloqueo y supresión de datos personales identificando los distintos períodos de prescripción de las obligaciones legales así como los procesos internos que se deben cumplir, y genera prueba[482] de que la política de cancelación, bloqueo y supresión de datos personales se aplica en la práctica cotidiana de la organización y que el personal realiza el tratamiento lo hace en cumplimiento a la misma. Por ejemplo, para verificar lo anterior, el responsable podrá realizar revisiones o auditorías que le permitan determinar si se cumple dicha obligación en la práctica.

477 Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos señalan:
"19.2. Cuando los datos personales hubieren dejado de ser necesarios para el cumplimiento de las finalidades que motivaron su tratamiento, el responsable los suprimirá o eliminará de sus archivos, registros, bases de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización".

478 *Vid*, artículo 11 de la LFPDPPP y artículo 23 de la LGPDPPSO.

479 *Vid*, artículo 37 del Reglamento de la LFPDPPP y artículo 23 de la LGPDPPSO.

480 INAI. (2016). *Guía para el Borrado Seguro de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

481 *Vid*, artículo 38 del RLFPDPPP y artículo 24 de la LGPDPPSO.

482 *Vid*, artículos 39 del RLFPDPPP y 24 de la LGPDPPSO.

Por otro lado, dicha política deberá considerar los mecanismos habilitados por el responsable para suprimir o eliminar los datos personales una vez concluido el período de retención aplicable. Dichos procedimientos deberán determinarse en función de la naturaleza de los datos personales, el tipo de soporte en que consten los mismos, así como las obligaciones que haya que cumplir sin que sea requisito obligado optar por una tecnología en particular.

En relación con la supresión final de los datos personales, si bien la ley da al responsable la posibilidad de usar diversas tecnologías o procedimientos para su eliminación segura, en la práctica es recomendado seguir lo dispuesto por la *Guía para el Borrado Seguro de Datos Personales*[483] que establece recomendaciones para realizar la eliminación de datos personales, ya sea que estos obren en soportes físicos o electrónicos.

Como apunte final, cabe resaltar que, para dar plena observancia a las obligaciones referidas, no debe obviarse que un paso previo y fundamental es que el responsable identifique el ciclo de vida de los datos personales en cada uno de sus procesos, desde la obtención, almacenamiento, procesamiento, cancelación o cualquiera que sea su tratamiento.[484]

Control de seguridad

Christian Paredes González

La expresión "control de seguridad" se emplea en la normatividad de datos personales para hacer referencia a las medidas de seguridad aplicables al tratamiento de los datos personales.[485] Esta expresión no aparece definida normativamente, pero se entiende relacionada con las propias medidas de seguridad establecidas para garantizar la seguridad y confidencialidad de los datos personales.[486]

Un control es definido, según el *Diccionario de la Real Academia Española*, como la regulación, manual o automática, sobre un sistema. Sobre esta acepción podemos entender que se trata de un mecanismo que puede ser físico o electrónico, tendiente a asegurar la seguridad de un sistema de tratamiento de datos personales.

La *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales* publicada en 2015[487] (GISGSDP) establece que como parte de la identificación de las medidas de segu-

483 INAI. (2016). *Guía para el Borrado Seguro de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

484 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2015, junio). *Guía para la Implementación de un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf Fecha de consulta: 18 de octubre de 2018.

485 El artículo 57 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares señala lo siguiente:
"El responsable y, en su caso, el encargado deberá establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales.
Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento".

486 El artículo 42 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados dispone lo siguiente:
"El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.
Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública".

487 INAI. (2015, junio). *Guía para la Implementación de un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf Fecha de consulta: 18 de octubre de 2018.

ridad y análisis de brecha (Paso 6) establece que las medidas de seguridad podrán estar basadas en los controles de seguridad presentados en el anexo D de la GISGSDP entre los que destacan diversos controles basados en los dominios siguientes:

- Políticas del Sistema de Gestión de Seguridad de Datos Personales (SGSDP)
- Cumplimiento legal
- Estructura organizacional de la seguridad
- Clasificación y acceso a los activos
- Seguridad del personal
- Seguridad física y ambiental
- Gestión de comunicaciones y operaciones
- Control de acceso
- Desarrollo y mantenimiento de sistemas
- Vulneraciones del sistema

La GISGSDP señala que los controles se pueden usar como referencia en la elaboración del plan de tratamiento del riesgo, en la valoración del riesgo o incluso para establecer el contexto de seguridad de la organización en función de la presencia o ausencia de los controles referidos.

Las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales[488] señalan que se pueden considerar los siguientes como controles que deben establecerse para la gestión de incidentes:

- Políticas: que respalden la creación y el funcionamiento del equipo de respuesta a incidentes.
- Elaboración del plan o estrategia: dependiendo de los mecanismos para detectar alertas de seguridad, se debe establecer una cadena de atención, revisión y aprobación de la mitigación de posibles incidentes de seguridad.
- Comunicación: durante cualquier etapa de la atención de un incidente se debe mantener comunicación entre los miembros del equipo de respuesta y otras partes interesadas como la alta gerencia o autoridades.
- Documentación: se deberá establecer un proceso y los formatos necesarios para documentar cada descubrimiento o acción realizada en atención a un incidente de seguridad.
- Control de acceso: el equipo de respuesta a incidentes debe de contar con las credenciales necesarias para tener acceso a cualquier activo involucrado en un incidente de seguridad.
- Herramientas: es altamente recomendable tener hardware y software destinados a atender una alerta de seguridad, y comenzar la mitigación en caso de confirmar un incidente.

En definitiva, podemos mencionar que la expresión "controles de seguridad" se refiere a una serie de controles físicos, técnicos y/o administrativas para asegurar la seguridad y confidencialidad de la información.

488 INAI. (2018). *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

Convenio 108 del Consejo de Europa

Alejandro Alday González

El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (en adelante Convenio 108 del consejo de Europa) para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108)[489] es un tratado internacional en materia de protección de datos personales adoptado en Estrasburgo, Francia el 28 de enero de 1981 y que entró en vigor el 1 de octubre de 1985. El acuerdo ha sido firmado y ratificado por los 47 países del Consejo de Europa[490] (CoE), así como por varios Estados no miembros (al 28 de septiembre de 2018, estos países son: Cabo Verde, Mauricio, México, Senegal, Túnez y Uruguay). El Convenio 108 cuenta con un protocolo adicional relativo a las autoridades de control y a los flujos trasfronterizos de datos personales (Protocolo Adicional),[491] que fue adoptado el 8 de noviembre de 2011 y entró en vigor el 1 de julio de 2004.

El Convenio 108 es uno de los tratados de mayor relevancia a nivel internacional en materia de protección de datos. Este instrumento tiene como objeto principal crear un marco legal en esta materia. Ha logrado influir en el diseño de políticas y en la legislación más allá de las fronteras de Europa y busca lograr un equilibrio proporcional entre la protección de datos personales y la libre transferencia de datos personales entre los países, de tal manera que los Estados no sufran limitaciones ni tengan obstáculos que frenen el comercio internacional.

1. Antecedentes

El Convenio 108 fue creado y adoptado por el CoE hace más de tres décadas. Está abierto a países no miembros del CoE y a organizaciones internacionales. Es considerado el primer instrumento internacional jurídicamente perentorio en el área de la protección de datos, ya que constriñe a los países que lo suscriben a tomar las medidas necesarias en el ámbito interno para adecuar su legislación a los principios establecidos en su texto.

El 28 de enero de 1981 el Consejo de Europa adoptó el Convenio 108 con el objeto de garantizar el derecho a la protección de datos personales en cada Estado parte.[492] El Convenio 108 es el único instrumento jurídicamente vinculante de vocación universal que salvaguarda el derecho fundamental de protección de datos personales, mismo que se encuentra consagrado en los artículos 6 y 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).

En cuanto a sus antecedentes nacionales, las consideraciones generales de la exposición de motivos de la discusión para la aprobación del Convenio 108 en México, se señala el contexto de los años setenta con importantes avances en las tecnologías de la comunicación y el argumento bajo el que se desarrolló el instrumento normativo:

> […] la protección de los datos personales desempeña un papel fundamental en el ejercicio del derecho humano al respeto de la vida privada y familiar y, por lo tanto, constituye también una

489 El texto del convenio se puede consultar en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

490 Es importante distinguir al Consejo como organismo internacional regional de la Unión Europea, que es una entidad geopolítica de derecho para promover la integridad de los estados de Europa.

491 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181

492 "Artículo 1. Objeto y fin
El fin del presente Convenio es garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»)".

condición *sine qua non* para el ejercicio de otros derechos fundamentales, tales como la libertad de expresión y la libertad de conciencia.

Considerando lo anterior, el comité de expertos realizó un análisis de las legislaciones nacionales de los Estados del CoE para determinar si éstas otorgaban las garantías necesarias para proteger el derecho a la privacidad establecido en el artículo 8 del Convenio Europeo de Derechos Humanos. El estudio encontró que las protecciones eran insuficientes y deficientes, y en razón de lo anterior, el Comité de Ministros aprobó una serie de recomendaciones. Sin embargo, el carácter no vinculante de las recomendaciones motivó al CoE a plantearse la necesidad de elaborar normas vinculantes que obligaran a los estados parte a fortalecer su legislación, con el propósito de proteger de manera eficaz e integral los datos personales de sus ciudadanos, así como de aquellos nacionales de otro Estado signatario, y, eventualmente, ampliar su ámbito de aplicación más allá de las fronteras del continente europeo. Fue así que el Convenio 108 se planteó como un instrumento de vocación universal cuyo contenido no se limitara al ámbito del CoE, sino que existiera la posibilidad de que lo suscribieran países que no fueran miembros de este organismo regional.

El dictamen emitido el 18 de abril de 2018 por las comisiones unidas de relaciones exteriores y de anticorrupción y participación ciudadana del Senado de la República relata que el 25 de agosto de 2017 México presentó al CoE la solicitud para recibir la invitación formal para adherirse al Convenio 108. El 16 de octubre, el comité consultivo aprobó por unanimidad una opinión favorable sobre la adhesión de México al instrumento internacional, concluyendo que la legislación mexicana de protección de datos personales cumplía de manera general con los principios del Convenio 108 y de su Protocolo Adicional. Asimismo, el 30 de noviembre, el Grupo de Relatores sobre Cuestiones Jurídicas (GRJ) del CoE aprobó por unanimidad la solicitud de México para adherirse al Convenio 108 y a su Protocolo Adicional. Por consiguiente, el 13 de diciembre, el Comité de Ministros del Consejo de Europa, tras analizar las opiniones del Comité Consultivo del Grupo de Relaciones Jurídicas, decidió, por unanimidad, extender la invitación formal a México para adherirse al Convenio 108 y a su Protocolo Adicional.

En sesión del 26 de abril de 2018, el Senado de la República, conforme a su facultad constitucional para aprobar los tratados internacionales que el Ejecutivo Federal suscriba, establecida en el artículo 76 fracción I de la CPEUM, aprobó la adhesión de México al Convenio 108 y a su Protocolo.[493]

El 12 de junio de 2018 se publicó en el *Diario Oficial de la Federación* (DOF) el Decreto por el que se aprueba el Convenio 108 y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente.[494] y [495]

493 En este sentido la ley sobre celebración de tratados señala lo siguiente:
"Artículo 4o. Los tratados que se sometan al Senado para los efectos de la fracción I del artículo 76 de la Constitución, se turnarán a comisión en los términos de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos para la formulación del dictamen que corresponda. En su oportunidad, la resolución del Senado se comunicará al presidente de la República".

494 SEGOB. (2018, diciembre 6). "DECRETO por el que se aprueba el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hechos en Estrasburgo, Francia, el 28 de enero de 1981, y el 8 de noviembre de 2001, respectivamente". *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5526265&fecha=12/06/2018 Fecha de consulta: 30 de agosto de 2018.

495 Lo anterior en cumplimiento a lo dispuesto por el segundo párrafo del artículo 4 de la Ley sobre Celebración de Tratados que señala lo siguiente:
"[...] Los tratados, para ser obligatorios en el territorio nacional deberán haber sido publicados previamente en el *Diario Oficial de la Federación*".

2. Características esenciales del Convenio y su protocolo adicional

El Convenio 108, de acuerdo con su artículo primero, tiene por objeto garantizar, en el territorio de cada "Estado parte", a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos).

En cuanto al ámbito de aplicación de este instrumento internacional, es muy importante señalar que éste no solo resultaría aplicable al sector privado como hoy se aplica la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en lo que toca al tratamiento de información personal, sino que extiende su ámbito de aplicación a la esquela pública, tal y como lo señala su artículo 3 que refiere: "Las partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado", donde en México en la actualidad a nivel federal contamos con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

El dictamen relativo a la suscripción del Convenio 108 y su Protocolo Adicional por parte del Estado mexicano señala, además, las siguientes características:

- El Convenio 108 y su Protocolo Adicional sientan un precedente importante, pues se trata de los primeros instrumentos internacionales en materia de protección de datos personales a los que se vincula formalmente el Estado mexicano.
- El Convenio y su Protocolo Adicional, suponen una serie de beneficios para el Estado mexicano en términos políticos y económicos; sin embargo, se destaca que los principales beneficiados son los individuos, toda vez que los instrumentos regulan un derecho humano fundamental.
- La adhesión de México a estos instrumentos internacionales lo sitúa en un plano de igualdad con los demás Estados parte. Por lo tanto, significaría que su normatividad interna se apega a los máximos estándares internacionales, así como a las buenas prácticas en la materia.
- Las empresas mexicanas resultarán beneficiadas por las facilidades para transferir y recibir datos de los estados parte del convenio, más aquellos que se adhieran posteriormente.
- Los connacionales mexicanos que residen en cualquiera de los Estados parte del Convenio podrán ejercer con dichos Estados su derecho de protección de datos personales y, por ende, acudir ante cualquier autoridad responsable de asegurar el cumplimiento del contenido del Convenio cuando sus datos personales sean vulnerados.
- El régimen que establece el Convenio prevé que cada Estado parte debe disponer que una o más autoridades independientes[496] que sean responsables de garantizar el cumplimiento de las medidas previstas por su derecho interno que hacen efectivos los principios del Convenio, así como en el Protocolo Adicional. Asimismo, que los organismos estatales cuenten con las competencias necesarias para el ejercicio de sus funciones, particularmente para atender las reclamaciones formuladas por cualquier persona en relación con la protección de sus derechos y libertades fundamentales respecto de los tratamientos de datos de carácter personal.[497]

496 Según el protocolo adicional al Convenio 108, los Estados partes en el Convenio deberían establecer una o varias autoridades independientes con el objetivo de asegurar el respeto de los principios enunciados en el Convenio. Estas autoridades de control tienen el poder de investigar e intervenir, de interponer una acción judicial o de poner en conocimiento de las autoridades judiciales las violaciones de la legislación sobre la protección de datos.

497 En el caso específico del Estado mexicano, y de conformidad con el artículo 6, apartado A, fracción VIII, de la Constitución Política, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales es el

También, en el dictamen se mencionan aspectos relevantes del Protocolo Adicional que amplió el espectro de la protección en materia de protección de datos personales que tenía el Convenio. Lo anterior, al señalar que éste adicionó artículos con las siguientes distinciones:

> En cuanto a su estructura, el Protocolo Adicional se divide en 3 artículos.
>
> El primero de ellos establece que cada Parte preverá una o más autoridades que sean responsables de asegurar el cumplimiento de los principios de protección de datos personales previstos en el Convenio 108, así como de las medidas adoptadas para asegurar la realización de flujos transfronterizos de datos personales para lo cual deberán contar con las siguientes características:
>
> - Tener facultades de investigación e intervención y competencias para en su caso iniciar procedimientos judiciales respecto a violaciones de las normas de derecho interno que tutelan este derecho:
> - Tener facultades para atender las reclamaciones formuladas por cualquier persona.
> - Deberán ejercer sus funciones con total independencia.
> - Las decisiones de la autoridad de control puedan ser recurridas Judicialmente.
>
> El segundo artículo del Protocolo prevé que las transferencias de datos personales a un destinatario no sometido a la competencia de un Estado u organización que no es parte del Convenio, se podrán llevar a cabo dicho Estado u organización asegura un adecuado nivel de protección […].[498]

3. Contenido del Convenio 108

En primer lugar, conviene precisar su objeto y fin, mismos que se prevén en su artículo 1:

> El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física, sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).

Asimismo, el Convenio incluye los principios básicos para la protección de datos. Las partes se comprometen, de acuerdo con el artículo 4, a tomar las medidas necesarias en su derecho interno para hacerlos efectivos. Estos principios son:

Calidad de los datos (artículo 5). Los datos personales objeto de un tratamiento automatizado:

a) se obtendrán y tratarán leal y legítimamente;
b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;
c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;
d) serán exactos y si fuera necesario puestos al día;

---

organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la normatividad correspondiente. A efecto de cumplir con la naturaleza jurídica para la que fue creado, el Instituto antes referido cuenta, entre otras, con las siguientes atribuciones: normativas, informativas, de verificación, resolutorias y sancionadoras.

498 Comisiones unidas de relaciones exteriores, Europa; de relaciones exteriores; y de anticorrupción y participación ciudadana (2018, 18 de abril).DICTAMEN DE LAS COMISIONES UNIDAS DE RELACIONES EXTERIORES, EUROPA; DE RELACIONES EXTERIORES; Y DE ANTICORRUPCIÓN Y PARTICIPACIÓN CIUDADANA, CON PROYECTO DE DECRETO POR EL QUE SE APRUEBA LA ADHESIÓN DE MÉXICO AL CONVENIO DEL CONSEJO DE EUROPA PARA LA PROTECCIÓN DE LAS PERSONAS CON RESPECTO AL TRATAMIENTO AUTOMATIZADO DE DATOS DE CARÁCTER PERSONAL Y A SU PROTOCOLO ADICIONAL RELATIVO A LAS AUTORIDADES DE CONTROL Y A LOS FLUJOS TRANSFRONTERIZOS DE DATOS PERSONALES. p. 6. Disponible en: http://infosen.senado.gob.mx/sgsp/gaceta/63/3/2018-04-26-1/assets/documentos/Dic_REE_Consejo_Europa_proteccion_datos.pdf

e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Categorías particulares de los datos (artículo 6). No pueden tratarse de forma automática los "datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual" así como los datos referentes a condenas penales, a menos que el derecho prevea garantías adecuadas.

Seguridad de los datos (artículo 7). "Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

Garantías complementarias para la persona concernida (artículo 8). Que establece los derechos de las personas a:

a) conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.

Protección más amplia (artículo 11). Este principio de interpretación, establece que las disposiciones no deben interpretarse en el sentido que "limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio".

Asimismo, debe considerarse que el Convenio limita las excepciones y restricciones que el Estado puede oponer a los derechos y el ejercicio de los mismos establecidos en el Convenio 108 (artículo 10). Además, el Convenio prevé que las partes deben establecer sanciones o recursos jurisdiccionales al incumplimiento de las disposiciones que hagan efectivos los principios (artículo 11).

El Convenio 108 del CoE busca que los Estados no sufran limitaciones u obstáculos que detengan el comercio internacional. En este sentido, el artículo 12 establece que las Partes no pueden prohibir los flujos trasfronterizos de datos personales con el objeto de un tratamiento automatizado "con el fin de proteger la vida privada". Sin embargo, permite que se establezcan excepciones:

> a) en la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra Parte establezca una protección equivalente;

b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo.

Finalmente, cabe agregar que el Convenio regula la ayuda mutua que puede existir entre las partes del acuerdo, y establece un comité consultivo que tiene la facultad, entre otras, de presentar propuestas para facilitar o mejorar la aplicación del Convenio.

4. Labor del INAI: autoridad independiente

Según el Protocolo Adicional al Convenio 108, los Estados parte del Convenio deberán establecer una o varias autoridades independientes con el objetivo de asegurar el respeto de los principios enunciados en el Convenio. Estas autoridades de control tienen el poder de investigar e intervenir, de interponer una acción judicial o de poner en conocimiento de las autoridades judiciales las violaciones de la legislación sobre la protección de datos.

En México, el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales (INAI) cuenta atribuciones normativas, informativas, de verificación, resolutorias y sancionadoras para garantizar el cumplimiento de los derechos de acceso a la información pública y la protección de datos personales en términos de lo dispuesto por la normatividad aplicable.

El Convenio 108 del CoE y su Protocolo Adicional forman parte de los tratados internacionales en materia de derechos humanos de los que el Estado mexicano es parte. Con estos instrumentos se robustece el respeto a los derechos y libertades fundamentales, así como a la vida privada de cualquier persona física, sin importar su nacionalidad o residencia.

Cookies

Andrés Velázquez Olavarrieta

La legislación mexicana retoma la definición técnica de las *cookies*. Las considera un archivo de datos que se almacena en el disco duro del equipo de cómputo o del dispositivo de comunicaciones electrónicas de un usuario al navegar en un sitio de internet específico, el cual permite intercambiar información de estado entre dicho sitio y el navegador del usuario. La información de estado puede revelar medios de identificación de sesión, autenticación o preferencias del usuario, así como cualquier dato almacenado por el navegador respecto al sitio de internet.

Existen varios tipos de *cookies*.[499] Se clasifican por categorías y una *cookie* puede pertenecer a más de una categoría. Por tiempo de vida hay *session cookies* y *persistent cookies*. Las primeras tienen un corto tiempo de vida ya que son borradas cuando de cierra el navegador. Las segundas se usan para rastrear al usuario guardando información sobre su comportamiento en un sitio *web* durante un período de tiempo determinado; pueden ser borradas limpiando los datos del navegador, aunque algunas tienen una fecha de expiración, que puede ir desde unos minutos a varios años.

499 La clasificación técnica de las *cookies* ha sido retomada por diversos organismos como la Agencia Española de Protección de Datos que ha establecido una guía sobre las normas de uso de cookies (http://www.residencia.csic.es/informacion/pdf/privacidad_cookies.pdf) para "impedir el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario". En México, las páginas de internet mexicanas deben informar si en su sitio se recaban datos personales de manera automática a través de *cookies,* de acuerdo con los Lineamientos del Aviso de Privacidad. El artículo 31 de esas disposiciones establece que se debe advertir que a través de esa tecnología "se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos".

También se clasifican según la entidad que las gestiona. Las *cookies* a terceros son aquellas que instala un sitio *web* que el usuario no está visitando. Por ejemplo, un sitio web que tenga un botón de me gusta de Facebook puede que instale una *cookie* que Facebook puede leer, por tanto, estás visitando una página que no tiene nada que ver con Facebook pero el navegador guarda una *cookie* de éstos. Contrarias a éstas están las *cookies* propias que se almacenan en el equipo del usuario, pero provienen únicamente de la *web* que se está visitando.

Por su finalidad, las *cookies* se clasifican en técnicas porque permiten controlar el tráfico y las comunicaciones de datos, de análisis ya que permiten al responsable de ellas hacer un análisis y seguimiento de comportamiento del usuario que hacen uso de sitios *web* que las contienen, permitiendo generar un perfil de usuario.

También hay *cookies* publicitarias, su objetivo es recoger datos de actuación sobre espacios publicitarios. Se usan para optimizar campañas y conocer la frecuencia en la que se muestra un anuncio. Las *cookies* de personalización dejan a los usuarios acceder según algunas características propias que se recogen (idioma, navegador, configuración regional, etc.).

NOTAS

NOTAS

NOTAS

Daño moral

Luis Manuel C. Meján

El concepto de daño involucra un deterioro de algo, una pérdida total o parcial de un valor.[500] Un principio elemental de justicia es que cuando alguien ha sufrido un daño, le asiste el derecho de reclamar la reparación del mismo a quien se lo ha causado. Mientras se trate de un daño patrimonial, el tratamiento es relativamente sencillo pues basta cuantificar el valor de lo deteriorado, ya sea parcial o total, y montar la obligación de cubrirlo a quien lo ha causado.

El daño moral es distinto, porque se trata de una agresión a cuestiones de muy difícil definición y valoración como los sentimientos, la dignidad, la honra, la reputación, el prestigio, etc. Normalmente, el daño moral se presenta en dos posibles vertientes. La primera es en el terreno de lo social, donde la apreciación que los demás tienen de una persona se ve lastimada. El daño se desplaza en círculos concéntricos, primero en el círculo de la familia y las personas más allegadas, después el del medio laboral, la comunidad en la que se vive y así sucesivamente, por ejemplo, cuando se ha difundido una noticia (real o falsa) que deteriora la imagen de alguien. La segunda vertiente del daño moral es en la parte afectiva y personal, por ejemplo, cuando se sufre la pérdida o el deterioro de un objeto con valor sentimental.

El concepto "daño moral" proviene del derecho antiguo. En las leyes de Esshnunna, de la cultura caldeo asiria o mesopotámica, se asienta que: "Quien propine a otro una bofetada en la cara pesará y entregará 10 shekels de plata". Justiniano dispuso acciones para el ofendido en su honor, decoro, consideración pública y reputación y en la doctrina moderna se le ha incluido entre los derechos de la personalidad.

La definición que da el Código Civil Federal (CCF), (artículo 1916) es: "Afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físico, o bien en la consideración que de sí misma tengan los demás".

Como no es posible establecer un valor patrimonial a dichos sentimientos, el derecho avizora tres posibles tratamientos. El primero es no crear una relación jurídica obligatoria y dejarle la sanción al derecho público (penal o administrativo), el segundo implica asignar una

500 Real Academia Española: Causar detrimento, perjuicio, menoscabo, dolor o molestia

reparación basada en un determinado porcentaje del valor del daño (si es que existe un daño material asociado al hecho que produce el daño moral) y el tercero, consiste en establecer un sistema de valuación (aunque sea difícil) pues es mejor compensar patrimonialmente el daño moral causado que no compensarlo de ninguna manera.

El derecho mexicano se ha pronunciado entre los dos últimos tratamientos e irroga al juez la difícil tarea de definir el valor de la reparación del daño.

Los elementos que deben ser tomados en cuenta para valuar y obligar a un responsable a restañar un daño moral son las condiciones socioeconómicas del causante y de la víctima, la culpa o dolo desplegado, la gravedad del daño causado (algunos son mayores que otros, por ejemplo, a una persona común le hace daño que se difunda que suele incumplir sus obligaciones, pero a una figura pública: un artista un comerciante, un político, le hace un daño más grave) y, en general, todas las circunstancias que rodean a los hechos (lugares, fechas, antecedentes, complicaciones, etcétera). Desde luego que una medida posible de reparación del daño moral está en la publicación y difusión de la verdad y la retracción de las afirmaciones que han causado el desprestigio hechas de una manera similar o superior (mismo medio, mismo espacio, misma circulación) a como se hicieron los actos que dañaron moralmente a la víctima.[501]

La acción para exigir la reparación del daño se atribuye a quien lo ha sufrido y le corresponde la carga de la prueba (tanto del suceso como del daño), lo cual puede ser, en ocasiones, muy difícil. Por sus características —pues el daño es íntimo y personal— se trata de una acción personalísima que no puede ser transmitida a otros. El CCF establece que solo se transmite a los herederos, si la acción ha sido iniciada y ejercida en vida del *de cujus*.[502]

El daño moral debe provenir de un acto ilícito. El principio general de la responsabilidad civil, contractual o extracontractual, es aquel que se enuncia: "El que actuando en contra de la ley o de las buenas costumbres, causa un daño a otro, está obligado a repararlo", eso comprende los casos de responsabilidad objetiva y de actos de terceros. Esto quiere decir que el que actúa sin ilicitud y conforme a derecho no puede ser responsable de un daño moral (salvo los casos específicos contemplados en la ley como es el caso del abuso de un derecho).

La ley ayuda con presunciones: comunicar un hecho cierto o falso que cause deshonra o desprecio; imputar un delito a un inocente, en forma directa o presentando denuncias y, en general ofender el honor, la vida privada o la imagen de alguien (artículo 1916 del CCF).

Un tema alrededor del daño moral se desarrolla al contactarse con el derecho a la información que ejercen periodistas y comunicadores, quienes tienen que mantener el difícil equilibrio entre hacer sus comunicaciones objetivas y no causar un daño moral. A este propósito se han desarrollado legislaciones específicas.

501 La Primera Sala de la Suprema Corte de Justicia de la Nación ha emitido tres tesis aisladas respecto de los parámetros de cuantificación del daño moral: Tesis 1a. CCLV/2014 (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época 2006880. Primera Sala. Libro 8. Julio de 2014. Tomo I, p. 158. Tesis Aislada (Civil); Tesis 1a. CCLIV/2014 (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época, 2006881. Primera Sala. Libro 8. Julio de 2014. Tomo I, p. 159. Tesis Aislada. (Civil) y Tesis 1a. CCLXXV/2014 (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época, 2006968. Primera Sala. Libro 8. Julio de 2014. Tomo I, p. 160. Tesis Aislada (Civil).

502 Enciclopedia jurídica. "De cujus". (Derecho Civil). Primeras palabras de la fórmula latina de *cujus succesione agitur* (aquel de cuya sucesión se trata); utilizada en nuestros días para designar al difunto causante de la sucesión: se dice el *de cujus*. Palabra que designa a la persona cuya sucesión ha sido abierta. El último domicilio del *de cujus* fija la competencia territorial (o circunscripción) y, en consecuencia, determina al juez competente para abrir el sucesorio. Abreviatura de la expresión latina de *cujus successione agnur*, aquel de cuya sucesión se trata. Equivale a causante, al difunto de cuya herencia se trate. Disponible en: http://www.enciclopedia-juridica.biz14.com/d/de-cujus/de-cujus.htm

En el manejo de los datos personales se puede generar un daño de esta naturaleza. Cuando un responsable hace un uso indebido de los datos personales, especialmente en el caso de datos sensibles, estos pueden caer en manos o en conocimiento de quien no debía ser un destinatario y ese solo hecho puede causar el daño moral al titular de los datos. Estos son casos en los que el responsable se puede ver sujeto a una sanción o a la imposición de una pena por haber incurrido en delito. Estas sanciones no excusan de enfrentar la responsabilidad civil de restañar el daño moral.[503]

Dato personal

Isabel Davara Fernández de Marcos,[504]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El concepto "dato personal" es el punto de partida de las normatividades en México en la materia de protección de datos personales. Tanto la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[505] como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[506] definen el concepto de dato personal como "cualquier información concerniente a una persona física identificada o identificable".

Podemos dividir el estudio de dicha definición en cuatro apartados:

A) cualquier información
B) concerniente
C) persona física
D) identificada o identificable

Los componentes antes mencionados son reiterativos en los principales cuerpos normativos internacionales en la materia. A manera de ejemplo, citamos las definiciones que prevén algunas de las principales normatividades internacionales al respecto:

- El Convenio 108 del Consejo de Europa (Convenio 108) del 28 de enero de 1981 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, del que México es parte, define el concepto de "dato personal" como cualquier información relativa a una persona física identificada o identificable (persona concernida).[507]

503 Ley Federal de Protección de Datos en Posesión de los Particulares (LFDPPP). Artículo 66. "Las sanciones que se señalan en este capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte. En el mismo sentido se pronuncian". Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). Artículo 165. "Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 163 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos".
Reglamento General de Protección de Datos de la Unión Europea (RGDP). Artículo 82, inciso 1. "Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos".
Estándares de Protección de Datos por los Estados Iberoamericanos: "44. Reparación del daño 44.1. La legislación nacional de los Estados Iberoamericanos aplicable en la materia reconocerá el derecho que tiene el titular a ser indemnizado cuando hubiere sufrido daños y perjuicios, como consecuencia de una violación de su derecho a la protección de datos personales".

504 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

505 Artículo 3, fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

506 Artículo 3, fracción V. de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

507 Artículo 2, inciso a) del Convenio 108.

- La Recomendación nº R (97) 5 del 13 de febrero de 1997 del comité de ministros del Consejo de Europa a los Estados miembros sobre protección de datos médicos, define el concepto "dato personal" como cualquier información relativa a un individuo identificado o identificable.[508]
- El inciso c) del artículo 2.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos indica que el dato personal es "cualquier información concerniente a una persona física identificada o identificable, expresada en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de cualquier otro tipo". El Reglamento General Europeo de Protección de Datos (RGPD o GDPR por sus siglas en inglés) en el apartado 1 de su artículo 4 previene que el dato personal[509] es toda información sobre una persona física identificada o identificable (el interesado).[510]

Las definiciones presentadas en el ámbito nacional e internacional son bastante similares y comparten, en esencia, los cuatro bloques de información que conforman el concepto "dato personal".

Estos cuatro componentes anteriores están estrechamente ligados y se complementan recíprocamente. Para efectos de la adecuada comprensión del concepto "dato personal" cada uno de ellos se analizará por separado en el siguiente apartado.

1. Elementos de la definición

A. Cualquier información

La expresión "cualquier información" empleada en la LFPDPPP y en la LGPDPPSO manifiesta la voluntad del legislador de dar un sentido amplio al concepto "dato personal". Con base en lo anterior, dicha redacción exige una interpretación amplia y podrá involucrar distintos elementos objetivos y subjetivos a partir de los cuales se puede lograr la identificación de la persona.

Existen aspectos del término "información" que facilitan identificar aquella información que será considerada como "dato personal". Estos aspectos son: (i) la naturaleza de la información, (ii) su contenido y (iii) su formato.

1. A. Naturaleza de la información

La información personal, según declara el Grupo de Trabajo del Artículo 29[511] (GTA29 o WP29 por sus siglas en inglés)[512] puede abarcar tanto información objetiva como las credenciales académicas de un trabajador, como también informaciones, opiniones o eva-

508 "1. Definiciones
A los fines de esta recomendación:
- la expresión "datos personales" abarca cualquier información relativa a un individuo identificado o identificable. Un individuo no se considerará "identificable" si la identificación requiere una cantidad de tiempo y de medios no razonables. En los casos en que el individuo no sea identificable, los datos son denominados anónimos […]".

509 Artículo 4, apartado 1 del Reglamento General de Protección de Datos Personales.

510 Previamente, la directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos definió a los datos personales en su artículo 2, inciso A, como "toda información sobre una persona física identificada o identificable (el interesado); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

511 Este Grupo se creó en virtud del artículo 29 de la directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la directiva 95/46/CE y en el artículo 15 de la directiva 2002/58/CE.

512 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

luaciones subjetivas, como la evaluación de un empleador a su trabajador,[513] sin que esto prejuzgue la certeza de la misma, es decir, la información no tiene que ser verdadera para ser considerada dato personal.

1. B. Contenido de la información

El concepto "datos personales" abarca información sobre las personas con independencia de su posición o capacidad (como consumidor, paciente, trabajador por cuenta ajena, cliente, etc.).[514] Esto es, comprende información relativa a la vida privada y familiar del individuo, así como también la información sobre cualquier tipo de actividad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social.

1. C. Formato de la información

Desde el punto de vista del formato, los datos personales incluyen información expresada en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.[515] Finalmente, en lo que respecta al soporte, el concepto de datos personales incluye toda aquella información que conste en soportes físicos[516] y/o electrónicos.[517]

B. Concerniente

De forma general, se puede considerar que la información concierne a una persona cuando se refiere a ella, esto es, cuando se le vincula. La normatividad protege al sujeto —persona física— a la que se vinculan dichos datos personales y, por tanto, se protege el tratamiento de los mismos en cuanto le conciernen a una persona física identificada o identificable.

Al respecto, el GTA29 ha señalado lo siguiente: "Dato se refiere a una persona si hace referencia a su identidad, sus características o su comportamiento o si esa información se utiliza para determinar o influir en la manera en que se la trata o se la evalúa".[518]

513 Según el GTA29, esta última clase de afirmaciones constituye una parte considerable del caudal de datos personales tratados en sectores como el de la banca para evaluar la fiabilidad de los prestatarios (Fulano es un prestatario fiable), el asegurador (no se espera que Fulano muera pronto) o el laboral (Fulano es un buen trabajador y merece un ascenso).

514 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf.

515 "Ámbito objetivo de aplicación
Artículo 3. El presente Reglamento será de aplicación al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
No se aplicarán las disposiciones del presente Reglamento cuando para acceder a los datos personales se requieran plazos o actividades desproporcionadas.
En términos del artículo 3, fracción V de la Ley, los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable".

516 El artículo 2 del RLFPDPPP indica que, además de las definiciones establecidas en el artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para los efectos del presente "Reglamento se entenderá por:
[...]
XI. Soporte físico: Medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales".

517 La fracción X del artículo 2 del RLFPDPPP indica:
"X. Soporte electrónico: Medio de almacenamiento al que se pueda acceder solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms;".

518 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

En relación con lo anterior, el GTA29 declara que para considerar que los datos versan sobre una persona debe haber un elemento contenido, un elemento finalidad o un elemento resultado.[519]

De acuerdo con el citado órgano de consulta, los elementos anteriores se explican de la siguiente forma:

- Contenido: este elemento está presente en aquellos casos en que —de acuerdo con lo que una sociedad suele, general y vulgarmente, entender por la palabra "sobre"— se proporciona información sobre una persona concreta, independientemente de cualquier propósito que puedan abrigar el responsable del tratamiento de los datos o un tercero o de la repercusión de esa información en el interesado. La información versa sobre una persona cuando se refiere a esa persona, lo que debe ser evaluado teniendo en cuenta todas las circunstancias que rodean el caso.
- Finalidad: el elemento de finalidad existe cuando los datos se utilizan, o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona.
- Resultado: se presenta este elemento cuando a pesar de la ausencia de un elemento de contenido o de finalidad cabe considerar que los datos versan sobre una persona determinada porque, teniendo en cuenta todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos y los intereses de determinada persona. Es decir, basta con que la persona pueda ser tratada de forma diferente por otras personas como consecuencia del tratamiento de tales datos.

Finalmente, debe tenerse en cuenta que estos tres elementos (contenido, finalidad y resultado) deben considerarse como condiciones alternativas y no acumulativas, pues cuando exista el elemento de contenido, no hay ninguna necesidad de que también aparezcan los otros elementos para considerar que la información se refiere a una persona física. [520] Es decir, para determinar si los datos se refieren a una persona hay que contestar, analizando cada dato, en función de sus características.[521]

C. Persona física

Tanto la LFPDPPP como la LGPDPPSO y su normatividad de desarrollo requieren que la información se refiera a una persona física identificada o identificable. Es decir, al tratarse de un derecho humano, las personas físicas son las titulares del mismo al ser un derecho directamente relacionado con la libertad y dignidad de la persona, mientras que las personas morales podrán gozar de prerrogativas distintas como son aquellas relacionadas con la protección de la información que se entregue con el carácter de confidencial.[522]

519 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

520 Ídem.

521 Ídem.

522 En este sentido se puede ver la tesis P. II/2014 (10a.). Décima época, 2005522. *Gaceta del Semanario Judicial de la Federación*. Pleno. Libro 3. Febrero de 2014. Tomo I, p. 274:
"El artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la protección de datos personales, consistente en el control de cada individuo sobre el acceso y uso de la información personal en aras de preservar la vida privada de las personas. En ese sentido, el derecho a la protección de datos personales podría entenderse, en primera instancia, como una prerrogativa de las personas físicas, ante la imposibilidad de afirmar que las morales son titulares del derecho a la intimidad y/o a la vida privada; sin embargo, el contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cierta

D. Identificada o identificable

Se considera que una persona es identificada cuando la información disponible indica directamente a quién pertenece, sin necesidad de realizar una averiguación posterior. Por su parte, una persona es identificable, en términos del artículo 2, fracción VIII del RL-FPDPPP cuando su identidad "pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas".

En consecuencia, para que una información se considere dato personal, deben existir dos elementos: la información y la persona a la que concierne dicha información. Si no concurren ambos habrá que entender que no se trata de datos personales.

En relación con el concepto "identificada" o "identificable" el GTA 29 señala que la identificación se logra, en la mayor parte de los casos, a través de datos identificadores, los cuales tienen una relación privilegiada y muy cercana con una determinada persona.

En el RGPD, por ejemplo, como parte de la definición de dato personal, se presenta un listado ejemplificativo de aquellos datos personales que pueden considerarse como datos de carácter identificador:

> …datos personales: toda información sobre una persona física identificada o identificable (el interesado) se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona...

La normatividad mexicana de datos personales hace referencia a estos identificadores cuando declara que "se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información".[523]

Finalmente, en este contexto, previene el RGPD que en relación con este último elemento, deben considerarse todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente[524] a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.[525]

---

información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo. Por tanto, los bienes protegidos por el derecho a la privacidad y de protección de datos de las personas morales, comprenden aquellos documentos e información que les son inherentes, que deben permanecer ajenos al conocimiento de terceros, independientemente de que, en materia de transparencia e información pública, opere el principio de máxima publicidad y disponibilidad, conforme al cual, toda información en posesión de las autoridades es pública, sin importar la fuente o la forma en que se haya obtenido, pues, acorde con el artículo 6o., en relación con el 16, párrafo segundo, constitucionales, la información entregada a las autoridades por parte de las personas morales, será confidencial cuando tenga el carácter de privada por contener datos que pudieran equipararse a los personales, o bien, reservada temporalmente, si se actualiza alguno de los supuestos previstos legalmente".

523 El Reglamento de la LFPDPPP establece en su artículo 2 la definición de persona física identificable.

524 Por ejemplo, la sentencia emitida por el Tribunal de Justicia de la Unión Europea en el caso "Patrick Beyer vs. la República Federal de Alemania" en la que el tribunal determinó que, bajo ciertas circunstancias, la dirección de IP dinámica podía llegar a constituir un dato personal, puesto que la persona física podría indirectamente ser identificada en caso de que las direcciones de IP dinámicas llegasen a combinarse con la información en posesión de un prestador de servicios de internet, como aquella consistente en las horas de conexión y las páginas de internet visitadas.

525 Considerando (26) del Reglamento General de Protección de Datos: "Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse

Dato personal sensible

Isabel Davara Fernández de Marcos,[526]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La definición de datos personales sensibles en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) tiene dos partes claramente diferenciadas.

De un lado, un primer apartado descriptivo o abierto, que puede dar lugar a interpretación,[527] y que señala que son aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.[528]

De otro, una enumeración[529] que explica que, en concreto, son aquellos datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

En todo caso, a pesar de que es una lista concreta, tampoco puede considerarse que sea un número cerrado y, por lo tanto, la definición puede resultar ambigua y gran parte de su concreción en la práctica dependerá del contexto en el que se realice el tratamiento y así lo establece específicamente la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPSO) que, específicamente, establece que la lista no es limitativa.[530]

---

en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto, los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación".

526 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

527 En este sentido, el INAI señaló en la resolución del Procedimiento de Verificación identificada con el expediente INAI.3S.07.02-039/2017 lo siguiente: "El listado de datos personales sensibles refiere de manera enunciativa más no limitativa la información que reviste dicha naturaleza jurídica, esto es, se destacan ciertos datos personales que el legislador consideró de manera ejemplificativa, como un mínimo a partir del cual se debe desarrollar el concepto de datos personales sensibles. No obstante, esto no impide que el INAI pueda interpretar el contenido del precepto legal en cuestión e incluir datos personales adicionales en este catálogo ya que la sensibilidad de un dato personal debe determinarse atendiendo a las circunstancias particulares del caso concreto […]".

528 En esta misma sintonía, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos indican que se consideran datos sensibles los siguientes: "Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física". (Artículo 2, inciso d., Estándares de Protección de Datos para los Estados Iberoamericanos).

529 La Ley Federal de Protección de Datos personales en Posesión de los Particulares en la fracción VI de su artículo 3 define a los datos personales sensibles de la siguiente forma: "datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual".

530 Artículo 3, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En todo caso, los datos personales sensibles forman parte de un determinado grupo de informaciones susceptibles de una reconsideración respecto a una categoría general y homogénea por sus especiales peculiaridades y características,[531] que los constituye en una categoría especial de datos, protegidos bajo reglas específicas.

En el entorno europeo, el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) para referirse a los datos personales sensibles el término de "categorías especiales de datos" señala que estos merecen especial protección, en virtud de su naturaleza, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales de los titulares.[532] Es resaltable que la denominación europea es muy neutral, pues solo señala que son categorías especiales de datos, sin remitir a otros adjetivos, como sensibles, que pueden generar cierto desconcierto, dado que la sensibilidad no es un término objetivo sino que depende del sujeto al que le concierne.

En la práctica, se busca restringir aún más la posibilidad legal de su tratamiento. De un lado, mediante herramientas normativas, como la imposibilidad de crear bases de datos con el exclusivo fin de tratar estos datos, y con la exigencia en nuestra normatividad de un consentimiento reforzado para su tratamiento, así como el establecimiento de medidas de seguridad reforzadas. De otro, en caso de un tratamiento ilícito de los mismos, las sanciones son más elevadas.

Como decíamos, la definición legal implica que no solo se encuentren dentro de la categoría datos personales sensibles los que por su naturaleza lo sean, sino también otros a partir de los cuales se puede inferir información personal sensible de una persona. Por lo tanto, no se trata de una definición estática ni monótona, ya que el contexto y las consecuencias del tratamiento puede convertir a una categoría de datos no especial a simple vista en datos sensibles.

La protección específica y reforzada para este tipo de datos parte de la presunción de que un uso ilícito de los mismos podría tener consecuencias más severas y de gran impacto, no solo sobre el derecho mismo a la protección de datos personales, sino también sobre otros derechos y libertades individuales como la dignidad de la persona, el derecho a la libertad de pensamiento, la libertad religiosa, el honor, la no discriminación, la intimidad y la vida privada y familiar de la persona. De ahí la redacción de la normatividad mexicana que explícitamente señala que la protección de estos datos es relevante debido a que "su utilización indebida puede dar origen a discriminación o conllevar un riesgo grave para el titular" (artículo 3, VI de la LFPDPPP y 2, X de la LGPDPPSO).

La normatividad de los sectores público (LGPDPPSO) y privado (LFPDPPP) establece condiciones específicas para el tratamiento de estos datos personales para prevenir su tratamiento indebido.

En este orden de cosas, la LGPDPPSO[533] y la LFPDPPP[534] prevén las siguientes garantías reforzadas:

1. Prohíben la creación de bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el responsable del tratamiento. Es decir, todas las bases de datos deben cumplir con una finalidad legítima

531 Álvarez, S. (2007). *Derechos fundamentales y protección de datos genéticos*. España. Dykinson, pp. 50-51.

532 *Vid*, Considerando (51) del Reglamento General de Protección de Datos.

533 Artículo 7 de la LGPDPPSO.

534 Segundo párrafo del artículo 9 de la LFPDPPP.

y concreta, pero la gran diferencia estriba en que la creación de bases de datos sensibles debe ir acorde con las actividades o fines del tratamiento informados en el aviso de privacidad y que justifiquen el tratamiento de los datos personales.

2. Establecen que cuando el tratamiento requiera del consentimiento del titular, en el caso de los datos personales sensibles se requerirá que sea expreso y por escrito, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación equivalente.[535]
3. Establecen la obligación de informar, de forma expresa, a través del aviso de privacidad sobre tratamiento de esta categoría de datos, mismo que debe ser el que resulte necesario, adecuado y relevante en relación con las finalidades que justifiquen su tratamiento y que se encuentren previstas en el aviso de privacidad.
4. Disponen que el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.[536]
5. El responsable debe reforzar las medidas de seguridad físicas, técnicas y administrativas para garantizar la seguridad de los datos personales.
6. En el supuesto de que las infracciones a la normatividad versen sobre el tratamiento de datos personales sensibles, las sanciones podrán incrementarse hasta por dos veces los montos establecidos.[537]

Datos personales biométricos

Isabel Davara Fernández de Marcos,[538]
Gregorio Barco Vega y
Alexis Cervantes Padilla

Los datos biométricos son datos personales de carácter sensible[539] referentes a las propiedades físicas, fisiológicas,[540] de comportamiento o rasgos de la personalidad, mesurables y que conciernen a una persona física identificada o identificable.[541]

El Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) en el apartado 14 de su artículo 4 dispone que los datos biométricos son datos persona-

535 Artículo 9 de la LFPDPPP y artículo 21 de la LGPDPPSO.

536 *Vid*, artículo 13 de la LFPDPPP.

537 *Vid*, artículo 64, fracción IV de la LFPDPPP.

538 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

539 Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos precisan que se consideran como datos sensibles los datos biométricos al definir a los datos sensibles de la siguiente forma: "Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física". (Artículo 2, inciso d, de Estándares de Protección de Datos para los Estados Iberoamericanos).

540 El GTA29 establece que, las muestras de tejido humano (al igual que las muestras de sangre) son fuentes a partir de las cuales se extraen datos biométricos, pero no son en sí mismas datos biométricos (por ejemplo, un modelo de huellas dactilares es un dato biométrico, pero no así un dedo). Cfr. Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

541 INAI. (2018). *Guía para el Tratamiento de Datos Biométricos*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf Fecha de consulta: 5 de septiembre de 2018.

les obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

De acuerdo con el Grupo de Trabajo del Artículo 29 (GTA29 o WP29 por sus siglas en inglés),[542] los datos biométricos se definen como: "Propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad".[543] El citado órgano de consulta europeo identifica como ejemplos de datos biométricos los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial y las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etcétera).[544]

En el terreno nacional no encontramos una definición normativa de datos personales biométricos. Sin embargo, podemos encontrar documentos publicados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en los que se ha definido el alcance de este concepto:

A. *Guía del INAI sobre el tratamiento de datos biométricos*: señala que los datos biométricos son propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad, atribuibles a una sola persona y que son medibles.[545]

B. Resoluciones: en la resolución del procedimiento de verificación identificada con el expediente INAI.3S.07.02-039/2017, el INAI definió a los datos biométricos como "Aquellos rasgos físicos, biológicos de comportamiento de un individuo que lo identifican como único del resto de la población como pueden ser de manera enunciativa mas no limitativa, la imagen del iris, los rasgos faciales, el patrón de voz y la huella digital".[546]

En consecuencia, se puede afirmar que los datos biométricos son datos personales sensibles relacionados con las propiedades físicas, fisiológicas, de comportamiento o rasgos de la personalidad mesurables y que corresponden a una persona física identificada o identificable.

1. Características

Los datos personales biométricos con independencia de la finalidad de su uso, según el GTA29[547] suelen tener las siguientes características:

a) universales, ya que son datos con los que contamos todas las personas;

542 Este grupo se creó en virtud del artículo 29 de la directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la directiva 95/46/CE y en el artículo 15 de la directiva 2002/58/CE.

543 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

544 Ídem.

545 INAI. (2018). *Guía para el Tratamiento de Datos Biométricos*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

546 INAI. (2017). Resolución del Procedimiento de Verificación 3S.07.02-039/2017. Disponible en: http://inicio.ifai.org.mx/pdf/resoluciones/2017/03S%2002-039.pdf Fecha de consulta: 4 de septiembre de 2018.

547 Grupo de Trabajo del Artículo 29, WP 80. Documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp80_es.pdf Fecha de consulta: 5 de septiembre de 2018.

b) únicos, ya que no existen dos biométricos con las mismas características por lo que nos distinguen de otras personas;

c) permanentes, ya que se mantienen, en la mayoría de los casos, a lo largo del tiempo en cada persona, y

d) medibles de forma cuantitativa.

Derivado de lo anterior, se distinguen dos tipos de técnicas biométricas:

I. Técnicas basadas en aspectos físicos y fisiológicos que miden las características fisiológicas de una persona e incluyen: comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN y análisis de los poros de la piel, etc.

II. Técnicas basadas en aspectos comportamentales que miden el comportamiento de una persona e incluyen la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, etc.

2. Los datos biométricos como datos personales

Una particularidad de los datos biométricos es que se les puede considerar como contenido de la información concerniente a una persona física determinada y como un elemento para vincular una información a una determinada persona. De esta manera, los datos biométricos pueden servir como identificadores de la persona, pues al corresponder a una única persona, los datos biométricos pueden utilizarse para identificarla.[548]

En este contexto, los datos biométricos siempre pueden considerarse como "información sobre una persona física" ya que afectan a datos que proporcionan, por su propia naturaleza, información sobre una persona determinada. En el contexto de la identificación biométrica, la persona es generalmente identificable porque los datos biométricos se usan para identificar o autenticar/comprobar al menos en la medida en que el interesado se distingue de cualquier otro.[549]

La capacidad de identificar a una persona depende también de la disponibilidad de otros datos que (conjunta o separadamente) permiten la identificación de la persona en cuestión.[550] La posibilidad de una identificación directa por medio de uno o varios elementos específicos, característicos de su identidad física se menciona explícitamente en la definición de datos personales prevista en las normatividades de datos personales aplicables para el sector público[551] y el sector privado[552] que definen al dato personal como "cualquier información concerniente a una persona física identificada o identificable".

548 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

549 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

550 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

551 La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala, en la fracción IX de su artículo 3, "… IX. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información…"

552 La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en la fracción V del artículo 3, señala: "Para los efectos de esta Ley, se entenderá por (V.) datos personales a cualquier información concerniente a una persona física identificada o identificable".

Además de lo anterior, de acuerdo con lo previsto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), se considera que una persona es identificable cuando su identidad pueda determinarse, directa o indirectamente a través de cualquier información.

En consecuencia, se considera que para que el dato biométrico sea considerado como dato personal debe referirse a una persona física e identificar o hacer identificable a su titular.

3. Los datos biométricos como datos personales sensibles

Pese a que los datos biométricos no se encuentran previstos de forma específica en el listado de datos personales sensibles referidos en la LFPDPPP y la LGPDPPSO, dicha situación no es obstáculo para que no puedan tener el calificativo de datos sensibles. Por ejemplo, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) los ubican dentro de la categoría de datos personales sensibles.[553]

Conforme a la normatividad nacional, para que los datos personales biométricos puedan ser considerados como datos personales sensibles deben referirse a la esfera más íntima de su titular o implicar un riesgo grave o discriminación para su titular como consecuencia de su tratamiento indebido.[554]

De esta forma, cuando los datos biométricos se encuadran como parte de categorías especiales de datos, quedan sujetos a un régimen legal de especial protección que limita la creación de bases de datos con dicha información y conmina a los responsables a limitar su tratamiento para fines explícitos y necesarios para dar cumplimiento a una lícita finalidad del tratamiento (ver definición de datos sensibles en la presente obra).

Datos personales genéticos

Isabel Davara Fernández de Marcos,[555]
Gregorio Barco Vega y
Alexis Cervantes Padilla

Los datos genéticos no tienen una definición legal en el panorama jurídico mexicano. Sin embargo, en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) sí se hace una mención específica de los mismos, al enumerarlos como una clase más dentro de los datos sensibles.[556]

553 En este sentido, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos precisan que se consideran como datos sensibles los datos biométricos al definir a los datos sensibles de la siguiente forma: "Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física". (Artículo 2, inciso d de los Estándares de Protección de Datos para los Estados Iberoamericanos).

554 Artículo 3, fracción VI de la Ley Federal de Protección de Datos personales en Posesión de los Particulares y artículo 3, fracción X de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

555 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

556 El artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su fracción X, define a los datos sensibles de la siguiente manera: "Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más

En el ámbito regional, en el mismo sentido, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) incluyen dentro de los de los datos sensibles a los datos genéticos, aunque igualmente sin prever una definición sobre estos últimos.[557]

En el panorama internacional, la Declaración Internacional sobre los Datos Genéticos Humanos, del 16 de octubre de 2003, de la UNESCO (DIDGH) define a este tipo de datos como la "información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos".[558]

La Recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre protección de datos médicos (Recomendación sobre Datos Médicos) señala que los datos genéticos se refieren a todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. Dentro de esta definición, también se incluyen todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya sea que se presente con características identificables o no.[559]

El Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) en el apartado 13 de su artículo 4 define a los datos genéticos como: "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona".

De acuerdo con el *Diccionario de la Real Academia Española* (RAE), la información genética es el "conjunto de mensajes codificados en los ácidos nucleicos que origina la expresión de los caracteres hereditarios propios de los seres vivos mediante reacciones bioquímicas".[560]

En relación con las características de los datos genéticos, Romeo Casabona[561] señala las siguientes particularidades:

---

no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual".

557 Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos indican que se consideran datos sensibles los siguientes: "Datos personales sensibles: aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física". (Artículo 2, inciso d de los Estándares de Protección de Datos para los Estados Iberoamericanos).

558 "Artículo 2: [...] i) Datos genéticos humanos: información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos; [...]".

559 Apéndice a la recomendación nº R (97) 5, de 13 de febrero de 1997.
"1. Definiciones
- la expresión "datos médicos" se refiere a todos los datos personales relativos a la salud de un individuo. Se refiere también a los datos que tengan una clara y estrecha relación con la salud y los datos genéticos.
- la expresión "datos genéticos" se refiere a todos los datos, cualquiera que sea su clase, relativos a las características hereditarias de un individuo o al patrón hereditario de tales características dentro de un grupo de individuos emparentados. También se refiere a todos los datos sobre cualquier información genética que el individuo porte (genes) y a los datos de la línea genética relativos a cualquier aspecto de la salud o la enfermedad, ya se presente con características identificables o no. La línea genética es la línea constituida por similaridades genéticas resultantes de la procreación y compartidas por dos o más individuos".

560 RAE. (2017). Información genética. En *Diccionario de la Lengua Española*. Disponible en: http://dle.rae.es/?id=LXrOqrN#MfSTJ1P Fecha de consulta: 5 de septiembre de 2018.

561 Romeo C. (2016). *Los genes y sus leyes*. España. Comares, p. 63.

a) Permanencia e inalterabilidad de la información genética, que no depende de la voluntad del individuo.
b) Singularidad, salvo en los gemelos monocigóticos.
c) Vinculación biológica con los demás miembros de la familia. Se trata de información generacional no vinculada, tal y como sucede con otro tipo de datos, únicamente al sujeto portador, sino que se trasmite entre generaciones.
d) Capacidad predictiva, tanto en enfermedades monogenéticas como en enfermedades plurigenéticas.

Dicha información, según Álvarez González puede ser obtenida a través de la realización de análisis genéticos que revelan o pueden revelar datos biológicos sobre la salud presente, pasada o futura, predisposición o susceptibilidad de padecer una enfermedad y las relaciones biológicas con terceras personas, y mediante "fuentes tradicionales de información", como la historia familiar.[562]

Los datos genéticos revisten características que los convierten en categorías especiales de datos. De acuerdo con el Grupo de Trabajo del Artículo 29 (GTA29),[563] los datos genéticos revelan características inherentes que los singularizan, puesto que proporcionan o podrán proporcionar, en el futuro, la información científica, médica y personal (que concierne a una física identificada o identificable) pertinente durante toda la vida de una persona. Esta información puede también incidir significativamente en la familia de la persona en cuestión, durante varias generaciones y, en algunos casos, en el conjunto del grupo al que pertenece esta persona.[564]

La DIDGH[565] en su artículo 4 establece que los datos genéticos son singulares por las siguientes razones:

a) Pueden indicar predisposiciones genéticas de los individuos.
b) Pueden tener consecuencias importantes que se perpetúen durante generaciones para la familia, comprendida la descendencia, y a veces para todo el grupo al que pertenezca la persona en cuestión.
c) Pueden contener información cuya relevancia no se conozca necesariamente en el momento de extraer las muestras biológicas.

562 Álvarez, S. (2007). *Derechos fundamentales y protección de datos genéticos*. España. Dykinson, p. 43.

563 Este Grupo se creó en virtud del artículo 29 de la directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y del derecho a la intimidad. Sus funciones se describen en el artículo 30 de la directiva 95/46/CE y en el artículo 15 de la directiva 2002/58/CE.

564 Grupo de Trabajo del Artículo 29. *Documento de trabajo sobre datos genéticos, WP 91, adoptado el 17 de marzo de 2004.* Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_es.pdf Fecha de consulta: 5 de septiembre de 2018.

565 En este sentido, la Declaración Internacional sobre los Datos Genéticos Humanos señala lo siguiente:
"Artículo 4.
Singularidad
a) Los datos genéticos humanos son singulares porque:
i) pueden indicar predisposiciones genéticas de los individuos;
ii) pueden tener para la familia, comprendida la descendencia, y a veces para todo el grupo al que pertenezca la persona en cuestión, consecuencias importantes que se perpetúen durante generaciones;
iii) pueden contener información cuya relevancia no se conozca necesariamente en el momento de extraer las muestras biológicas;
iv) pueden ser importantes desde el punto de vista cultural para las personas o los grupos.
b) Se debería prestar la debida atención al carácter sensible de los datos genéticos humanos e instituir un nivel de protección adecuado de esos datos y de las muestras biológicas".

d) Pueden ser importantes desde el punto de vista cultural para las personas o los grupos.

Como características de los datos genéticos, además, el GTA29[566] ha identificado las siguientes:

a) Si bien la información genética es única y distingue a una persona de las demás, también puede revelar información sobre la persona y tener implicaciones para sus consanguíneos (familia biológica), incluidas las generaciones anteriores y posteriores. Por otra parte, los datos genéticos pueden caracterizar a un grupo de personas (por ejemplo, comunidades étnicas).

b) Los datos genéticos pueden revelar vínculos de parentesco y de familia.

c) El propio portador desconoce a menudo la información genética y ésta no depende de su voluntad individual dado que los datos genéticos no son modificables.

d) Los datos genéticos pueden obtenerse fácilmente o extraerse de materias primas, aunque estos datos pueden, a veces, ser de dudosa calidad, si se tiene en cuenta la evolución de la investigación, los datos genéticos podrán revelar aún más información en el futuro y ser utilizados por un número creciente de organismos con distintos fines.

Debido a estas especificidades, el tratamiento de los datos genéticos requiere y justifica una protección jurídica particular,[567] principalmente cuando son terceros los que acceden a los datos personales.

En la normatividad aplicable al sector público, los datos genéticos son considerados datos personales sensibles al encontrarse previstos en la fracción X del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que define a los datos personales sensibles de la siguiente forma:

> Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, **información genética**, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual. (Énfasis agregado).

Además, derivado de lo previsto en el inciso d) del artículo 2 de los Estándares de Protección de Datos para los Estados Iberoamericanos los datos genéticos son considerados datos de carácter sensible:

> Aquellos que se refieran a la esfera íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física.

Aquí habría que señalar resoluciones: Si bien en la definición de datos sensibles aplicable al sector privado no señala específicamente entre los mismos a los datos genéticos son considerados sensibles en razón de que la información genética puede permitir identificar a las personas, relacionarlas entre sí y revelar datos complejos sobre su salud y evolución futura de estas personas y de otras con las que estén genéticamente relacionadas.[568] Los datos genéticos

566 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

567 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

568 Grupo de Trabajo del Artículo 29. Dictamen 6/2000 sobre el genoma humano y la vida privada, aprobado el 13 de julio de 2000, WP 34. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp34_es.pdf Fecha de consulta: 5 de septiembre de 2018.

son datos relativos a la salud (y por tanto sensibles) cuando revelan el estado de salud físico o psíquico pasado, presente y futuro de un individuo.[569] No obstante, en determinados casos, lo datos genéticos también pueden referirse a otros aspectos como la relación del individuo con terceras personas, su origen étnico, entre otros aspectos que hacen que estos datos no necesariamente encajen como datos de salud.[570]

Al respecto, el GTA29 puntualiza que la correcta protección de los datos genéticos puede considerarse como una condición previa para garantizar el respeto del principio de igualdad y para que el derecho a la salud exista realmente,[571] pues los datos genéticos constituyen información cuyo uso ilícito podría acarrear consecuencias negativas para el titular, entre ellas, la discriminación con motivo de la revelación de aspectos complejos sobre el estado de salud presente y/o futuro de las personas.

Así, es preciso señalar que el calificativo "sensibles" de los datos genéticos tiene su razón de ser como resultado de varias cuestiones, en primer lugar, por la propia naturaleza de los mismos, que muchas veces se ven relacionados con categorías de datos que ya de por sí son considerados sensibles (como, por ejemplo, los datos de salud o el origen étnico) y porque su tratamiento puede dar lugar a un riesgo grave o una discriminación de su titular.

En la práctica, son diversos los instrumentos internacionales que han establecido el derecho de las personas a no ser discriminadas con motivo de su patrimonio genético. Al respecto, la Declaración Universal sobre el Genoma Humano y los Derechos Humanos del 11 de noviembre de 1997 de la UNESCO indica que ninguna persona podrá ser discriminada con motivo de sus características genéticas:

> Artículo 6
>
> Nadie podrá ser objeto de discriminaciones fundadas en sus características genéticas, cuyo objeto o efecto sería atentar contra sus derechos humanos y libertades fundamentales y el reconocimiento de su dignidad.

Por otro lado, el convenio relativo a los Derechos Humanos y la Biomedicina del 4 de abril de 1997, conocido en el ámbito internacional como Convenio de Oviedo o Convenio de Asturias impuesto por el Consejo de Europa, establece la regla de no discriminación personal como parte del patrimonio genético en su artículo 11:

> Artículo 11
>
> No discriminación
>
> Se prohíbe toda forma de discriminación de las personas por su patrimonio genético.

La DIDGH en su artículo 7 reitera la obligación de no discriminación al tenor siguiente:

> Artículo 7: No discriminación y no estigmatización
>
> a) Debería hacerse todo lo posible por garantizar que los datos genéticos humanos y los datos proteómicos humanos no se utilicen con fines que discriminen, al tener por objeto o consecuencia la violación de los derechos humanos, las libertades fundamentales o la dignidad humana de una persona, o que provoquen la estigmatización de una persona, una familia, un grupo o comunidades.
>
> b) A este respecto, habría que prestar la debida atención a las conclusiones de los estudios de genética de poblaciones y de genética del comportamiento y a sus interpretaciones.

569 Álvarez, S. (2007). *Derechos fundamentales y protección de datos genéticos*. España. Dykinson, p. 43.

570 Álvarez, S. (2007). *Derechos fundamentales y protección de datos genéticos*. España. Dykinson, p. 43.

571 Grupo de Trabajo del Artículo 29. *Documento de trabajo sobre datos genéticos, WP 91, adoptado el 17 de marzo de 2004.* Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_es.pdf Fecha de consulta: 5 de septiembre de 2018.

Así es que se vuelve indispensable limitar el acceso a los datos genéticos y su utilización. La Declaración Universal sobre Bioética y Derechos Humanos, en su artículo 17, ha previsto lo siguiente:

> Artículo 17. Protección del medio ambiente, la biosfera y la biodiversidad.
>
> Se habrán de tener debidamente en cuenta la interconexión entre los seres humanos y las demás formas de vida, la importancia de un acceso apropiado a los recursos biológicos y genéticos y su utilización, el respeto del saber tradicional y el papel de los seres humanos en la protección del medio ambiente, la biosfera y la biodiversidad.

De esta manera, es dable sostener que los datos genéticos constituyen información que revela una amplia gama de características específicas que pueden revelar aspectos íntimos del titular o de terceros y cuyo tratamiento no autorizado podría generar un perjuicio en los derechos y libertades fundamentales de su titular y/o titulares, por lo que su protección reforzada es legalmente requerida.

Datos personales relativos a la salud

Isabel Davara Fernández de Marcos,
Gregorio Barco Vega y
Alexis Cervantes Padilla

Según la normatividad vigente,[572] los datos relativos a la salud son datos personales de carácter sensible, en tanto que se refieren al estado de salud física o mental de un individuo. Los datos relativos a la salud incluyen la prestación de servicios de atención médica que puede revelar información sobre el estado de salud actual, presente o futuro de su titular.

No obstante, es preciso señalar que en la legislación nacional aplicable a los sectores público y privado no existe una definición concreta de datos relativos a la salud, por lo que la delimitación de este concepto la apoyaremos en distintas fuentes teóricas y normativas.

El Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés), en el apartado 15 de su artículo 4, define a los datos relativos a la salud como "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud".[573]

En relación con lo anterior, el considerando 35 del RGPD indica que deben considerarse incluidos los datos relativos al estado de salud del interesado (titular en términos de la normatividad nacional) que dan información sobre su estado de salud física o mental pasado, presente o futuro. De acuerdo con el RGPD, en esta categoría se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria,[574] o con ocasión de la prestación de tal asistencia.

572 La Ley Federal de Protección de Datos personales en Posesión de los Particulares en la fracción VI de su artículo 3 define a los datos personales sensibles de la siguiente forma: "Datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual". Por su parte, el artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su fracción X, define a los datos sensibles de la siguiente manera: "Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual".

573 Artículo 4, apartado 15, del Reglamento General de Protección de Datos.

574 Al respecto, la Directiva 2011/24/UE del Parlamento Europeo y del Consejo del 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, señala:

Así, el RGPD considera que los datos relativos a la salud pueden incluir un listado amplio:

> Todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.[575]

La definición "datos relativos a la salud" pertenece a un conjunto y subconjunto a su vez. Por un lado, la denominación de "dato personal" es genérica, debido a que son datos personales pues se trata de información concerniente a una persona física identificada o identificable, esto es, no son disociados, remitiéndonos a la voz correspondiente en esta obra para delimitar dicho alcance. Además de lo anterior, dada la naturaleza especial de estos datos, se considera que entran bajo la categoría de datos sensibles a los que hace referencia la normatividad de datos personales vigente en México, de nuevo remitiéndonos a la voz específica para delimitar el alcance de la misma.

El otro elemento de la definición es la referencia que se hace al concepto de salud. Para entender a qué se refiere la expresión datos relativos a la salud se debe explicar qué se entiende por salud al ser el concepto correlacionado con dicho tratamiento. De acuerdo con el *Diccionario de la Real Academia de la Lengua Española* (DRAE) se entiende por salud al "conjunto de condiciones físicas en que se encuentra un organismo en un momento determinado".[576]

Por otro lado, en la faceta normativa, la Ley General de Salud (LGS) establece en su artículo primero que se entiende por salud un estado de completo bienestar físico, mental y social, y no solamente la ausencia de afecciones o enfermedades.

Los datos relativos a la salud son considerados datos personales sensibles, según se dispone en la normatividad de datos personales aplicable al sector público y al sector privado,[577] considerando que estos pueden referirse a la esfera más íntima de su titular o bien su tratamiento ilícito pueden implicar un riesgo grave o discriminación para su titular.

Asimismo, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) identifican en el inciso d) de su artículo 2 a los datos relativos a la salud como datos de carácter sensible.[578]

Artículo 3
Definiciones
A los efectos de la presente directiva, se entenderá por:
a) asistencia sanitaria: los servicios relacionados con la salud prestados por un profesional sanitario a pacientes para evaluar, mantener o restablecer su estado de salud, incluidos la receta, dispensación y provisión de medicamentos y productos sanitarios.

575 (35) Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la directiva 2011/24/UE del Parlamento Europeo y del Consejo (9); todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico o una prueba diagnóstica in vitro.

576 RAE. (2017). Salud. *Diccionario de la Real Academia de la Lengua Española*. Disponible en: http://dle.rae.es/?id=X7MRZku

577 Artículo 3, fracción VI de la Ley Federal de Protección de Datos personales en Posesión de los Particulares.

578 En esta misma sintonía, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos indican que se consideran datos sensibles los siguientes: "Datos personales sensibles: aquellos que se refieran a la esfera íntima de

Derivado de la naturaleza sensible de los datos relativos a la salud, se considera que estos deben ubicarse bajo un régimen de protección legal especial ya que su utilización no autorizada podría afectar los derechos y libertades fundamentales del titular de los datos personales.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[579] y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[580] prohíben la creación de bases de datos que contengan datos personales sensibles. Esta regla se aplica a los datos relativos a la salud, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el responsable del tratamiento. Es decir, si bien todas las bases de datos deben cumplir con una finalidad legítima y concreta, la creación de bases de datos sensibles debe ir acorde con las actividades o fines del tratamiento que persigue el responsable.

Asimismo, según disponen la LFPDPPP[581] y la LGPDPPSO,[582] cuando se requiera el consentimiento para el tratamiento de datos personales sensibles, como es el tratamiento de datos relativos a la salud, éste deberá ser expreso y por escrito, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca.

En consecuencia, el tratamiento de datos personales relativos a la salud, además, deberá ser el que resulte necesario, adecuado y relevante[583] en relación con las finalidades que justifiquen su tratamiento y que se encuentren previstas en el aviso de privacidad, el cual deberá señalar explícitamente el tratamiento de estos datos. En especial, frente a éste, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.[584]

---

su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, preferencia u orientación sexual, datos genéticos o datos biométricos dirigidos a identificar de manera unívoca a una persona física". (Artículo 2, inciso d de los Estándares de Protección de Datos para los Estados Iberoamericanos).

579 "Artículo 7. Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley".

580 En este sentido, el segundo párrafo del artículo 9 de la LFPDPPP indica lo siguiente: "No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado".

581 "Artículo 9. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca [...]".

582 En este sentido, el último párrafo del artículo 21 de la LGPDPPSO indica lo siguiente: "Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta Ley".

583 El artículo 25 de la LGPDPPSO.

584 Artículo 13 de la LFPDPPP.

Deber de confidencialidad

Uciel Fragoso Rodríguez

La confidencialidad es la propiedad que posee un objeto, acción, pensamiento, idea, información o cualquier ente de no ser divulgado o expuesto a entidades no autorizadas.

En el caso de la información, constituye una de las piedras angulares junto con la integridad y la disponibilidad de lo que es la seguridad de la información, características conocidas como la triada de la seguridad.

Por otro lado, el deber de confidencialidad es la obligación que tiene una entidad de resguardar la confidencialidad de lo que tiene bajo responsabilidad o custodia. En algunas profesiones como la medicina, el derecho, la psicología, el periodismo o la milicia, se considera un principio ético o de secreto profesional.

En el ámbito de los datos personales, el deber de confidencialidad es tratado en diversas legislaciones, por ejemplo, el artículo 21 de la LFPDPPP expresa:[585]

> Artículo 21. El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de estos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Y el artículo 63 de la misma ley agrega:

> Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:
>
> [...]

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley.

El artículo 21 confiere la obligación de preservar la confidencialidad de los datos personales a toda persona que realice algún tratamiento a los datos personales durante su ciclo de vida, esta obligación estará vigente aun después de terminar la relación con el titular de los datos, y, por lo tanto, finalice cualquier actividad que tenga que ver con el tratamiento de los mismos. Mientras que el artículo 63 establece que es una infracción a la Ley no cumplir con el deber de confidencialidad y, por lo tanto, dicho incumplimiento será sancionado.

Por otro lado, el RLFPDPPP[586] establece claramente en el artículo 50 las obligaciones del encargado en el tratamiento de los datos personales:

> Artículo 50. El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:
>
> [...]
>
> IV. Guardar confidencialidad respecto de los datos personales tratados.

En el caso de que los datos personales sean tratados en el denominado cómputo en la nube, el artículo 52 establece que el deber de confidencialidad debe extenderse a los proveedores de cómputo en la nube como se menciona a continuación:

> Artículo 52. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, solo podrá utilizar aquellos servicios en los que el proveedor:

585 DOF. (2010, julio). "Ley Federal de Protección de Datos Personales en Posesión de los Particulares", en *Diario Oficial de la Federación*. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

586 DOF. (2011, diciembre). Artículo 61 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

I. Cumpla, al menos, con lo siguiente:

a) Guardar confidencialidad respecto de los datos personales sobre los que preste el servicio.

El deber de confidencialidad también aplica a entidades federales que hagan tratamiento de datos personales, según se establece en los artículos 31, 42, 59, 64, 67, 82 y 163 de la LGPDPPSO[587] y en los artículos 71 y 72 de LGPDPSP.[588]

Prácticamente en todos los artículos de la Ley y de los Lineamientos Generales que tratan sobre el deber de confidencialidad, establecen que los responsables y encargados del tratamiento de los datos personales a lo largo del ciclo de vida e independientemente de su ubicación y de los sistemas empleados para su tratamiento, deben implementar mecanismos de seguridad de carácter administrativo, físico o técnico.

Los mecanismos de seguridad del tipo administrativo implican realizar modificaciones en los procesos de negocio de las organizaciones, cambios en la asignación de roles y responsabilidades de las personas que tratan datos personales, utilización de instrumentos jurídicos, programas de capacitación y concientización, entre otros.

Como los datos personales pueden estar contenidos en cualquier medio y en diferentes formatos, no solamente en forma electrónica en sistemas informáticos, los mecanismos de seguridad físico para garantizar el deber de confidencialidad incluyen medidas de control de acceso físico a los datos personales.

Por otro lado, los mecanismos de seguridad de carácter técnico implican el uso de infraestructura tecnológica para garantizar el deber de confidencialidad en los datos personales en cualquier etapa del ciclo de vida de su tratamiento. En forma general, los mecanismos de seguridad técnicos para garantizar la confidencialidad se clasifican en:

a) mecanismos de cifrado
b) mecanismos de control de acceso
c) mecanismos de prevención de fuga de datos

Los mecanismos de cifrado consisten en el uso de algoritmos matemáticos o lógicos de sustitución y de reemplazo para modificar los datos personales de tal forma que sean ilegibles aun cuando sean accedidos por personas no autorizadas. Los algoritmos de transformación operan mediante una clave o llave que debe ser conocida únicamente por la entidad que realiza el cifrado y las entidades autorizadas para descifrar los datos personales y hacer el tratamiento correspondiente. La tecnología de cifrado es ampliamente utilizada para la protección de la información y puede aplicarse a los datos que se encuentran almacenados (en reposo) o datos que se están procesando o transmitiendo (en movimiento) a lo largo del ciclo de vida de los datos personales.

Los mecanismos de control de acceso para garantizar el deber de confidencialidad consisten en tecnologías que garantizan que el acceso a los datos personales es otorgado únicamente a personas autorizadas.

El control de acceso está compuesto por dos funcionalidades: autenticación y autorización.

La autenticación consiste en la validación de la identidad de las personas que tienen acceso a los datos personales. La autenticación se realiza mediante la verificación de credenciales presentadas por las personas. Las credenciales se clasifican en tres tipos o factores:

587 Segob. (2017, enero). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados". *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

588 INAI. (2017). *Lineamientos Generales de Protección de Datos Personales para el Sector Público*.

a) factor I: algo que se sabe, como pudiera ser una contraseña, una clave, una respuesta, reconocer una imagen, entre otros.

b) factor II: algo que se tiene, como pudiera ser un *token*, un certificado digital, una *cookie*, entre otros.

c) factor III: algo que se es, como pudiera ser cualquier elemento biométrico (huella digital, reconocimiento de voz, reconocimiento facial, entre otros).

Una vez que la persona se autenticó en forma segura, la segunda funcionalidad del control de acceso consiste en la autorización, es decir, a qué tipo de datos personales se tiene acceso y qué tipo de tratamiento se puede realizar. La autorización segura se logra mediante una adecuada definición de roles y responsabilidades, así como una correcta asignación de privilegios sobre el tratamiento de los datos personales.

Los mecanismos de prevención de fuga de datos tienen como finalidad evitar la transmisión no autorizada de datos personales.

Los sistemas informáticos que procesan datos personales tienen múltiples aplicativos y canales de comunicación por donde pueden fugarse datos personales. Los controles de prevención de fuga de datos personales son componentes de *hardware* y *software* que analizan el flujo de información y bloquean cualquier transmisión de datos personales no autorizado.

La LFPDPPP[589] en el capítulo V, "Los deberes y las obligaciones que cumplir", recomienda una serie de acciones que deberá llevar a cabo el responsable del tratamiento de datos personales para garantizar el cumplimiento del deber de confidencialidad.

Para guardar confidencialidad de los datos personales, aun después de terminar la relación con el titular se recomienda:

a) implementar procedimientos para evitar la fuga de información;

b) establecer procedimientos seguros de control de acceso a los datos personales y

c) capacitar al personal en relación a sus obligaciones en el tratamiento de datos personales.

Para garantizar que los encargados del tratamiento de datos personales a nombre del responsable cumplan con el deber de confidencialidad, se propone:

a) agregar cláusulas de confidencialidad en los contratos realizados con terceros o establecer explícitamente acuerdos de confidencialidad (NDA por sus siglas en inglés) y

b) realizar verificaciones periódicas a las actividades de los encargados para garantizar que cumplan con el deber de confidencialidad en torno a la protección de datos personales.

Los procedimientos para evitar fuga de información y para establecer un control de acceso seguro ya fueron explicados en párrafos anteriores.

La capacitación al personal que realiza tratamiento de datos personales es un mecanismo muy eficiente para garantizar el deber de confidencialidad. Se trata de un control de seguridad del tipo administrativo que sensibiliza a las personas sobre su responsabilidad y permite que con acciones simples se tenga una alta protección de los datos. Los planes de capacitación deben diseñarse e instrumentarse de acuerdo con el perfil y las responsabilidades de las personas a lo largo del ciclo de vida de los datos personales.

En caso de los encargados o terceros que realicen tratamiento de datos personales a nombre del responsable y cuya infraestructura tecnológica quede fuera del control del respon-

589 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

sable, existen mecanismos de seguridad del tipo administrativo para garantizar el deber de confidencialidad.

El primer mecanismo es establecer una responsabilidad formal mediante acuerdos de confidencialidad o cláusulas dentro de los contratos que impliquen obligaciones y en su caso sanciones en caso de incumplimiento.

El segundo mecanismo es a través de verificaciones formales a todas las actividades relacionadas con el tratamiento de datos personales. Las verificaciones deben realizarse en forma periódica y podrá llevarse a cabo mediante pruebas que traten de violentar los mecanismos de seguridad existentes para salvaguardar la confidencialidad de los datos personales o también se podrá realizar una revisión de evidencias que comprueben que se están realizando todas las acciones recomendadas para garantizar el cumplimiento del deber de confidencialidad.

Deber de seguridad

Uciel Fragoso Rodríguez

La seguridad de la información se define como el conjunto de reglas, procedimientos y controles para asegurar las siguientes características de la información: confidencialidad, integridad y su disponibilidad, características conocidas como la triada de la información.

Asegurar la confidencialidad de la información significa que no será expuesta o accedida por entidades no autorizadas. Garantizar la integridad de la información significa que su creación, modificación o eliminación la podrán realizar solo entidades autorizadas. En el caso de la disponibilidad, implica que la información estará lista para para acceder a ella en el momento que se necesite y en la forma requerida.

Las reglas o políticas indican los lineamientos a seguir para garantizar la seguridad de la información. Las políticas son reflejo de los principios rectores de cada organización y deben estar alineadas a su misión y visión. Las políticas de seguridad de la información deben establecer, en forma clara, las acciones a realizar para no poner en riesgo la información.

Las políticas deben ser creadas bajo un marco normativo que contenga una estructura de gobierno y un procedimiento de gestión de ciclo de vida de las políticas que asegure su correcta creación, autorización, difusión, cumplimiento y actualización.

Los procedimientos para garantizar la seguridad de la información son actividades que, en su conjunto, conforman un proceso sistemático de gestión de seguridad de la información. Generalmente los procesos de gestión de la seguridad de la información son implementados con apoyo de guías, estándares o mejores prácticas reconocidas a nivel internacional.

Los controles son mecanismos de seguridad que se implementan para mitigar los riesgos y pueden ser administrativos, de procedimiento o tecnológicos.

Cuando la información a proteger se trata de datos personales, entonces el deber de seguridad refiere a la obligación de implementar y mantener mecanismos de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.

En este sentido, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[590] en su artículo 19 establece lo siguiente:

> Artículo 19. Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado

590 DOF. (2010, julio). "Ley Federal de Protección de Datos Personales en Posesión de los Particulares". *Diario Oficial de la Federación*, Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

> Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

La LFPDPPP establece que el responsable del tratamiento de datos personales tiene la obligación de implementar mecanismos de seguridad para proteger los datos y cumplir con el deber de seguridad. Además, se obliga al responsable que las medidas de seguridad sean equiparables a las utilizadas en la protección de los demás tipos de información.

La identificación y selección de las medidas de seguridad se llevará a cabo mediante un proceso formal de análisis de riesgo.

Aun cuando se implementen medidas de seguridad para proteger los datos personales, pueden presentarse vulneraciones de seguridad afectando directamente al titular de los datos, en este sentido, el artículo 20 de la LFPDPPP contempla lo siguiente:

> Artículo 20. Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

El responsable debe implementar un proceso de detección de vulneraciones a las medidas de seguridad, de tal forma que permita reaccionar lo más pronto posible, minimizando de esta manera el impacto sobre el titular de los datos.

Asimismo, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[591] establece en sus artículos 50 y 52 las obligaciones sobre el deber de seguridad para los encargados que realizan tratamiento de datos personales a nombre del responsable. Particularmente el artículo 52 especifica:

> Artículo 52. Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o clausulas generales de contratación, solo podrá utilizar aquellos servicios en los que el proveedor:
>
> 1. Cumpla, al menos, con lo siguiente:
>
> III. Implementar las medidas de seguridad conforme a la LFPDPPP, el RLFPDPPP y las demás disposiciones aplicables.

Cuando los datos personales se almacenen o se traten en la nube, el proveedor deberá implementar las medidas de seguridad correspondientes que permitan cumplir con el deber de seguridad.

Para las dependencias del gobierno federal, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO),[592] a través de sus artículos 31 y 33, fija los lineamientos para garantizar el cumplimiento del deber de seguridad. El artículo 31 establece la obligación de implementar medidas de seguridad que protejan los datos personales contra acceso no autorizado o daño a los mismos. Por otro lado, el artículo 33 enlista una serie de acciones para poder implementar y mantener las medidas de seguridad requeridas para la protección de datos personales.

591 DOF. (2011, diciembre). "Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares". *Diario Oficial de la Federación*. Artículo 61. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

592 DOF. (2017, enero). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados". *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

El deber de seguridad se cumple con la implementación y mantenimiento de medidas de seguridad en todas las fases del ciclo de vida en donde se traten los datos personales y exista algún riesgo de vulneración hacia los mismos.

La implementación de las medidas de seguridad se realiza a través de un proceso de gestión sistemático que abarca como mínimo las siguientes tareas:

a) crear políticas de seguridad internas
b) identificar el tipo de datos personales tratados en la organización
c) identificar las personas y sistemas que hacen tratamiento de los datos personales
d) realizar un análisis de riesgo
e) efectuar un análisis de brecha
f) identificar las medidas de seguridad y hacer un plan de implementación
g) ejecutar programas de capacitación según el rol y nivel de responsabilidad del personal

Las políticas de seguridad se crean bajo el marco normativo de la organización, alineadas a los requerimientos legales de carácter nacional o internacional.

La identificación del tipo de datos personales manejados a lo largo del flujo de información en los procesos de la organización es importante porque, dependiendo de la sensibilidad de los datos, será el tipo de medida de seguridad implementado.

La identificación de las personas y sistemas que hacen tratamiento de los datos personales permite validar si los roles y permisos asignados a las personas son los adecuados para el correcto tratamiento de los datos personales. La identificación de los sistemas que tratan los datos, permite visualizar en que parte del ciclo de vida y la forma en que los datos son creados, almacenados, usados y eliminados.

El análisis de riesgo es un proceso que ayuda a identificar escenarios de riesgo de los datos personales, es decir, identificar todas las amenazas que pueden causar algún daño a los datos personales. Las amenazas son entidades o eventos que de manera accidental o intencional afectan la confidencialidad, integridad o disponibilidad de los datos personales. El siguiente paso en el proceso de análisis de riesgo consiste en identificar las vulnerabilidades existentes alrededor del tratamiento de los datos personales. Las vulnerabilidades pueden ser de origen tecnológico, de procedimiento o de gente. El nivel de exposición de las vulnerabilidades depende de la existencia o falta de mecanismos de seguridad actualmente implementados. Una vez identificados los componentes del riesgo, se procede a evaluar el riesgo asignando un valor cualitativo o cuantitativo al escenario de riesgo.

El resultado del proceso de análisis de riesgo es una lista evaluada y priorizada de escenarios de riesgo.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[593] desarrolló la MARBAA[594] que consiste en una metodología de análisis de riesgo enfocada a la protección de datos personales. Para evaluar el riesgo, la metodología contempla tres factores:

1) Beneficio. Valor que deriva del riesgo inherente de los datos personales o del nivel de sensibilidad y del volumen de titulares de las que se traten los datos. Este factor

593 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

594 INAI. (2015, junio). *Metodología de Análisis de Riesgo BAA*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

está fundamentado en el hecho de que entre más sensible sea el dato y la cantidad de datos personales manejados sea mayor, entonces es más atractivo a los atacantes.

2) Accesibilidad. Valor que está relacionado con el número de accesos potenciales a los datos. Factor que considera que entre más veces sean tratados los datos personales, mayor es el riesgo de ataque.

3) Anonimidad. Valor que toma en cuenta el entorno desde donde se acceden los datos personales. Los entornos considerados son: acceso físico, acceso desde la red interna de la organización, acceso desde la red inalámbrica, acceso desde redes de terceros y accesos desde internet. Este factor considera que entre mayor sea la anonimidad, es decir, la falta de capacidad de identificar a las personas que acceden los datos personales, mayor es el riesgo.

Una vez que se evalúan los tres factores anteriores, se realiza la evaluación del nivel de riesgo latente por cada tipo de dato personal tratado. El nivel de riesgo latente permite identificar las medidas de seguridad a implementar. Se identifican patrones de control que consisten en listas de controles perfectamente agrupados y que garantizan el cumplimiento del deber de seguridad.

Una vez identificadas las medidas de seguridad, se procede a realizar un plan de implementación para cada uno de los controles identificados. Para la especificación detallada de los controles, así como la descripción de la guía de implementación, el responsable se apoya en estándares internacionales como el ISO/IEC 27002[595] o el NIST 800-5.[596]

El proceso de implementación de medidas se seguridad para proteger los datos personales y cumplir con el deber de seguridad debe estar soportado por un programa de capacitación de diferentes niveles dirigido a toda persona según su rol y responsabilidad en el tratamiento de datos personales a lo largo de su ciclo de vida.

Delegado de protección de datos

Daniel Antonio Pérez Cirera Santacruz

El delegado de protección de datos o *Data Protection Officer* (DPD o DPO por sus siglas en inglés) es el profesional designado por la parte responsable y/o encargado del tratamiento para ocuparse de la aplicación y cumplimiento de la normatividad de protección de datos personales y privacidad en el interior de la organización.

1. La figura del DPD en la normatividad de protección de datos personales

La figura del DPD no se encuentra expresamente reconocida ni ordenada en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) pero el artículo 30 de la citada normada da pie a que esta figura sea instituida en la organización al disponer que todo responsable deberá designar a una persona, o departamento de datos personales, que dé trámite a las solicitudes ARCO y fomente la protección de datos personales al interior de la organización.[597]

595 ISO. (2013). *ISO/IEC 27002, Information technology —Security techniques— Code of practice for information security controls.* ISO/IEC.

596 Joint Task Force Transformation Initiative. (2013, 4 de abril). *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST

597 "Artículo 30.- Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente Ley. Asimismo, fomentará la protección de datos personales al interior de la organización".

Por otro lado, en el ámbito público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) en el penúltimo párrafo de su artículo 85 indica que se podrá designar a un oficial de protección de datos personales especializado en la materia para que realice las atribuciones mencionadas en dicho artículo y forme parte de la unidad de transparencia cuando los responsables lleven a cabo tratamientos intensivos de datos personales.[598]

En relación con lo anterior, los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) indican, en su artículo 121, además de lo señalado en el artículo 85 de la LGPDPPSO que, la persona designada como oficial de protección de datos (OPD o DPD) deberá contar con la jerarquía o posición dentro de la organización del responsable que le permita implementar políticas transversales en esta materia. Así se detalla que el DPD deberá ser designado en atención a sus conocimientos, cualidades profesionales, experiencia en la materia, y en su caso, a las certificaciones con que cuente en materia de protección de datos personales.

Por su parte, los Estándares de Protección de Datos para los Estados Iberoamericanos (Estándares Iberoamericanos) en su artículo 39 hacen referencia a la figura del DPD y precisan que el responsable deberá designarlo en los casos que establezca la legislación nacional y cuando concurran las circunstancias específicas señaladas en los incisos a, b y c del referido artículo.[599]

No obstante, es en el ámbito europeo donde se ha desarrollado con mayor claridad esta figura. Al respecto, el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) indica, en el apartado 1 de su artículo 37, que los responsables y encargados del tratamiento tendrán la obligación de designar a un DPD siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales[600] del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala[601] de categorías especiales de datos personales con arreglo al artículo 9[602] y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

598 [...]
Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia.
[...]

599 "39.1. El responsable designará a un oficial de protección de datos personales o figura equivalente en los casos que establezca la legislación nacional de los Estados Iberoamericanos aplicable en la materia y cuando:
sea una autoridad pública.
Lleve a cabo tratamientos de datos personales que tengan por objeto una observación habitual y sistemática de la conducta del titular.
Realice tratamientos de datos personales donde sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, considerando, entre otros factores y de manera enunciativa más no limitativa, las categorías de datos personales tratados, en especial cuando se trate de datos sensibles; las transferencias que se efectúen; el número de titulares; el alcance del tratamiento; las tecnologías de información utilizadas o las finalidades de éstos".

600 El Grupo de trabajo del Artículo 29 nota que una actividad no debe excluirse de las actividades principales las que sean indisociables de la misma, tal como que el tratamiento de datos sensibles es indisociable de la actividad principal de un hospital: prestar atención sanitaria.

601 El grupo de trabajo del artículo 29 recomienda considerar los siguientes factores para determinar si un tratamiento se hace a gran escala: el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente; el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento; la duración, o permanencia, de la actividad de tratamiento de datos, y el alcance geográfico de la actividad de tratamiento.

602 De acuerdo con el artículo 9 del GDPR, se consideran datos de categorías especiales "los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física".

Asimismo, señala el RGPD que el Derecho de la Unión Europea (UE) o el derecho de algún estado de la UE podrán volver obligatorio la designación de DPD para casos diversos a los anteriores.[603]

El RGPD prevé, además, que podrá designarse un DPD único en los siguientes casos:

- Se trate de grupos empresariales (siempre y cuando sea fácilmente accesible desde cada establecimiento).
- Se trate de varias de estas autoridades u organismos, cuando el responsable o encargado sea una autoridad u organismo público (teniendo en cuenta la estructura organizativa y tamaño).[604]
- Se trate de asociaciones y otros organismos que representen a responsables o encargados en supuestos distintos a los señalados en el apartado 1 del artículo 37, citado anteriormente.

Al determinar si para cierta organización es obligatorio designar a un DPD, el Grupo de Trabajo del Artículo 29 recomienda a responsables y encargados, en las directrices sobre los delegados de protección de datos (DPD) (Directrices),[605] realizar y documentar un análisis interno. Con esta documentación podrá demostrarse que se tomaron en cuenta los factores adecuados en la decisión, exigencia del principio de rendición de cuentas. Dichas Directrices también notan que no necesariamente porque un responsable esté en un supuesto que lo obliguen a designar un DPD, su encargado estará en la misma situación. Por lo tanto, habrá que evaluar caso por caso para ver si el encargado cae en el mismo supuesto.[606]

Por otro lado, en los casos en los que no sea obligatorio, el RGPD hace potestativo que el responsable o el encargado del tratamiento, o las asociaciones y otros organismos que representen a categorías de responsables o encargados designen un DPD.[607] Sin embargo, al designar un DPD, el responsable y/o encargado deberá seguir todos los requisitos establecidos en el RGPD.

2. Perfil del DPD

Para designar a un DPD deberá atenderse a sus cualidades profesionales y, en particular, a sus conocimientos especializados en la materia y capacidades para desempeñar sus funciones.[608] El nivel de conocimientos necesario dependerá de la cantidad, frecuencia y complejidad de los tratamientos realizados por la organización y las cualidades profesionales refieren a que el individuo tenga un conocimiento de la normatividad aplicable y de la práctica de la materia.

Para cumplir con sus funciones, el DPD[609] deberá ser capaz de:

a) recabar información para determinar las actividades de tratamiento;

603 De acuerdo con el apartado 4 del artículo 37 del GDPR.

604 De acuerdo con el artículo 37, apartados 2 y 3 del GDPR.

605 Adoptadas el 13 de diciembre de 2016 por el Grupo de Trabajo del Artículo 29, revisadas por última vez y adoptadas el 5 de abril de 2017.

606 Sin embargo, las Directrices como buena recomendable del encargado designar a un DPO cuando el responsable lo haga.

607 También, de acuerdo con el apartado 4 del artículo 37 del GDPR.

608 De acuerdo con el artículo 37, apartado 5 del GDPR.

609 AEPD, Esquema de Certificación de Delegados de Protección de Datos, disponible en: https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf

b) analizar y comprobar la conformidad de las actividades de tratamiento;

c) informar, asesorar y emitir recomendaciones al responsable o el encargado del tratamiento;

d) recabar información para supervisar el registro de las operaciones de tratamiento;

e) asesorar en la aplicación del principio de la protección de datos por diseño y por defecto;

f) asesorar sobre:

1. si se debe llevar a cabo o no una evaluación de impacto de la protección de datos, qué metodología debe seguirse al efectuar una evaluación de impacto de la protección de datos, si se debe llevar a cabo la evaluación de impacto de la protección de datos con recursos propios o con contratación externa, qué salvaguardas (incluidas medidas técnicas y organizativas) aplicar para mitigar cualquier riesgo para los derechos e intereses de los afectados en el caso de alguna vulneración.

2. si se ha llevado a cabo correctamente o no la evaluación de impacto de la protección de datos.

3. si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardas aplicar) son conformes con la normatividad.

g) priorizar sus actividades y centrar sus esfuerzos en aquellas cuestiones que presenten mayores riesgos relacionados con la protección de datos;

h) asesorar al responsable del tratamiento sobre:

1. qué metodología emplear al llevar a cabo una evaluación de impacto de la protección de datos, qué áreas deben someterse a capacitaciones y auditoría de protección de datos interna o externa.

2. qué actividades de formación internas proporcionar al personal o los directores responsables de las actividades de tratamiento de datos y a qué operaciones de tratamiento dedicar más tiempo y recursos.

En términos de los Lineamientos Generales, el DPD deberá ser designado en atención a sus conocimientos, cualidades profesionales, experiencia en la materia, y en su caso, a las certificaciones con que cuente en materia de protección de datos personales.

3. Funciones del DPD

En relación con la designación del DPD, la normatividad del sector privado indica que la persona designada por el responsable tendrá a su cargo la atención de los derechos de los titulares y fomentará la protección de datos personales en la organización.

De la mano con lo anterior, las Recomendaciones para la Designación de la Persona o Departamento de Datos Personales (Recomendaciones) publicadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[610] indican que la persona designada podrá desarrollar funciones adicionales para dar cumplimiento a la normatividad de la materia (ver la definición de departamento de datos personales).

Por otra parte, la LGPDPPSO indica, en su artículo 85, que en el caso de que se designe un DPD, las funciones originalmente atribuidas a la Unidad de Transparencia serán realizadas por el DPD y consistirán en:

610 INAI. (2016, agosto). *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.* Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/RecomendacionesDesignar.pdf

- Auxiliar y orientar al titular que lo requiera en relación al ejercicio del derecho a la protección de datos personales.
- Gestionar las solicitudes para el ejercicio de los derechos ARCO.
- Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados.
- Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, de acuerdo con las normativas aplicables.
- Proponer al comité de transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO.
- Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.

Además, los Lineamientos Generales señalan, en su artículo 122, que el DPD tendrá a su cargo las siguientes funciones:

- Asesorar al Comité de Transparencia respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.
- Proponer al comité de transparencia políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la LGPDPPSO y los Lineamientos Generales.
- Implementar políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la LGPDPPSO y los Lineamientos Generales, previa autorización del comité de transparencia.
- Asesorar permanentemente a las áreas adscritas al responsable en materia de protección de datos personales.
- Las demás que determine el responsable y la normatividad que resulte aplicable.

Los Estándares Iberoamericanos, señalan también como funciones del DPD las siguientes:

- Asesorar al responsable respecto a los temas que sean sometidos a su consideración en materia de protección de datos personales.
- Coordinar, al interior de la organización del responsable, las políticas, programas, acciones y demás actividades que correspondan para el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.
- Supervisar, al interior de la organización del responsable, el cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

Finalmente, de acuerdo con el RGPD,[611] el DPD tiene al menos ciertas funciones que citamos a continuación:

> a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
>
> b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la

611 Artículo 39, apartado 1.

asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;[612]

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;[613]

d) cooperar con la autoridad de control y

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El DPD tiene, además, la obligación de mantener en secreto o confidencialidad el desempeño de sus funciones. Asimismo, cabe agregar que el DPD puede desempeñar otras funciones siempre y cuando no den lugar a conflicto de interés.[614]

4. Responsabilidad del DPD

De conformidad con la normatividad aplicable, el DPD no es responsable ante el incumplimiento de la normatividad de datos personales. Es decir, la responsabilidad concreta recae en el responsable o el encargado, según sea el caso. De ahí la importancia de que la designación del DPD deba cubrir altos estándares de probidad y profesionalismo.

Delito en materia de protección de datos personales

Olivia Andrea Mendoza Enríquez

Podemos dar una aproximación conceptual al término delito en materia de protección de datos personales, afirmando que es aquella acción llevada a cabo y contraria a lo establecido por los ordenamientos legales en la materia —que contraviene a la dignidad de la persona— específicamente respecto del tratamiento indebido de información de carácter personal y cuya garantía prevé una sanción que puede ser agravada, respecto de condicionantes como las veces que se ha cometido la falta, la gravedad y trascendencia de la falta o el tratamiento indebido de datos personales sensibles.

El marco legal en materia de protección de datos personales en México está dividido entre disposiciones aplicables a responsables del tratamiento de datos personales en el sector público y aquellas aplicables a responsables del tratamiento de datos personales en el sector privado.

En este sentido, la legislación específica que invoca el término de delitos en materia de tratamiento indebido de datos personales es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual es de orden público y de obser-

612 Las directrices del Grupo de Trabajo del Artículo 29 establecen que el DPO puede, en el cumplimiento de esta obligación, recabar información para determinar las actividades de tratamiento, analizar y comprobar la conformidad con la normativa de las actividades de tratamiento e informar, asesorar y emitir recomendaciones al responsable o al encargado del tratamiento.

613 El Grupo de Trabajo del Artículo 29, en este respecto, recomienda que el DPO asesore en: si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos, qué metodología debe seguirse al llevar a cabo una evaluación de impacto, si debe realizarse la evaluación de impacto en la propia organización o subcontratarse, qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar cualquier riesgo para los derechos e intereses de los interesados, si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD.

614 De acuerdo con el artículo 38 apartados 5 y 6 del GDPR.

vancia general en toda la República y cuyo objeto es la protección de los datos personales en posesión de los particulares con la finalidad de regular su tratamiento legítimo, controlado e informado a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.[615]

Los sujetos regulados por esta Ley son todas aquellas personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal y sin fines de divulgación o utilización comercial.[616]

A efecto de normar aquellos delitos derivados del tratamiento indebido de datos personales, se dispuso el capítulo XI denominado: "De los delitos en materia de Tratamiento Indebido de Datos Personales" de la LFPDPPP, el cual establece las siguientes sanciones:

a) Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.[617] En este sentido, es importante hacer la precisión que tanto el responsable,[618] como el encargado,[619] pueden llevar a cabo el tratamiento de datos personales, por lo que existe una corresponsabilidad para el debido tratamiento de los mismos.

b) Se establece la sanción de prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.[620]

Existe una agravante de la pena: esta se duplica cundo se trata de datos personales sensibles.[621] Para tal efecto, se debe decir que el concepto de dato personal sensible, no es un concepto acabado, ya que dependerá del contexto en el que información personal pueda ser considerada como dato personal de carácter general, o en su caso, dato personal sensible. No obstante, la legislación en materia de protección de datos personales para el sector privado define como dato personal sensible a aquellos datos personales que afecten a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave. En particular, se consideran sensibles aquellos datos que puedan revelar aspectos como origen racial o étnico, estado de salud pasado, presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual.[622]

615 Artículo 1 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Fecha de consulta: 13 de agosto de 2018.

616 Artículo 2 de la LFPDPPP. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Fecha de consulta: 13 de agosto de 2018.

617 Artículo 67 de la LFPDPPP. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Fecha de consulta: 20 de agosto de 2018.

618 En términos del artículo 3, fracción XIV de la LFPDPPP, el responsable es aquella persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

619 En términos del artículo 3, fracción IX de la LFPDPPP, el encargado es la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

620 Artículo 68 de la LFPDPPP.

621 Artículo 69 LFPDPPP.

622 Artículo 3, fracción VI de la LFPDPPP.

Por otro lado, si bien la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[623] (LGPDPPSO) no reconoce expresamente un apartado para los delitos derivados del tratamiento indebido de datos personales, sí contiene disposiciones aplicables al caso:

a) Los órganos garantes estatales o el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) podrán imponer dentro del catálogo de medidas de apremio para asegurar el cumplimiento de sus determinaciones: Amonestación pública, o multa equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización (UMA).[624] En caso de que el incumplimiento de las determinaciones de los órganos garantes estatales o del propio INAI implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163[625] de LFPDPPP, deberán denunciar los hechos ante la autoridad competente.[626]

b) En caso de que el incumplimiento de las determinaciones de los órganos garantes estatales o del INAI implique la presunta comisión de un delito, el organismo garante respectivo deberá denunciar los hechos ante la autoridad competente.

---

623 De acuerdo con el artículo 1 de la LGPDPPSO, este instrumento es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6, base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados. Sus disposiciones son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal y tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.
Es importante señalar que son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. En el caso de los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

624 Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

625 "Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la LGPDPPSO, las siguientes:
I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.
II. Incumplir los plazos de atención previstos en la Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.
III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.
IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la Ley.
V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia.
VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción solo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.
VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la Ley.
VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la Ley.
IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la Ley.
X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la Ley.
XI. Obstruir los actos de verificación de la autoridad.
XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la Ley;
XIII. No acatar las resoluciones emitidas por el Instituto y los organismos garantes.
XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.
Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.
En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso sanción, corresponderán a la autoridad electoral competente".

626 Artículo 153 de la LGPDPPSO.

El desarrollo tecnológico ha permitido que se manifiesten nuevos medios de comisión de delitos, particularmente a partir de las tecnologías de la información y comunicación (TIC). Algunas de las denominaciones que se han dado a este tipo de delitos son los delitos informáticos, tecnológicos o cometidos a través de las TIC.

En este sentido, es importante decir que el Código Penal Federal (CPF) no reconoce la tipificación de delitos informáticos bajo esa denominación, partiendo de que la mayoría de los delitos cometidos a través de las tecnologías ya son sancionados en el orden tradicional, pero que tienen como medio comisivo, nuevos instrumentos derivados del desarrollo científico. Sin embargo, en su título noveno denominado "Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática", particularmente capítulo II del acceso a sistemas y equipos de informática, sí se prevén sanciones a las conductas relacionadas a modificar, destruir o provocar pérdida de información, —sin autorización alguna— contenida en sistemas o equipos de informática tanto privados como del Estado, protegidos por algún mecanismo se seguridad.

Aunado a lo anterior, dicho ordenamiento también sanciona al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad y a quien sin autorización, conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad y en caso de que el responsable sea o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, la destitución e inhabilitación de cuatro a 10 años, para desempeñarse en otro empleo, puesto, cargo o comisión pública. En el mismo tenor, las sanciones se duplicarán cuando la conducta obstruya, entorpezca, obstaculice, limite o imposibilite la procuración o impartición de justicia, o recaiga sobre los registros relacionados con un procedimiento penal resguardados por las autoridades competentes.

El CPF también sanciona a quien, estando autorizado para acceder a sistemas y equipos de informática del Estado, modifique indebidamente, destruya o provoque pérdida de información contenida en éstos. En este sentido, también se sanciona a quien, autorizado para acceder a sistemas y equipos de informática del Estado, copie de manera indebida información. Ambas sanciones aplican a información contenida en sistemas y equipos de informática en materia de seguridad pública y de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, con la agravante en la pena, respecto de los responsables que funjan o hayan fungido como servidores públicos de una institución de seguridad pública, o de las instituciones que conforman el sistema financiero.

Es importante destacar que las sanciones derivadas de las conductas descritas en líneas anteriores aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

En el mismo tenor, la lógica del legislador en materia penal federal invoca al catálogo de delitos tradicionales reconocidos en el ordenamiento jurídico como mecanismos suficientes para sancionar conductas contrarias a derecho y cometidas a través de medios electrónicos. Sin embargo, la necesidad de tipificar nuevos delitos surge especialmente con figuras como la usurpación, robo y suplantación de identidad cometidos a través de nuevas tecnologías.

En este rubro, en septiembre de 2017 fue presentada una iniciativa que adiciona el artículo 430 al CPF en materia de usurpación para tipificar la usurpación de identidad como un delito federal y sancionar a quienes usurpen, asuman, transfieran, utilicen, se apoderen, suplanten

o se apropien de la identidad de otra persona sin autorización a través de medios informáticos y castigarlos con penas de uno a seis años de prisión y de 400 a 600 días de multa. [627]

Dicho lo anterior, a nivel federal encontramos tipificación de delitos que, como consecuencia primaria o secundaria salvaguardan la vida privada de las personas, tales como la tipificación de la violación de correspondencia, la revelación de secretos, el acceso ilícito a sistemas y equipos de informática, el ejercicio ilícito de servicio público, la falsificación de documentos en general, el abuso de confianza y el fraude. En este sentido, podemos decir que, si bien hay delitos que no tienen como objetivo principal salvaguardar la vida privada de las personas, su alcance obliga a tratar de manera lícita la información de carácter personal.

Departamento de protección de datos personales

Daniel Antonio Pérez Cirera Santacruz

La expresión "departamento de protección de datos personales" (DDP) hace referencia a la instancia, unidad o grupo de personas dentro de una organización de carácter privado que tiene a su cargo las obligaciones de dar trámite a las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO)[628] y fomentar la protección de datos personales al interior de la organización para evitar una posible vulneración o uso inadecuado de los mismos.[629]

La figura del DDP tiene su sustento normativo en el artículo 30 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que dispone la obligación de que todo responsable del tratamiento de datos designe una persona o departamento de datos personales.

> Artículo 30. Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente Ley. Asimismo, fomentará la protección de datos personales al interior de la organización.

La designación de un DDP debe realizarse considerando las capacidades materiales y humanas de la organización para dar cumplimiento a esta obligación. En particular, es relevante considerar el tipo y cantidad de datos personales que trata, la frecuencia, naturaleza e intensidad del tratamiento, el número potencial de solicitudes de titulares de datos personales que podrá recibir y el valor (o falta de valor) que tengan los datos personales para la organización.

De este modo, cuando las capacidades de la organización le permitan asignar mayores recursos humanos y económicos para atender las tareas previstas en la normatividad, deberá preferirse la constitución formal de un DDP que tenga a su cargo dar cumplimiento, entre otras, a las obligaciones previstas en el artículo 30 de la LFPDPPP.

627 Información consultada en la página del Senado de México. Disponible en: http://comunicacion.senado.gob.mx/index.php/multimedia/infografias/infografias-2/38896-resumen-de-la-sesion-del-5-de-septiembre.html

628 Estos derechos incluyen los derechos de acceso, rectificación, cancelación y oposición (conocidos como derechos ARCO), el derecho a la revocación del consentimiento y el derecho de limitación de uso y/o divulgación del tratamiento. Para más información sobre ellos, consulte el desarrollo de sus definiciones en esta obra.

629 Cabe señalar que el transitorio tercero de la LFPDPPP dio un plazo de un año después de la entrada en vigor de dicha Ley para que los responsables designaran a la persona o departamento de datos personales. Dado que la LFPDPPP entró en vigor el 6 de julio de 2010, esto significa que dicha obligación existe desde el 6 de julio de 2011. Cabe mencionar la posibilidad de ejercer los derechos ARCO y los procedimientos subsecuentes se prorrogó hasta el 6 de enero de 2012.

1. Funciones del DDP

En términos del citado artículo 30 de la LFPDPPP, la persona o departamento de datos personales tiene las siguientes obligaciones específicas:

- dar trámite a las solicitudes de ejercicio de los derechos ARCO que formulen los titulares de datos personales y
- fomentar la protección de datos personales al interior de la organización.

Respecto de las funciones del DDP, las Recomendaciones para la Designación de la Persona o Departamento de Datos Personales (Recomendaciones) publicadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI),[630] dada la naturaleza transversal de la protección de datos personales en las organizaciones, consisten en realizar funciones adicionales que puede desarrollar el DDP con el objetivo de garantizar que el responsable cumpla cabalmente con sus obligaciones y compromisos, así como para poder atender a las mejores prácticas y estándares en la materia.

En relación con la atención de las solicitudes de los derechos ARCO, las Recomendaciones proponen que el DDP tenga a su cargo también la ejecución de las siguientes funciones:

- Establecer y administrar los procedimientos para la recepción, tramitación, seguimiento y atención oportuna de las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como para la atención de quejas o solicitudes presentadas por los titulares relacionados con las políticas y/o prácticas de protección de datos personales desarrolladas por la organización.
- Monitorear los avances o cambios legislativos en materia de privacidad y protección de datos personales que pudieran impactar en los ejes rectores y acciones desarrolladas en este tema al interior de la organización, haciendo las adecuaciones necesarias.

Por otro lado, en relación la promoción del derecho a la protección de datos personales en el interior de la organización, se recomienda[631] también la concreción de estas funciones como las atribuciones y facultades del DDP:

- Diseñar y ejecutar una política y/o prácticas de protección de datos personales, o que adecuar y mejorar las ya existentes, desarrollando un mecanismo para evaluar su eficacia y eficiencia, y verificando que las mismas cumplan la normatividad aplicable.
- Alinear la política y/o prácticas a los procesos internos de la organización que demanden o aprovechen información personal.
- Monitorear y evaluar los procesos y prácticas internas de la organización vinculados con la obtención, uso, explotación, conservación, aprovechamiento, cancelación y transferencia de datos personales.
- Colaborar y coordinar acciones con otras áreas de la organización para asegurar el debido cumplimiento de la política y/o prácticas de privacidad en sus procesos internos, formatos, avisos, recursos y gestiones que se lleven a cabo.
- Difundir y comunicar la política y/o prácticas de protección de datos personales implementadas al interior de la organización, así como capacitar a todo el personal al respecto.
- Fomentar una cultura de protección de datos personales orientada a elevar el nivel de concienciación del personal y terceros involucrados en el tratamiento de datos personales.

630 INAI. (2016. Agosto). *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.* Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/RecomendacionesDesignar.pdf

631 INAI. (2016. Agosto). *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.*

- Monitorear el cumplimiento de la política y/o prácticas de protección de datos personales de las sociedades subsidiarias o afiliadas bajo el control de común de la organización o cualquier sociedad del mismo grupo del responsable que opere y le sean aplicables estas prácticas.
- Identificar e implementar mejores prácticas.
- Promover la adopción de esquemas de autorregulación.
- Diseñar e implementar un plan de respuesta en caso de vulneración de datos personales, así como entrenar a la organización en el mismo, y proceder a su ejecución en el caso de que ocurra alguna vulneración.
- Ser el representante de la organización en materia de protección de datos personales ante otros actores.

La ejecución de las funciones referidas puede ser desarrollada en distintos niveles organizativos en función de las características de la entidad responsable del tratamiento.

2. Perfil de las personas que integren el DDP y posición del DDP

Las personas que integren el DDP deben contar con determinadas cualificaciones que les permitan llevar a buen puerto la gestión de sus obligaciones en materia de privacidad y protección de datos personales. De manera general, el perfil de los integrantes del DDP debe considerar lo siguiente:

- Experiencia en materia de protección de datos personales. Las personas que integren el DDP deben contar, preferentemente, con experiencia en materia de protección de datos personales o bien, realizar funciones afines al tema como las que realizan las áreas de *compliance* o de auditoría en la organización.[632]
- Jerarquía o posición dentro de la organización. El DDP debe contar con la adecuada jerarquía o posición dentro de la organización que le permita implementar políticas transversales en materia de protección de datos personales dentro de todos los niveles de la organización.[633]
- Recursos suficientes. El DDP de datos personales debe contar con los recursos materiales, técnicos y humanos necesarios para el ejercicio de sus funciones y acciones, a efecto de dar cumplimiento a las disposiciones previstas en la normatividad.[634]
- Contar con conocimiento en la materia. Las personas que integren el DDP deben de contar conocimientos sobre regulación y temas de protección de datos personales y seguridad de la información.[635]
- Visión y liderazgo. Con la finalidad de hacer cumplir los proyectos que entrañen la protección de datos personales, las personas que integren el DDP deben contar con una amplia capacidad de liderazgo y visión para implementar la política de privacidad a lo largo de la organización.
- Amplio conocimiento de los procesos internos y modelos de negocio. A fin de poder ejercer sus funciones de manera adecuada, debe de contar con un amplio conocimiento de todos los procesos internos de la organización, así como de los modelos

632 INAI. (2016. Agosto). *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.*

633 INAI. (2016. Agosto). *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.*

634 INAI. (2016. Agosto). *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.*

635 INAI. (2016. Agosto). *Recomendaciones para la Designación de la Persona o Departamento de Datos Personales.*

de negocio y finalidades y tratamiento que le brindaran a los datos personales.

- Habilidades de organización y comunicación. Los integrantes del DDP deben contar con habilidades gerenciales que les permitan dirigir los esfuerzos para concretar los proyectos necesarios para dar cumplimiento a la normatividad y difundir los logros en la organización.

Debe destacarse además que, aunque el responsable no está obligado a registrar a la persona o DPD designada ante el INAI, en la práctica es importante que se realice una constitución formal del departamento a través del cual se documente, formalmente, el proceso de designación correspondiente y las atribuciones concretas de cada uno de sus integrantes, así como sus nombres, cargos y funciones en la organización.

Finalmente, pese a que no se trata de un elemento informativo a incluir en el aviso de privacidad, como buena práctica, el INAI recomienda que el responsable publicite los datos de contacto del DDP en el aviso de privacidad o en algún otro medio de conocimiento adecuado para los titulares.

Derecho a la imagen

Kiyoshi Tsuru Alberú y
Patricio González Granados

Para explicar el derecho a la imagen y su ejercicio, es importante entender que es considerado —tanto por la doctrina como por la legislación mexicana— como un derecho de la personalidad, inherente a la dignidad de la persona, en cuanto emerge de la propia naturaleza del ser humano y que, excepcionalmente, se manifiesta en las personas morales, según el derecho de que se trate.

Los derechos de la personalidad son inherentes a las personas, en cuanto que éstas no pueden despojarse de ellos (en su totalidad) y permiten el desarrollo de las capacidades personales.[636] Al considerar el derecho a la imagen como un derecho de la personalidad, la jurisprudencia mexicana establece que una persona puede disponer su propia imagen y autorizar su uso en una fotografía, pero esa autorización queda limitada a una obra fotográfica determinada y no podría renunciarse a este derecho de forma permanente.[637]

Algunas posturas[638] señalan que aun cuando el derecho a la imagen es un derecho de la personalidad y se vincula estrechamente con otros derechos como el honor, la fama y la privacidad, el derecho a la imagen es independiente. Concordamos con esta afirmación de autonomía del derecho a la imagen, pues con un mismo acto se pueden vulnerar todos los derechos mencionados. Sin embargo, puede vulnerarse solamente el derecho a la imagen de una persona, sin causar perjuicio a su honor y fama.

636 Mendoza, L. (2014). *La acción civil del daño moral.* México. UNAM, Instituto de Investigaciones Jurídicas. serie Estudios Jurídicos, núm. 235, p. 29. Disponible en: *https://archivos.juridicas.unam.mx/www/bjv/libros/8/3636/5.pdf.*

637 "El Pleno de la Suprema Corte de Justicia de la Nación, en las tesis aisladas P. LXV/2009 y P. LXVII/2009 sostuvo que el derecho a la propia imagen es personalísimo y faculta a su titular a decidir en forma libre sobre la manera en que elige mostrarse frente a los demás y, por consiguiente, se configura, junto con otros también personalísimos (a la intimidad y a la identidad personal y sexual), como un derecho de defensa y garantía esencial para la condición humana". Tesis I.7o. A. 144. *Semanario Judicial de la Federación y su Gaceta*. Tomo IV, libro 38. Enero de 2017, p. 2513.

638 Flores, E. (2014). "Derecho a la imagen personal", en Ferrer Mac-Gregor, Eduardo et al. (coords.). *Diccionario de derecho procesal constitucional y convencional*. México. Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica. Núm. 692-693, p. 34. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3683/27.pdf

Para una mejor comprensión de la dimensión del derecho a la imagen debe tenerse en cuenta el significado común que se le atribuye al término "imagen" como figura, representación y apariencia de algo. En tanto que "imagen pública" significa el conjunto de rasgos que caracterizan ante la sociedad a una persona o entidad.[639]

Siguiendo esta concepción de imagen, la legislación de la Ciudad de México cuenta con una definición legal de "imagen personal" en el artículo 16 de Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen que la señala como: "La reproducción identificable de los rasgos físicos de una persona sobre cualquier soporte material" y paralelamente define el derecho a la imagen en el artículo 17 como: "La facultad para disponer de su apariencia autorizando, o no, la captación o difusión de la misma".

En tales condiciones, siempre que se aborde el derecho a la propia imagen, se deberá recurrir a la legislación local aplicable para poder delimitar el alcance y modulación en relación con el caso a estudiar.

1. Antecedentes históricos

Tradicionalmente, la protección a la imagen personal ha ido de la mano de otros derechos de la personalidad e, inclusive, derechos afines como los derechos de autor. Encontramos los primeros antecedentes legislativos precisamente en legislaciones en materia de derechos de autor en Alemania (1876), en Austria (1885) y en Bélgica en (1886). En estas disposiciones abordaban la necesidad de que existiera consentimiento de la persona retratada en una obra e incluso de sus causahabientes (leyes austriaca y belga) para la reproducción de la obra.[640]

Durante la segunda mitad del siglo XIX, la jurisprudencia francesa realizó avances importantes en la materia al reconocer, de manera implícita, en por lo menos siete resoluciones que van de 1855 a 1896, el derecho a la imagen. En estas resoluciones se abordaron cuestiones como la revocabilidad del consentimiento dado, la posibilidad de generar un contrato formal para la publicación de un retrato fotográfico, el derecho de la familia a oponerse a la difusión de la imagen de una persona fallecida, entre otras.[641]

Es relevante mencionar que la tendencia de protección del derecho a la imagen en relación con el derecho de reproducción de la obra o *copyright* se perpetuó en muchas legislaciones nacionales y tratados internacionales incluyendo la mexicana que analizaremos más adelante, sin embargo, Azurmendi señala que entre 1910 y 1948 el derecho a la imagen se reorientó en un nuevo marco jurídico, el de los derechos humanos,[642] al introducir nuevas concepciones doctrinales como el derecho de la personalidad y la necesidad de su reconocimiento y protección.[643]

639 El *Diccionario de la Lengua Española* es la obra lexicográfica de referencia de la Academia. Real Academia Española. Vigesimotercera edición, publicada en octubre de 2014. Disponible en: http://dle.rae.es/?id=KzwDY4y

640 Azurmendi, A. (1998). *El derecho a la propia imagen: su identidad y aproximación al derecho a la información.* España. Fundación Manuel Buendía-Universidad Iberoamericana, p. 52-54. Disponible en: https://books.google.com/books/about/El_Derecho_a_la_propia_imagen.html?id=YEigZ25K5JgC

641 Azurmendi, A. (1998). *El derecho a la propia imagen: su identidad y aproximación al derecho a la información.* España. Fundación Manuel Buendía-Universidad Iberoamericana, pp. 55-59.

642 Azurmendi, A. (1998). *El derecho a la propia imagen: su identidad y aproximación al derecho a la información.* España. Fundación Manuel Buendía-Universidad Iberoamericana, p. 50.

643 Azurmendi, A. (1998). *El derecho a la propia imagen: su identidad y aproximación al derecho a la información.* España. Fundación Manuel Buendía-Universidad Iberoamericana, p. 60-61.

2. *Análisis técnico*

El derecho a la propia imagen tiene dos facetas que se han desarrollado de manera doctrinal y jurisprudencialmente. La positiva consistente en la facultad personalísima de imprimir, difundir, publicar o distribuir la propia imagen, con o sin un provecho comercial, y la negativa radica en impedir la obtención, reproducción, difusión y distribución de la imagen por un tercero sin su consentimiento expreso o tácito.[644]

La incorporación de este derecho en nuestro sistema jurídico no es explícita, sino que se debe recurrir a los instrumentos internacionales a través de la regla de reconocimiento prevista en el artículo 133 de la Constitución Federal. En este sentido, el derecho a la propia imagen es protegido como un derecho fundamental relacionado con o como una faceta de la vida privada, la intimidad, el honor y la buena reputación de una persona en diversos instrumentos internacionales firmados y ratificados por México,[645] entre los cuales destacan el artículo 12 de la Declaración Universal de los Derechos Humanos, los artículos 17 y 19 del Pacto Internacional de Derechos Civiles y Políticos, los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos y el artículo 16 de la Convención sobre los Derechos del Niño.

La concreción y desarrollo de este derecho en los ordenamientos locales de nuestras entidades federativas no es uniforme, pues, por una parte, existen algunas que no lo regulan, mientras que otras tutelan el derecho a la imagen a través del resarcimiento en caso de daño moral por su vulneración y otros derechos de la personalidad.

Un ejemplo de esta regulación es la de la Ciudad de México, en la cual se encuentra vigente la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen. Esta ley busca garantizar los derechos a la vida privada, al honor y la propia imagen frente a cualquier daño que un acto ilícito pudiera causarle al patrimonio moral de una persona. La ley enuncia, en su artículo 24, como parte del patrimonio moral "el afecto del titular del patrimonio moral por otras personas, su estimación por determinados bienes, el derecho al secreto de su vida privada, así como el honor, el decoro, el prestigio, la buena reputación y la imagen de la persona misma".

Como lo hemos expuesto, esta ley define de manera autónoma los conceptos de imagen y al derecho a la imagen, pero vincula su protección con la de otros derechos de la personalidad como la buena reputación de una persona. En su artículo 20 establece que una autoridad judicial puede, a petición del interesado, disponer que cese el acto de abuso y se reparen los daños ocasionados cuando la imagen de una persona sea expuesta o publicada sin su consentimiento, pero señala "con perjuicio de la reputación de la persona", lo que condiciona la acción del interesado a la existencia de una afectación a la buena reputación.

Además, esta ley limita el ejercicio de este derecho al interés público (artículos 19, 21, 25 y 27), ya que permite la reproducción de la imagen de una persona sin su consentimiento

644 Flores, E. (2014). "Derecho a la imagen personal", en Ferrer Mac-Gregor, Eduardo et al. (coords.). *Diccionario de derecho procesal constitucional y convencional*. México. Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica. Núm. 692-693, p. 343. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3683/27.pdf

645 En este sentido, el séptimo Tribunal Colegiado en Materia Administrativa del Primer Circuito ha señalado que la Corte Interamericana de Derechos Humanos, al resolver el caso *Fontevecchia y D'Amico vs. Argentina* (fondo, reparaciones y costas), sentencia de 29 de noviembre de 2011, serie C, Núm. 238, "sostuvo que aunque el derecho a la propia imagen no se encuentra expresamente enunciado en el artículo 11 de la Convención Americana sobre Derechos Humanos, las imágenes o fotografías personales están incluidas dentro del ámbito de protección de la vida privada, y que la fotografía es una forma de expresión que recae en el ámbito de protección del artículo 13 de la propia convención". Tesis I.7o.A.144 A 10a. *Semanario Judicial de la Federación y su Gaceta*. Tomo IV, libro 38. Enero de 2017, p. 2513.

cuando esté justificada por la notoriedad o la función pública que desempeña esa persona y cuando predomine un interés público, histórico, científico o cultural, o bien, la reproducción se haga en relación con hechos, acontecimientos o ceremonias de interés público o que tengan lugar en público y sean de interés público.

También establece, en el artículo 21, como límites del derecho a la imagen, cuando se utiliza la caricatura de una persona de acuerdo con el uso social, o cuando una persona aparece como accesoria en la información gráfica sobre un suceso o acontecimiento público.

Esta regulación y límites al ejercicio del derecho a la imagen (supeditados al interés común) se asemejan mucho a la limitada regulación que existe en disposiciones legales federales, que se enfocan en materias como la protección de datos personales y los derechos de autor, pero que hacen breves referencias al citado derecho.

La jurisprudencia se ha manifestado en este sentido señalando que "constitucionalmente no existe prohibición para que una misma materia tenga una doble protección —en los ámbitos civil y del derecho de autor— y porque el derecho de autor no puede ser asimilado de forma únicamente enunciativa y limitativa, sino que, como cualquier otro derecho, no es absoluto, por lo que tiene su límite en los derechos de terceros, así como en el orden público y el interés social".[646]

Precisamente, la Ley Federal del Derecho de Autor establece que es necesario el consentimiento expreso de una persona para el uso o publicación su retrato (artículo 87) o para incluir su nombre, seudónimo o imagen como parte de una reserva de derechos (artículo 188, fracción 1, inciso e).[647] Inclusive, tratándose de retratos, la ley presume que existe consentimiento cuando a cambio de una remuneración una persona se deja retratar.[648]

En este sentido, no será necesario dicho consentimiento si la imagen de una persona es capturada en un lugar público y con fines informativos o periodísticos, o se tome el retrato de una persona que forme parte menor de un conjunto o bien, forme la parte minoritaria de la fotografía.

El artículo 3, fracción V, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) define a los "datos personales" como cualquier información concerniente a una persona física identificada o identificable. Lo anterior cobra relación con la imagen de una persona en el Reglamento del referido ordenamiento, en cuyo artículo 3 se establece que los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.

Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) define en los mismos términos a los datos personales en su artículo 3, fracción IX, es decir, como cualquier información concerniente a una persona física identificada o identificable, precisando que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.[649]

646 Tesis 2a. XXIV/2016. *Semanario Judicial de la Federación y su Gaceta*. Tomo II, libro 31. Junio de 2016, p. 1205.

647 Capítulo II de las Infracciones en Materia de Comercio."Artículo 231. Constituyen infracciones en materia de comercio las siguientes conductas cuando sean realizadas con fines de lucro directo o indirecto:[…]
II. Utilizar la imagen de una persona sin su autorización o la de sus causahabientes […]".

648 "Artículo 87[…] Cuando a cambio de una remuneración, una persona se dejare retratar, se presume que ha otorgado el consentimiento a que se refiere el párrafo anterior y no tendrá derecho a revocarlo, siempre que se utilice en los términos y para los fines pactados. No será necesario el consentimiento a que se refiere este artículo cuando se trate del retrato de una persona que forme parte menor de un conjunto o la fotografía sea tomada en un lugar público y con fines informativos o periodísticos".

649 INAI. (2018, marzo). *Guía para el Tratamiento de Datos Biométricos*. México. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf

Como se ha mencionado, la jurisprudencia en México reconoce el derecho a la propia imagen dentro de los derechos personalísimos y lo define como aquel derecho de decidir, en forma libre, sobre la manera en que elige mostrarse frente a los demás.[650]

De igual manera, el Quinto Tribunal Colegiado en Materia Civil del Primer Circuito de la SCJN ha señalado que los derechos concernientes al honor, a la intimidad y a la propia imagen constituyen derechos subjetivos del ser humano, en tanto que son inseparables de su titular y por ende, no pueden considerarse renunciables, transmisibles o prescriptibles, porque como se mencionó, son inherentes a la persona misma, es decir, son intrínsecos al sujeto quien no puede vivir sin ellos.[651]

En consecuencia, las disposiciones legales, criterios doctrinales y jurisprudenciales que hemos analizado reflejan dos problemáticas esenciales sobre el ejercicio y protección del derecho a la imagen. Por una parte, al considerar este derecho como un derecho humano correspondiente a la categoría de derechos de la personalidad, es intransmisible, al menos en su totalidad, porque ciertas disposiciones legales que ya hemos comentado permiten la explotación o contratación de determinadas proyecciones físicas o psíquicas, pero no de la universalidad de dichas cualidades.[652] Esta clasificación hace que resulte muy complicado empatar supuestos de causahabiencia[653] de derechos tales como la propiedad o posesión, con la causahabiencia[654] de ciertos aspectos del derecho a la imagen, como la facultad de consentir la divulgación de un retrato propio.

Estos cuestionamientos nos dirigen a la segunda problemática, la limitada regulación sobre derecho a la imagen, tanto a nivel nacional como en tratados internacionales y el hecho de que la regulación existente carece de una verdadera autonomía frente a otros derechos de la personalidad y derechos humanos en general.[655]

650 Tesis P. LXVII/2009. *Semanario Judicial de la Federación y su Gaceta*. Novena época, 165821. Tomo XXX. Diciembre de 2009, p.7.

651 Tesis I.5o.C.4 K. *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo 2, libro XXI. Junio de 2013, p. 1258.

652 Mendoza, L. (2014). *La acción civil del daño moral*. México. Universidad Nacional Autónoma de México- Instituto de Investigaciones Jurídicas, p. 29. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3636/5.pdf

653 Tribunales Colegiados de Circuito. Novena época. Semanario Judicial de la Federación y su Gaceta. Tomo III, abril de 1996, Pág. 356

654 La causahabiencia no es otra cosa más que la substitución del titular de un derecho por otro; pero implica que se trate del mismo derecho. Así, el titular de un derecho de propiedad es causante del comprador respecto del bien materia del contrato. Disponible en: http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/202/202612.pdf

655 Evans, D. (2015, mayo). "¿Se puede proteger la imagen igual que se protege una marca?". *Revista de la Organización Mundial de la Propiedad Intelectual*. Reino Unido. Disponible en: http://www.wipo.int/wipo_magazine/es/2015/02/article_0008.html

Derecho a la limitación del tratamiento

Isabel Davara Fernández de Marcos,[656]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El derecho a la limitación del tratamiento de los datos personales consiste en la facultad del titular de los datos de solicitar, ante el responsable del tratamiento, que a sus datos personales no se apliquen determinadas operaciones de tratamiento cuando se actualicen las condiciones establecidas por la normatividad aplicable en el entorno internacional.

El derecho a la limitación del tratamiento no encuentra sustento en la legislación nacional de protección de datos personales que se aplica para los sectores público y privado. Sin embargo, en el ámbito internacional este derecho ha sido desarrollado y regulado jurídicamente, por lo que es previsible que también se adopte en nuestro país en el futuro.

En primer lugar, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) tienen el mérito de contener previsiones específicas sobre el derecho a la limitación del tratamiento de los datos personales:

1. El artículo 31.1 del referido ordenamiento consigna que "el titular de los datos personales tiene derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable". Es decir, el titular puede exigir que sus datos sean conservados exclusivamente durante el lapso comprendido entre el ejercicio de los derechos de oposición y rectificación[657] hasta el momento en que el responsable haga efectivos los derechos referidos en tiempo y forma.
2. El artículo 31. 2 amplía el alcance de este derecho al precisar que el titular puede solicitar la limitación al tratamiento de sus datos personales cuando no sean necesarios para el responsable, pero los necesite para formular una reclamación. Con base en esta disposición se entiende que la prerrogativa del titular de limitar el tratamiento de sus datos personales también comprende aquellos datos que no sean necesarios para cumplir con las finalidades del tratamiento, pero sean requeridos para dar trámite a una reclamación ante la autoridad de control competente.

Por su parte, el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) incorpora este derecho como otra de sus novedades. Entre los puntos a destacar cabe señalar:

a) Define al derecho a la limitación del tratamiento como "el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro".[658] Bajo esta concepción, el derecho a la limitación del tratamiento se perfila como un derecho distinto de la figura del bloqueo de datos personales, subsistiendo ambas en la legislación como figuras diferenciadas de forma independiente y concreta.
b) El apartado 1 del artículo 18 del RGPD señala que el interesado (titular) tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla cualquiera de las condiciones siguientes:

656 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

657 Para mayor referencia, recomendamos la lectura de las definiciones relativas a los derechos de acceso, rectificación, cancelación y oposición que forman parte de este *Diccionario de Protección de Datos Personales*.

658 Artículo 4, apartado 3 del Reglamento General de Protección de Datos Personales.

I. el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

II. el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

III. el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones y

IV. el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1,[659] mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

c) Cuando el tratamiento de los datos se hubiera limitado conforme a lo dispuesto en la sección anterior, los datos involucrados solo podrán ser objeto de tratamiento, con excepción de su conservación:

I. con el consentimiento del interesado o

II. para la formulación, el ejercicio o la defensa de reclamaciones o

III. con miras a la protección de los derechos de otra persona física o jurídica o

IV. por razones de interés público importante de la Unión Europea o de un determinado Estado miembro.[660]

d) En el supuesto de que el titular de los datos (interesado en términos del RGDP) haya sido favorecido con la concesión del derecho de limitación al tratamiento, el responsable deberá informar al titular de los datos de forma previa a la práctica de la limitación del tratamiento.

e) Los métodos admisibles para la limitación del tratamiento de datos personales serán aquellos consistentes en:

I. trasladar temporalmente los datos seleccionados a otro sistema de tratamiento,

II. impedir el acceso de usuarios a los datos personales seleccionados o

III. retirar temporalmente los datos publicados de un sitio internet.[661]

f) En el caso de archivos automatizados, se dispone que la limitación del tratamiento habrá de realizarse inicialmente a través de medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse siendo necesario que el responsable indique en el sistema utilizado que el tratamiento de los datos se encuentra limitado.[662]

---

659 "Artículo 21
Derecho de oposición
1. El interesado tendrá derecho a oponerse, en cualquier momento y por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e o f, incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado o para la formulación, el ejercicio o la defensa de reclamaciones".

660 Apartado 2, artículo 18 del Reglamento General de Protección de Datos Personales.

661 Considerando 67) del Reglamento General de Protección de Datos Personales.

662 Reglamento (UE) 2018/1725 del parlamento europeo y del consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la unión, y a la libre circulación de esos datos, y por el que se derogan el reglamento (ce) n.º 45/2001 y la decisión n.º 1247/2002/ce

g) El responsable, según el artículo 19 del RGPD, tendrá que comunicar cualquier rectificación o supresión de datos personales o limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado.[663] Con base en lo anterior, en el supuesto de que el interesado lo solicite al responsable, este último también le deberá informar sobre la identidad de los destinatarios a los que se hayan compartido sus datos personales.

h) El ejercicio de este derecho se sujetará a los mismos plazos y procedimientos que los restantes derechos previstos en el RGPD. Es decir, el responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de un mes (pudiendo extenderse a dos meses más cuando se trate de solicitudes especialmente complejas y siempre que la ampliación se informe en el primer mes).[664]

En consecuencia, con motivo de ejercicio del derecho de limitación al tratamiento se otorga control al titular de los datos y se impide la práctica poco leal de borrar los datos cuando se ejercitan otros derechos, como el de acceso, ya que impediría el ejercicio del derecho a la limitación del tratamiento.[665]

Derecho al honor

Eduardo Ferrer Mac-Gregor Poisot

1. Delimitación conceptual

El derecho al honor doctrinalmente se conoce como uno de los "derechos de la personalidad".[666] Como derecho de la personalidad,[667] el honor es una cualidad o atributo inherente a la persona que deriva de la propia persona humana y se encarga de defender la propia personalidad, frente a sí misma y frente a los demás.[668] Esto es, se trata de los atributos o cualidades más próximos a la persona,[669] que en palabras de Castán de Tobeñas "son aquellas facultades concretas de que está investido todo el que tiene personalidad. Constituyen un núcleo esencial".[670]

Los derechos de la personalidad,[671] como el derecho al honor, son derechos *erga omnes*, limitados, subjetivos, privados, innatos, inherentes, esenciales, intransmisibles, irrenunciables,

663 Artículo 19 del Reglamento General de Protección de Datos Personales.

664 Agencia Española de Protección de Datos, et al., (2017). *Guía del Reglamento General de Protección de Datos, Guía de Protección de Datos UE*. Disponible en: https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf Fecha de consulta: 14 de noviembre de 2018.

665 Artículo 19 del Reglamento General de Protección de Datos Personales.

666 Mendoza, L. (2014). *La acción civil del daño moral*. México. UNAM-Instituto de Investigaciones jurídicas, p. 26.

667 Los llamados derechos de la personalidad, que también se denominan derechos sobre la propia persona, individuales o personalísimos, constituyen un tipo singular de facultades reconocidas a las personas físicas para el aprovechamiento legal de diversos bienes derivados de su propia naturaleza somática, de sus cualidades espirituales y, en general, de las proyecciones integrantes de su categoría humana. Enciclopedia Jurídica Mexicana. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. (2000). Tomo III D-E. México. Editorial Porrúa, pp. 408-410.

668 Cfr., Pacheco, A. (1991). *La persona en el derecho civil mexicano*. 2a. ed. México. Panorama, p. 62.

669 Mendoza, L. (2014). *La acción civil del daño moral*. México. UNAM-Instituto de Investigaciones jurídicas, p. 26.

670 Castán, J. (1952). *Los derechos de la personalidad*. Madrid. Reus, p. 15.

671 La Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal, en la fracción IV de su artículo 7, define a los derechos de la personalidad de la siguiente manera: "IV. Derecho de Personalidad: Los bienes constituidos por determinadas proyecciones, físicas o psíquicas del ser humano, relativas a su integridad física y mental, que las atribuye para sí o para algunos sujetos de derecho, y que son individualizadas por el ordenamiento jurídico. Los derechos de personalidad tienen, sobre todo, un valor moral, por lo que componen el patrimonio moral de las personas".

inembargables e inmateriales.[672] Dada su naturaleza personal, estos derechos corresponden a las personas físicas y son inalienables, imprescriptibles, irrenunciables e inembargables. No obstante, se ha admitido jurídica[673] y doctrinalmente que las personas morales gocen de estos derechos en aquellos aspectos que no resulten incompatibles con su naturaleza jurídica.[674]

El Poder Judicial Federal (PJF) ha destacado que debido a que los derechos humanos se consideran esenciales e inherentes al ser humano y derivados de su propia naturaleza, resulta lógico que los atributos de la personalidad se enlacen directamente con tales derechos, pues los mencionados atributos tienen una coincidencia con las libertades protegidas por los derechos del hombre, como son los concernientes al honor, a la intimidad y a la propia imagen, que constituyen derechos subjetivos del ser humano, en tanto que son inseparables de su titular, quien nace con ellos, y el Estado debe reconocerlos. Así, se ha enfatizado que como no recaen sobre bienes materiales, sino sobre la personalidad de los individuos,[675] son generales porque corresponden a todos los seres humanos y no pueden considerarse renunciables, transmisibles o prescriptibles porque son inherentes a la persona misma, es decir, son intrínsecos al sujeto, quien no puede vivir sin ellos.[676]

El derecho al honor normalmente aparece dentro de una trilogía de derechos íntimamente vinculados entre sí y resulta casi imposible analizarlos por separado: el derecho al honor, el derecho a la intimidad (personal y familiar) y el derecho a la propia imagen.[677] Se habla así de derechos humanos estrechamente relacionados y tutelados en el orden jurídico nacional y los tratados internacionales en materia de derechos humanos de los que México es parte.

2. Definición

El derecho al honor no tiene una definición universalmente aceptada. Se trata de un concepto jurídico indeterminado frente al que no existe una acepción unívoca de alcance general.[678] El honor, entonces, constituye un "concepto jurídico normativo cuya precisión

672 Mendoza, L. (2014). *La acción civil del daño moral*. México. UNAM-Instituto de Investigaciones jurídicas, p. 26.

673 Por ejemplo, la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal indica en su artículo sexto lo siguiente:
Artículo 6.
Los derechos de la personalidad corresponden a las personas físicas y son inalienables, imprescriptibles, irrenunciables e inembargables.
La persona moral también goza de estos derechos, en lo que sea compatible con la naturaleza jurídica de ésta.

674 En este contexto, autores como Carlos Rogel Vide destacan que "en realidad, plantearse el tema del honor de las personas jurídicas es un contrasentido pues, en puridad, el honor, en cuanto valoración de uno mismo, en cuanto sentimiento, solo puede ser propio de las personas físicas". *Vid*. Rogel, C. (2007) "Origen y actualidad de los derechos de la personalidad". *IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C.* México. Núm. 20, p. 278.

675 En relación con el significado personalista del derecho al honor, resulta interesante la postura del Tribunal Constitucional Español 107/1988, del 8 de junio de 1988, al señalar lo siguiente: "En el contexto de estos asuntos de relevancia pública, es preciso tener presente que el derecho al honor tiene en nuestra Constitución un significado personalista, en el sentido de que el honor es un valor referible a personas individualmente consideradas, lo cual hace inadecuado hablar del honor de las instituciones públicas o de clases determinadas del Estado, respecto de las cuales es más correcto, desde el punto de vista constitucional, emplear los términos de dignidad, prestigio y autoridad moral, que son valores que merecen la protección penal que les dispense el legislador, pero que no son exactamente identificables con el honor, consagrado en la Constitución como derecho fundamental, y, por ello, en su ponderación frente a la libertad de expresión debe asignárseles un nivel más débil de protección del que corresponde atribuir al derecho al honor de las personas públicas o de relevancia pública".

676 Tesis: I.5o.C.4 K (10a.). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro XXI. Junio de 2013. Tomo 2, pp. 1258.

677 *Cfr*. Risso, J. (2002). "Algunas reflexiones sobre los derechos al honor, a la intimidad, a la propia imagen y a la libertad de prensa". *Anuario de Derecho Constitucional Latinoamericano*. Uruguay, p. 279.

678 Villanueva, E. y Gómez, P. (2012). *Libertad de expresión en Latinoamérica*. México. Novum, p. 42.

depende de las normas, valores e ideas sociales vigentes en cada momento",[679] por lo que será posible encontrar variantes en la definición de su contenido y alcance.

El honor, de acuerdo con el *Diccionario de la Real Academia Española* (RAE), se define como: "Cualidad moral que lleva al cumplimiento de los propios deberes respecto del prójimo y de uno mismo".[680] Desde la perspectiva jurídica, este término se considera como "una cualidad moral que nos hace cumplir severamente nuestros deberes, lo que provoca que la sociedad nos considere como personas de estima y nos otorgue una consideración determinada, la cual se convierte en una reputación como opinión general y así gozamos de cierta fama".[681]

De acuerdo con la *Enciclopedia Jurídica Mexicana*, el honor, en estricta subjetividad, alude a aquella cualidad de carácter moral que nos lleva al más rígido cumplimiento de nuestros deberes respecto del prójimo y de nosotros mismos. El honor es un valor cultural, un bien esencial y eminentemente cultural, de ahí que (desde un punto de vista jurídico-penal) se trata de uno de los bienes jurídicos más difíciles de captar y de concretar.[682]

Por otro lado, Fernández Bogado señala que el honor "es el sentimiento o la conciencia de la propia dignidad, y es también el más valioso atributo que una persona pueda tener frente a las demás; de su reconocimiento depende en alto grado la estima que los demás tengan hacia esa persona".[683] El derecho al honor, así, se concibe como un bien inalienable de las personas, que se puede exigir *erga omnes*, de decir, frente a todo el mundo.[684]

El derecho al honor, según Villanueva, puede destacarse como "la potestad jurídica que tienen las personas físicas o jurídicas[685] para proteger su estima, su crédito y/o reconocimiento social frente a intrusiones ilegítimas que las pueden hacer desmerecer en la consideración propia y ajena".[686] El derecho al honor, según el referido autor y Gómez Gallardo, es "la facultad exigible para ser dejado en paz, para no ser, por ende, expuesto al odio, al desprecio o al ridículo frente a uno mismo y de cara a la propia sociedad".[687]

679 Beltrá, C. (2016). "Protección del derecho al honorcolisión de la libertad de expresión y de información y el derecho al honor". *CEFLegal: revista práctica de derecho. Comentarios y casos prácticos*. España. Núm. 185, pp. 71-76.

680 *Diccionario de la Lengua Española*, versión electrónica. Disponible en: http://dle.rae.es/?id=KdBUWwv Fecha de consulta: 15 de agosto de 2018.

681 Bazúa, A. (2005). *Los derechos de la personalidad. Sanción civil a su violación.* Colección Colegio de Notarios del Distrito Federal. México. Porrúa-Colegio de Notarios del Distrito Federal, p. 51.

682 *Enciclopedia Jurídica Mexicana*. (2000). Tomo IV F-L. Instituto de Investigaciones Jurídicas. Universidad Nacional Autónoma de México. Editorial Porrúa. México, p. 332.

683 Fernández, B. (2010). "Derecho al honor", en *Diccionario de Derecho de la Información*. Tomo I. Instituto de Investigaciones Jurídicas. Tercera Edición. México.

684 Villanueva, E. y Gómez, P. (2012). *Libertad de expresión en Latinoamérica*. México. Novum, p. 42.

685 En relación con la titularidad de este derecho para las personas jurídicas conviene destacar la sentencia 139/1995, de 26 de septiembre de 1995 del Tribunal Constitucional Español en la que se precisó lo siguiente: "Cierto es que, por falta de una existencia física, las personas jurídicas no pueden ser titulares del derecho a la vida, del derecho a la integridad física, ni portadoras de la dignidad humana. Pero si el derecho a asociarse es un derecho constitucional y si los fines de la persona colectiva están protegidos constitucionalmente por el reconocimiento de la titularidad de aquellos derechos acordes con los mismos, resulta lógico que se les reconozca también constitucionalmente la titularidad de aquellos otros derechos que sean necesarios y complementarios para la consecución de esos fines. En ocasiones, ello solo será posible si se extiende a las personas colectivas la titularidad de derechos fundamentales que protejan —como decíamos— su propia existencia e identidad, a fin de asegurar el libre desarrollo de su actividad, en la medida en que los derechos fundamentales que cumplan esta función sean atribuibles, por su naturaleza, a las personas jurídicas".

686 Villanueva, E. (2014). "Derecho al honor", en Ferrer Mac-Gregor, Eduardo, Martínez Ramírez, Fabiola, *et al.,* (coords.). *Diccionario de derecho procesal constitucional y convencional*. 2a. ed. México. Instituto de investigaciones Jurídicas Universidad Nacional Autónoma de México, p. 400.

687 Villanueva, E. y Gómez, P. (2012). *Libertad de expresión en Latinoamérica*. México. Novum, p. 42.

El artículo 12 de la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal indica que el honor es "la valoración que las personas hacen de la personalidad ético-social de un sujeto y comprende las representaciones que la persona tiene de sí misma, que se identifica con la buena reputación y la fama". En términos de lo dispuesto por el segundo párrafo del referido ordenamiento "el honor es el bien jurídico constituido por las proyecciones psíquicas del sentimiento de estimación que la persona tiene de sí misma, atendiendo a lo que la colectividad en que actúa considera como sentimiento estimable".

Por ejemplo, en España, la ley orgánica 1/1982, del 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, establece, en su artículo primero, que el derecho fundamental al honor (y así también los derechos a la intimidad personal y familiar y a la propia imagen) será protegido civilmente frente a todo género de intromisiones ilegítimas. Como características de este derecho, el apartado 3 del citado artículo primero precisa que el derecho al honor es irrenunciable, inalienable e imprescriptible.[688]

En el orden nacional, la Suprema Corte de Justicia de la Nación (SCJN), en la tesis de jurisprudencia 1a./J. 118/2013 (10a.), ha indicado que es posible definir al honor como "el concepto que la persona tiene de sí misma o que los demás se han formado de ella, en virtud de su proceder o de la expresión de su calidad ética y social". La SCJN señala que todo individuo, al vivir en sociedad, tiene el derecho de ser respetado y considerado y, correlativamente, tiene la obligación de respetar a aquellos que lo rodean. En el campo jurídico esta necesidad se traduce en un derecho que involucra la facultad que tiene cada individuo de pedir que se le trate en forma decorosa y la obligación de los demás de responder a este tratamiento.[689]

La Primera Sala de la SCJN ha destacado que, en esta dimensión, el derecho al honor ampara también la buena reputación de una persona en sus cualidades morales y profesionales, protegiéndola frente a expresiones o mensajes que la hagan desmerecer en la consideración ajena, al ir en su descrédito o menosprecio.[690] De esta forma, también se ha señalado en el ámbito judicial que el honor es un bien objetivo que hace que la persona sea merecedora de confianza.[691]

En consecuencia, el honor es "un patrimonio personal que se requiere como requisito *sine qua non* para hacer vivible la vida en el entorno comunitario. De ahí, por tanto, que su afectación injustificada constituya condición para sanción, sea de carácter legal o de naturaleza deontológica".[692]

688 "Artículo 1
1. El derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo 18 de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido en la presente ley orgánica.
2. El carácter delictivo de la intromisión no impedirá el recurso al procedimiento de tutela judicial previsto en el artículo 9 de esta Ley. En cualquier caso, serán aplicables los criterios de esta Ley para la determinación de la responsabilidad civil derivada de delito.
Número 2 del artículo 1 redactado por la disposición final 4ª de la L.O. 10/1995, 23 noviembre, del Código Penal (BOE 24 noviembre).
3. El derecho al honor, a la intimidad personal y familiar y a la propia imagen es irrenunciable, inalienable e imprescriptible. La renuncia a la protección prevista en esta ley será nula, sin perjuicio de los supuestos de autorización o consentimiento a que se refiere el artículo 2 de esta ley".

689 Tesis: 1a./J. 118/2013 (10a.). Décima época. *Gaceta del Semanario Judicial de la Federación*. Tomo I. Febrero 2014, p. 470.

690 Tesis: 1a. LXII/2013 (10a.). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro XVII. Febrero de 2013. Tomo 1, Pp. 798.

691 Tesis: I.4o.C.57 C. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XVII. Marzo de 2003, pp. 1709.

692 Cfr. Villanueva, E. y Gómez, P. (2012). *Libertad de expresión en Latinoamérica*. México. Novum, p. 52.

3. Contenido

El derecho al honor, según Villanueva, "tiene por objeto la protección de la consideración, estima o valor personal en el ámbito público y en la percepción propia, cuyo valor jurídico debe ser establecido casuísticamente, a la luz de los principios prevalecientes en la sociedad en un tiempo y espacio determinados".[693] Por lo que, al tratarse de un concepto jurídico indeterminado, su contenido también es variable y habrá de ajustarse en razón de los procesos de evolución y permanencia de esos mismos valores sociales.[694]

De esta manera, se ha aceptado que el derecho al honor, además de ser un término complejo y dinámico, tiene atribuidos dos elementos fundamentales: el honor subjetivo, que se refiere a la esfera íntima de las personas (cómo se ven y se valoran a sí mismos en su relación con la sociedad) y el honor objetivo, que se traduce en la consideración que los demás tienen de uno mismo.[695]

La SCJN al abordar el tema del derecho al honor ha distinguido de manera precisa estas dos facetas aplicativas y ha señalado que la primera se refiere al aspecto subjetivo o ético, donde el honor se basa en un sentimiento íntimo que se exterioriza por la afirmación que la persona hace de su propia dignidad y que la segunda se refiere a un aspecto objetivo, externo o social, que se concibe como la estimación interpersonal que la persona tiene por sus cualidades morales y profesionales dentro de la comunidad. Se destaca así que, en el aspecto subjetivo, el honor es lesionado por todo aquello que lastima el sentimiento de la propia dignidad. En el aspecto objetivo, el honor es lesionado por todo aquello que afecta a la reputación que la persona merece, es decir, el derecho a que otros no condicionen negativamente la opinión que los demás hayan de formarse de nosotros.[696]

De la misma forma, la SCJN ha distinguido, a partir de la titularidad de este derecho, determinadas cuestiones prácticas referentes a su aplicación en relación con las personas físicas y morales. De este modo, se ha enfatizado que toda persona física es titular del derecho al honor, pues su reconocimiento es una consecuencia de la afirmación de la dignidad humana. Sin embargo, tratándose de personas jurídicas o morales[697] presenta mayores dificultades, toda vez que de ellas no es posible predicar dicha dignidad como fundamento de un eventual derecho al honor. Por ello, la Primera Sala de SCJN ha señalado la pertinencia de hacer uso de la faceta objetiva del derecho al honor aplicándola a las personas morales y señalando que éstas también pueden ver lesionado su derecho al honor a través de la divulgación de hechos concernientes a su entidad, cuando otra perso-

693 Villanueva, E. (2014). "Derecho al honor", en Ferrer Mac-Gregor, Eduardo, Martínez Ramírez, Fabiola, *et al.,* (coords.). *Diccionario de derecho procesal constitucional y convencional*. 2a. ed. México. Instituto de investigaciones Jurídicas Universidad Nacional Autónoma de México, p. 400.

694 Ídem.

695 Cfr. Villanueva, E. y Gómez, P. (2012). *Libertad de expresión en Latinoamérica*. México. Novum, p. 52.

696 1a./J. 118/2013 (10a.). Décima época. *Gaceta del Semanario Judicial de la Federación*. Libro 3. febrero de 2014. Tomo I, pp. 470.

697 Sobre la titularidad de este derecho a personas morales, la sentencia 139/1995, del 26 de septiembre de 1995 del Tribunal Constitucional Español ha señalado lo siguiente: "Cierto es que, por falta de una existencia física, las personas jurídicas no pueden ser titulares del derecho a la vida, del derecho a la integridad física, ni portadoras de la dignidad humana. Pero si el derecho a asociarse es un derecho constitucional y si los fines de la persona colectiva están protegidos constitucionalmente por el reconocimiento de la titularidad de aquellos derechos acordes con los mismos, resulta lógico que se les reconozca también constitucionalmente la titularidad de aquellos otros derechos que sean necesarios y complementarios para la consecución de esos fines. En ocasiones, ello solo será posible si se extiende a las personas colectivas la titularidad de derechos fundamentales que protejan —como decíamos— su propia existencia e identidad, a fin de asegurar el libre desarrollo de su actividad, en la medida en que los derechos fundamentales que cumplan esta función sean atribuibles, por su naturaleza, a las personas jurídicas".

na la difame o la haga desmerecer en la consideración ajena.[698] En todo caso, en el amparo directo en revisión 1621/2010, resolución de la que se desprenden las consideraciones de la tesis recién citada, la Primera Sala reconoció los efectos de los derechos fundamentales en todo tipo de relaciones, incluyendo las jurídico-privadas.[699]

El derecho al honor personal prohíbe que se refiera a una persona de forma insultante o injuriosa, o atentando injustificadamente contra su reputación, haciéndola desmerecer ante la opinión ajena,[700] situación que, en términos de lo previsto por el Código Civil Federal, dará lugar a una reclamación de reparación por daño moral.[701]

Un caso paradigmático sobre reparación por daño moral, en el marco de la tensión entre el derecho al honor y la libertad de expresión, fue resuelto por la Primera Sala de la SCJN el 23 de enero de 2011 en el amparo directo 28/2010. El caso además es importante porque se trató de un conflicto entre dos medios de comunicación. La revista *Letra Libres* publicó un artículo en el que acusaba a *La Jornada* de ser el periódico de la asociación terrorista ETA. *La Jornada* demandó en la vía ordinaria civil a *Letra Libres* y al autor de la nota por daño moral. Después de que el juez de primera instancia absolviera a los demandados y, en apelación, se les condenara, ambas partes promovieron un amparo.

En la resolución del alto tribunal, después de reconocer que *La Jornada*, como persona moral, es titular de derechos fundamentales (esto es, tiene derecho al honor, no porque puedan herirse sus sentimientos, pero sí en cuanto a su reputación y su nombre)[702] y de identificar los derechos en pugna entre las partes (derecho al honor frente a libertad de expresión)[703]

698 Tesis: 1a. XXI/2011 (10a.). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro IV. Enero de 2012. Tomo 3, pp. 2905.

699 "A juicio de esta Primera Sala, los derechos fundamentales previstos en la Constitución gozan de una doble cualidad, ya que si por un lado se configuran como derechos públicos subjetivos (función subjetiva), por el otro se traducen en elementos objetivos que informan o permean todo el ordenamiento jurídico, incluyendo aquellas que se originan entre particulares (función objetiva). En un sistema jurídico como el nuestro —en el que las normas constitucionales conforman la ley suprema de la Unión— los derechos fundamentales ocupan una posición central e indiscutible como contenido mínimo de todas de las relaciones jurídicas que se suceden en el ordenamiento. / […] / Como señalamos anteriormente, la fuerza vinculante de los derechos fundamentales en todo tipo de relaciones, incluyendo las jurídico-privadas, tiene como efecto que los tribunales deben atender a la influencia de los valores que subyacen a dichos derechos en los asuntos que son de su conocimiento". Suprema Corte de Justicia de la Nación. Amparo directo en revisión 28/2010, del 15 de junio de 2011.

700 Tribunal Constitucional Español. Sentencia 180/1999, del 11 de octubre.

701 Artículo 1916. Por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, o bien en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas.

702 "En primer lugar es necesario tomar en cuenta que las personas denominadas morales o jurídicas son creadas por personas físicas para la consecución de fines determinados, que de otra forma no se podrían alcanzar, de modo que las personas jurídicas constituyen un instrumento al servicio de los intereses de las personas que las crearon. En segundo lugar, debemos considerar que los entes colectivos creados son la consecuencia del ejercicio previo de otros derechos, como la libertad de asociación, y que el pleno ejercicio de este derecho requiere que la organización creada tenga suficientemente garantizados aquellos derechos fundamentales que sean necesarios para la consecución de los fines propuestos. / Por lo anterior es posible afirmar que las personas jurídicas deben ser titulares de aquellos derechos fundamentales que sean acordes con la finalidad que persiguen, por estar encaminados a la protección de su objeto social, así como de aquéllos que aparezcan como medio o instrumento necesario para la consecución de la referida finalidad. / Es en este ámbito que se encuentra el derecho al honor, pues el desmerecimiento en la consideración ajena sufrida por determinada persona jurídica conllevará, sin duda, la imposibilidad de que esta pueda desarrollar libremente sus actividades encaminadas a la realización de su objeto social o, al menos, una afectación ilegítima a su posibilidad de hacerlo. En consecuencia, la persona jurídica también puede ver lesionado su derecho al honor a través de la divulgación de hechos concernientes a su entidad, cuando otra persona la difame o la haga desmerecer en la consideración ajena". Suprema Corte de Justicia de la Nación. Amparo directo 28/2010, del 23 de noviembre de 2011, p. VIII.

703 "De conformidad con lo antes expuesto y tal y como se planteó desde los escritos de demanda y contestación de la misma, así como en los recursos y juicios interpuestos con posterioridad, en el presente caso existe un conflicto entre el derecho a la libre expresión de la revista *Letras Libres* y el derecho al honor del diario *La Jornada*, de modo que la *litis* se centrará en la colisión entre ambos principios". Ídem, p. X.

se llegó a la conclusión de que *La Jornada*, como medio de comunicación, tiene un estatus de figura pública equivalente al de un servidor público,[704] que además cuenta con los mecanismos de difusión para contrarrestar las opiniones discrepantes (dicho de otra forma, existe una simetría de poder entre los contendientes)[705] que son necesarias y refuerzan el papel de los medios de comunicación en el marco de una sociedad democrática:

> El debate en temas de interés público debe ser desinhibido, robusto y abierto, pudiendo incluir ataques vehementes, cáusticos y desagradablemente mordaces sobre personajes públicos o, en general, ideas que puedan ser recibidas desfavorablemente por sus destinatarios y la opinión pública en general, de modo que no solo se encuentran protegidas las ideas que son recibidas favorablemente o las que son vistas como inofensivas o indiferentes. Estas son las demandas de una sociedad plural tolerante y abierta, sin la cual no existe una verdadera democracia.[706]

De esta forma, el alto tribunal da continuidad a su línea jurisprudencial fijada en el amparo directo en revisión 2044/2008, en el sentido de que los límites de crítica son más amplios cuando se trata de personas dedicadas a actividades públicas, pues están expuestas a un control mayor que aquellas personas sin proyección pública, lo cual se encuentra justificado en el marco de una sociedad democrática.

4. Tratados internacionales

El derecho al honor, a diferencia de otros derechos humanos, no se encuentra expresamente reconocido en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), pues más bien se puede encontrar referido como un límite a la libertad de expresión.[707] Sin embargo, dada la distinción que hace el artículo primero de la CPEUM,[708] al "poner de ma-

704 "En la actualidad existe una tendencia a subestimar el poder de los medios de comunicación, sin embargo, es un error minimizarlo pues se trata de entidades cuyas opiniones suelen imponerse en la sociedad, dominando la opinión pública y generando creencias. La televisión, la radio, los periódicos, las revistas y demás medios de comunicación son fácilmente accesibles para el público y, de hecho, compiten para atraer su atención. Así pues, es usual encontrar que muchas de las discusiones que se presentan día con día, se basan o hacen referencia a creencias públicas generadas por alguna noticia o análisis. Asimismo, es importante señalar que, en la prensa y televisión modernas, se da por sentado que toda opinión debe quedar equilibrada por otra contraria. / A través de los medios de comunicación, los líderes de opinión despliegan sus ideas, convirtiéndose así en los sujetos a quienes se atribuye la misión de elaborar y transmitir conocimientos, teorías, doctrinas, ideologías, concepciones del mundo o simples opiniones, que constituyen las ideas o los sistemas de ideas de una determinada época y de una sociedad específica. Lo importante para efectos del presente estudio, es señalar que, mediante sus opiniones, los líderes de opinión ejercen un cierto tipo de poder, valiéndose de la persuasión y no de la coacción. / Lo antes expuesto evidencia que estamos ante una tercera especie de figura pública: los medios de comunicación, de la mano de los líderes de opinión". Ídem, p. XVII

705 "Si la prensa goza de la mayor libertad y del más amplio grado de protección para criticar personajes con proyección pública, es no solo lógico sino necesario concluir que la crítica a su labor también debe gozar de la mayor libertad y más amplio grado de protección, pues de lo contrario se estaría dotando a una persona, en este caso un medio de comunicación impreso, de un gran y desequilibrado poder para criticar impunemente, opinando e informando sin ser sujeto del mismo escrutinio público que pregona, ejerce y cuya protección invoca. / Lo anterior adquiere mayor relevancia si consideramos que en el debate surgido del ejercicio de la libertad de expresión, la réplica y la contra-argumentación son las mejores y más efectivas herramientas para defender la propia actuación o punto de vista. Así pues, nadie tiene un mayor acceso al derecho de réplica que un medio de comunicación, máxime si se trata de un rotativo cuya publicación es diaria". Ídem., p. XXIII

706 Tesis de jurisprudencia 32/2013 (10a.). Aprobada por la Primera Sala de este Alto Tribunal, en sesión de fecha 27 de febrero de 2013.

707 Artículo 6. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

708 Artículo 1. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.
Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.

nifiesto que son tan importantes los derechos humanos que tienen reconocimiento constitucional como aquellos que figuran en tratados internacionales",[709] se puede atribuir al derecho al honor la naturaleza de derecho humano reconocido y tutelado en el ordenamiento jurídico mexicano que el Estado mexicano tiene la obligación de garantizar. [710]

De lo anterior, se advierte que nuestro país actualmente adopta una protección amplia de los derechos humanos, mediante el reconocimiento claro del principio *pro personae* como rector de la interpretación y aplicación de las normas jurídicas, en aquellas que favorezcan y brinden mayor protección a las personas, aunado a que también precisa de manera clara la obligación de observar los tratados internacionales firmados por el Estado mexicano al momento de aplicar e interpretar las normas jurídicas en las que se vea involucrado este tipo de derechos, como son los señalados atributos de la personalidad conforme a la Convención Americana sobre Derechos Humanos (CADH) y el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), y en casos en los que se involucra la posible afectación por daño moral de un atributo de la personalidad —en su vertiente del derecho al honor— debe aplicarse la tutela y protección consagrada en los principios reconocidos al efecto en nuestra Carta Magna, con independencia de que no exista una referencia expresa en el texto constitucional hacia la salvaguarda concreta del citado atributo, pues la obligación de protección deriva de disposiciones contenidas en dos tipos de ordenamientos superiores —Constitución y tratados internacionales— con los que cuenta el Estado mexicano.[711]

El derecho humano al honor, se encuentra reconocido en los siguientes instrumentos internacionales de los que México es parte:

La Declaración Universal de Derechos Humanos en su artículo 12 señala lo siguiente:

> Artículo 12.
>
> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

La CADH en su artículo 11 dispone lo siguiente:

> Artículo 11. Protección a la honra y de la dignidad
>
> Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado deberá prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley.
Está prohibida la esclavitud en los Estados Unidos Mexicanos. Los esclavos del extranjero que entren al territorio nacional alcanzarán, por este solo hecho, su libertad y la protección de las leyes.
Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

709 Cfr., Carbonell, M. (2013). *Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana*. México. SCJN-UNAM. Instituto de Investigaciones Jurídicas-Fundación Konrad Adenauer. Tomo I, p. 36.

710 Esta obligación de garantizar es mucho más amplia que las obligaciones específicas consagradas en otros instrumentos internacionales pues engloban obligaciones de protección, investigación, sanción, reparación, cooperación y en general la adecuación de todo el aparato gubernamental para asegurar el libre y pleno ejercicio de los derechos humanos. Cfr., Ferrer, E. y Pelayo, C. (2017). "Las obligaciones generales de la Convención Americana sobre Derechos Humanos (deber de respeto, garantía y adecuación de derecho interno)", en *Colección Estándares del Sistema Interamericano de Derechos Humanos: miradas complementarias desde la academia*. Núm. 7. México. IIJ-UNAM. CENADEH-CNDH, p.9.

711 Tesis: I.5o.C.4 K (10a.). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro XXI. Junio de 2013. Tomo 2, p. 1258.

Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Por su parte, el artículo 17 del PIDCP precisa lo siguiente:

ARTÍCULO 17.-

Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

En consecuencia, el derecho al honor se consagra como un derecho humano sustancial[712] protegido por la CPEUM y los instrumentos de carácter internacional de los que México forma parte.

5. El derecho al honor en las resoluciones de la Corte Interamericana de Derechos Humanos

La Corte Interamericana de Derechos Humanos (Corte IDH) ha emitido diversas resoluciones en las que se manifiesta a propósito del derecho al honor, preponderantemente en casos en los que la libertad de expresión aparece analíticamente contrapuesta al derecho al honor o la protección de la reputación (de los funcionarios públicos, candidatos, militares, etcétera).[713] A continuación se presentan los casos más relevantes resueltos por la Corte IDH en los que se han involucrado conceptos jurídicos sobre el derecho al honor.

A. Caso "Herrera Ulloa vs. Costa Rica"

En el caso "Herrera Ulloa vs. Costa Rica" se adujo la violación del artículo 13 de la CADH[714] como consecuencia de la imposición de una condena por difamación en perjuicio de un periodista y la falta de un recurso adecuado y efectivo para cuestionar dicha medida.[715]

712 De acuerdo con la doctrina, son derechos sustantivos los que se identifican con los bienes de la vida. En ese sentido, pueden considerarse sustantivos, sin pretender asignarles un orden, entre otros, los derechos patrimoniales, los que surgen de las relaciones de familia y del estado civil de las personas, la vida misma, la libertad personal, la de conciencia, la de expresión, el derecho al honor, a la intimidad, etc. En cambio, los derechos procesales o instrumentales, también llamados adjetivos, son únicamente el medio para hacer observar o proteger el derecho sustantivo. Tales derechos procesales no tienen por objeto su propio ejercicio, ni constituyen un fin en sí mismos, sino que se trata solo de las reglas para obtener del Estado la garantía del goce de los bienes de la vida. *Vid*. Tesis: I.8o.C. J/2 (10a.). Décima época. *Gaceta del Semanario Judicial de la Federación*. Libro 40. Marzo de 2017. Tomo IV, pp. 2416.

713 Cfr., Pou, F. (2013). "La libertad de expresión y sus límites", en *Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana.* México. SCJN-UNAM. Instituto de Investigaciones Jurídicas-Fundación Konrad Adenauer. Tomo I, pp. 919-920.

714 "Artículo 13. Libertad de Pensamiento y de Expresión
1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
a) el respeto a los derechos o a la reputación de los demás, o
b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.
3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.
4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.
5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional".

715 CIDH. (2018). Ficha Técnica: "Herrera Ulloa Vs. Costa Rica". Disponible en: http://www.corteidh.or.cr/cf/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=209&lang=es Fecha de consulta: 21 de agosto de 2018.

Al abordar las restricciones permitidas a la libertad de pensamiento y de expresión en una sociedad democrática, la Corte IDH señaló lo siguiente: "En este contexto, es lógico y apropiado que las expresiones concernientes a funcionarios públicos o a otras personas que ejercen funciones de una naturaleza pública deben gozar, en los términos del artículo 13.2 de la Convención, de un margen de apertura a un debate amplio respecto de asuntos de interés público, el cual es esencial para el funcionamiento de un sistema verdaderamente democrático. Esto no significa, de modo alguno, que el honor de los funcionarios públicos o de las personas públicas no deba ser jurídicamente protegido, sino que éste debe serlo de manera acorde con los principios del pluralismo democrático". [716]

En el orden nacional, destaca la emisión de la sentencia en el amparo directo en revisión 2044/2008,[717] en la cual la SCJN hizo propios los estándares del Sistema Interamericano de Derechos Humanos y, así, amparó al director de un periódico que había sido condenado a indemnizar a un expresidente municipal por la publicación de una entrevista a un antiguo empleado con informaciones que al exfuncionario le parecían injuriosas.[718] Asimismo, al resolver el caso, la SCJN declaró inconstitucionales distintos artículos de la Ley de Imprenta del Estado de Guanajuato.

Este fallo tiene una notable importancia en el terreno práctico, como destaca Pou Giménez, por una orientación certera, en el plano sustantivo, respecto del tratamiento de un conflicto entre la libertad de expresión y el derecho al honor de los políticos o expolíticos, así como por sus pronunciamientos acerca de la inconstitucionalidad de la ley de imprenta aplicada para la resolución del caso.[719] Asimismo, siguiendo la línea de exposición de Gómez Marinero, este caso es relevante debido a que "dio lugar a la adopción del criterio proveniente de las resoluciones de organismos internacionales, al analizar los conflictos de libertad de expresión, en el sentido que las personas que desempeñan o han desempeñado responsabilidades públicas, así como los candidatos a desempeñarlas, tienen un derecho a la intimidad y al honor, con menor resistencia normativa general que el que asiste a los ciudadanos ordinarios frente a la actuación de los medios de comunicación".[720]

Posteriormente, la SCJN analizó en el amparo directo en revisión 1302/2009, en el que determinó, por mayoría de votos, que los medios impresos no poseen un deber de cuidado encaminado a verificar que las inserciones pagadas contratadas por particulares no contengan mensajes que vulneren los derechos a la intimidad o al honor de otros particulares.[721]

B. Caso "Ricardo Canese vs. Paraguay"

En el caso "Ricardo Canese vs. Paraguay" se adujo la violación al artículo 13 de la CADH y se atribuyó al Estado de Paraguay la responsabilidad internacional por la condena en un proceso de difamación y calumnia y las restricciones para salir del país impuestas en perjuicio Ricardo Nicolás Canese Krivoshein.[722]

716 Cfr. Corte IDH. (S/f). Caso "Herrera Ulloa vs. Costa Rica". Sentencia de 2 de julio de 2004. (Excepciones Preliminares, Fondo, Reparaciones y Costas). Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf

717 Sentencia de Amparo Directo en Revisión 2044/2008. Disponible en: http://207.249.17.176/Transparencia/Paginas/SentenciasCriterio_Sentencia.aspx Fecha de consulta: 23 de agosto de 2018.

718 Cfr., Pou, F. (2013). *La libertad de expresión y sus límites. Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana.* México. SCJN-UNAM. Instituto de Investigaciones Jurídicas-Fundación Konrad Adenauer. Tomo I, p. 927.

719 Ídem.

720 Gómez, C. (2016, julio-agosto). "La libertad de expresión en las sentencias de la Suprema Corte de Justicia". *Revista Hechos y Derechos*. México. Núm. 34, p. 130.

721 *Cfr.*, García, L. (2013). *El derecho a la libertad de expresión, la libertad de imprenta y los medios de comunicación. Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana.* México. SCJN-UNAM. Instituto de Investigaciones Jurídicas-Fundación Konrad Adenauer. Tomo II, p. 1008.

722 Ficha Técnica: "Ricardo Canese vs. Paraguay", consultado el 21 de agosto de 2018, disponible en http://www.corteidh.

En relación con el alcance del derecho al honor, la Corte IDH, al abordar las restricciones permitidas a la libertad de pensamiento y de expresión en una sociedad democrática, refirió: "Las anteriores consideraciones no significan, de modo alguno, que el honor de los funcionarios públicos o de las personas públicas no deba ser jurídicamente protegido, sino que éste debe serlo de manera acorde con los principios del pluralismo democrático. Asimismo, la protección de la reputación de particulares que se encuentran inmiscuidos en actividades de interés público también se deberá realizar de conformidad con los principios del pluralismo democrático".[723]

En este mismo sentido, encontramos la tesis 1a. CCXIX/2009 de la Primera Sala de la Suprema Corte de Justicia de la Nación, publicada en diciembre de 2009, en la que se precisó que las actividades desempeñadas por las personas con responsabilidades públicas interesan a la sociedad, y la posibilidad de crítica que esta última pueda legítimamente dirigirles debe entenderse con criterio amplio. Citando a la Corte IDH, se destaca que el umbral de protección al honor de un funcionario público debe permitir el más amplio control ciudadano sobre el ejercicio de sus funciones, porque el funcionario público se expone voluntariamente al escrutinio de la sociedad al asumir ciertas responsabilidades profesionales —lo que conlleva naturalmente mayores riesgos de sufrir afectaciones en su honor— y porque su condición le permite tener mayor influencia social y acceder con facilidad a los medios de comunicación para dar explicaciones o reaccionar ante hechos que lo involucren. Las personas con responsabilidades públicas mantienen la protección derivada del derecho al honor incluso cuando no estén actuando en carácter de particulares, pero las implicaciones de esta protección deben ser ponderadas con las que derivan del interés en un debate abierto sobre los asuntos públicos.[724]

Finalmente, respecto de la titularidad del derecho al honor, la CIDH destacó: "El artículo 11 de la Convención establece que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad, por lo que este derecho implica un límite a la expresión, ataques o injerencias de los particulares y del Estado. Por ello, es legítimo que quien se sienta afectado en su honor recurra a los mecanismos judiciales que el Estado disponga para su protección".

C. Caso "Tristán Donoso vs. Panamá"

En el caso "Tristán Donoso vs. Panamá" también se adujo la violación al artículo 13 de la CADH y se declaró la responsabilidad internacional del Estado de Panamá como resultado de la divulgación de una conversación telefónica de Santander Tristán Donoso, así como por la condena penal impuesta debido a sus declaraciones.[725]

Al analizar el caso, respecto a las restricciones a la libertad de expresión, la Corte IDH precisó que éste no es un derecho absoluto y que el artículo 13.2 de la Convención —que prohíbe la censura previa— también prevé la posibilidad de exigir responsabilidades ulteriores por el ejercicio abusivo de este derecho. Estas restricciones tienen carácter excepcional y no deben limitar, más allá de lo estrictamente necesario, el pleno ejercicio de la libertad de expresión y convertirse en un mecanismo directo o indirecto de censura previa. De esta forma, en rela-

or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=218

723 *Cfr.* Corte IDH, caso "Ricardo Canese vs. Paraguay". Fondo, Reparaciones y Costas. Sentencia de 31de agosto de 2004. Serie C N°. 111.

724 Tesis: 1a. CCXIX/2009. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXX. Diciembre de 2009, pp. 278.

725 Ficha Técnica: "Tristán Donoso vs. Panamá", consultado el 21 de agosto de 2018. Disponible en: http://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=253

ción los mecanismos para la defensa del derecho al honor, el tribunal internacional puntualizó: "Por su parte, el artículo 11 de la Convención establece que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Esto implica límites a las injerencias de los particulares y del Estado. Por ello, es legítimo que quien se considere afectado en su honor recurra a los medios judiciales que el Estado disponga para su protección".[726]

D. Caso "Escher y otros vs. Brasil"

En el caso "Escher y otros vs. Brasil", se imputó responsabilidad internacional al Estado de Brasil por la interceptación, monitoreo y divulgación de conversaciones telefónicas de diversos ciudadanos por parte de la policía militar del estado de Paraná.[727]

La Corte IDH destacó la consagración del derecho al honor en la CADH y su alcance al indicar lo siguiente: "El artículo 11 de la Convención reconoce que toda persona tiene derecho al respeto a su honor, prohíbe todo ataque ilegal contra la honra y reputación e impone a los Estados el deber de brindar la protección de la ley contra tales ataques. En términos generales, el derecho a la honra se relaciona con la estima y valía propia, mientras que la reputación se refiere a la opinión que otros tienen de una persona".[728]

Este caso es interesante debido a que en él se involucraron otros derechos, como la vida privada, la intimidad y la privacidad. La Corte IDH determinó que fue violada la vida privada y honor de los ciudadanos brasileños citados, en virtud de la interceptación, grabación y divulgación de las conversaciones telefónicas, considerándose además que dichas personas fueron víctimas de la violación a sus derechos de asociación, a las garantías judiciales y a la protección judicial.

E. Caso "Kimel vs. Argentina"

El caso "Kimel vs. Argentina" se refiere a la responsabilidad internacional del Estado de Argentina por la condena a Eduardo Kimel por el delito de calumnia debido a la publicación de un libro. Este libro analizaba los asesinatos de cinco religiosos pertenecientes a la orden palotina, ocurridos en Argentina el 4 de julio de 1976, durante la última dictadura militar. Asimismo, se criticaba la actuación de las autoridades encargadas de la investigación de los homicidios, en particular la de un juez.[729]

En este caso la Corte IDH, al abordar el tema del derecho al honor, señaló lo siguiente: "…la Corte deja establecido que el derecho al honor de todas las personas es materia de protección y que los funcionarios públicos se encuentran "amparados por la protección que les brinda el artículo 11 convencional que consagra el derecho a la honra" (párrafo 71) ya que la protección de la honra y reputación de toda persona es un fin legítimo acorde con la Convención" (párrafo 71). "El distinto umbral de protección no es sinónimo de ausencia de límites para quien comunica por un medio masivo, ni la carencia de derechos para dichos personajes públicos. El derecho al honor es uno vigente para todos por lo cual en ejercicio de la libertad de expresión no se deben emplear frases injuriosas, insultos o insinuaciones insidiosas y vejaciones".[730]

---

726 Cfr. Corte IDH. Caso "Tristán Donoso vs. Panamá". Excepción Preliminar, fondo, reparaciones y costas. Sentencia de 27 de enero de 2009. Serie C. No. 193.

727 *Escher y otros vs. Brasil*, consultado el 21 de agosto de 2018. Disponible en http://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=277&lang=

728 Cfr. Corte IDH. Caso "Escher y otros vs. Brasil". Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 6 de julio de 2009. Serie C No. 200.

729 Ficha Técnica: "Kimel vs. Argentina", consultado el 21 de agosto de 2018. Disponible en: http://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=291

730 Voto concurrente del Juez Diego García-Sayán en Corte IDH. Caso "Kimel vs. Argentina". Fondo, reparaciones y costas. Sentencia de 2 de mayo de 2008. Serie C. No. 177, párr. 13.

Sobre el concepto de honor, la Corte IDH realiza una importante precisión sobre el denominado "honor objetivo" y señala que tiene que ver con "[…] el valor que los demás le asignan a la persona en cuestión en tanto se afecte la buena reputación o la buena fama de que goza una persona en el entorno social en el que le corresponde desenvolverse. En ese orden de ideas, dentro del marco jurídico de la vigencia del derecho al honor, la libertad de expresión como derecho fundamental no sustenta ni legitima frases y términos manifiestamente injuriosos y que vayan más allá del legítimo ejercicio del derecho a opinar o el ejercicio de la crítica".[731]

Este caso es relevante, ya que al realizar un análisis de los límites a la libertad de expresión, en la Tesis: 1a./J. 38/2013 (10a.), la SCJN ha destacado la adopción del denominado "sistema dual de protección", según el cual, los límites de la crítica son más amplios cuando se refiere a personas que, por dedicarse a actividades públicas o por el rol que desempeñan en una sociedad democrática, están expuestas a un control más riguroso de sus actividades y manifestaciones que aquellos particulares sin proyección pública alguna, pues en un sistema inspirado en los valores democráticos, la sujeción a esa crítica es inseparable de todo cargo de relevancia pública. Sobre este tema, la Primera Sala de la SCJN puntualiza que la Corte Interamericana de Derechos Humanos precisó, en los casos "Herrera Ulloa vs. Costa Rica" y "Kimel vs. Argentina", que el acento de este umbral diferente de protección no se asienta en la calidad del sujeto, sino en el carácter de interés público que conllevan las actividades o actuaciones de una persona determinada.

Esta aclaración es fundamental en tanto que las personas no estarán sometidas a un mayor escrutinio de la sociedad en su honor o privacidad durante todas sus vidas, sino que dicho umbral de tolerancia deberá ser mayor solamente mientras realicen funciones públicas o estén involucradas en temas de relevancia pública. Esto no significa que la proyección pública de las personas las prive de su derecho al honor, sino simplemente que el nivel de intromisión admisible será mayor, aunque dichas intromisiones deben estar relacionadas con aquellos asuntos que sean de relevancia pública. La principal consecuencia del sistema de protección dual es la doctrina conocida como "real malicia" o "malicia efectiva", misma que ha sido incorporada al ordenamiento jurídico mexicano. Esta doctrina se traduce en la imposición de sanciones civiles exclusivamente en aquellos casos en que exista información falsa (en caso del derecho a la información) o que haya sido producida con "real malicia" (aplicable tanto al derecho a la información como a la libertad de expresión). El estándar de "real malicia" requiere, para la existencia de una condena por daño moral por la emisión de opiniones, ideas o juicios, que hayan sido expresados con la intención de dañar, para lo cual, la nota publicada y su contexto constituyen las pruebas idóneas para acreditar dicha intención.[732]

En este sentido, la Primera Sala de la SCJN observa que, dependiendo de su gravedad y de la calidad del sujeto pasivo, las intromisiones al derecho al honor pueden ser sancionadas con: (i) sanciones penales, en supuestos muy limitados, referentes principalmente a intromisiones graves contra particulares; (ii) con sanciones civiles, para intromisiones graves en casos de personajes públicos e intromisiones medias contra particulares y (iii) mediante el uso del derecho de réplica o respuesta, cuyo reconocimiento se encuentra,

731 Voto concurrente del Juez Diego García-Sayán en Corte IDH. Caso "Kimel vs. Argentina". Fondo, reparaciones y costas. Sentencia de 2 de mayo de 2008 Serie C. No. 177, párr. 16.

732 Tesis: 1a./J. 38/2013 (10a.). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro XIX. Abril de 2013. Tomo 1, p. 538.

tanto en el texto constitucional como en la Convención Americana sobre Derechos Humanos, para intromisiones no graves contra personajes públicos e intromisiones leves contra personas privadas.[733]

En esta misma sintonía, la Primera Sala de la SCJN ha destacado que existen una serie de derechos destinados a la protección de la vida privada, entre ellos el del honor, que es un bien objetivo que permite que alguien sea merecedor de estimación y confianza en el medio social donde se desenvuelve y, por ello, cuando se vulnera dicho bien, también se afectan la consideración y estima que los demás le profesan, tanto en el ámbito social como en el privado. En esa tesitura, se concluye que cuando se lesiona el honor de alguien con una manifestación o expresión maliciosa, también se afecta su vida privada.[734]

F. Caso "Mémoli vs. Argentina"

El caso "Mémoli vs. Argentina" se refiere a la alegada violación al derecho a la libertad de expresión de los señores Carlos y Pablo Mémoli por la condena penal que se les impuso debido a sus denuncias públicas sobre la venta (supuestamente irregular) de nichos del cementerio local por parte de la Comisión Directiva de una asociación mutual de la ciudad de San Andrés de Giles. Asimismo, el caso se relaciona con la violación a la garantía de plazo razonable en perjuicio de las presuntas víctimas en el marco del proceso civil que se sigue en su contra y mediante el cual, desde hace más de 15 años, se pretende hacer valer una indemnización establecida en el proceso penal.[735]

A diferencia de los casos precedentes donde el derecho del honor fungió como una limitante del derecho a la libertad de expresión, la Corte IDH consideró que en efecto había existido una afectación del derecho al honor que podría dar lugar a una persecución judicial. La Corte IDH señaló lo siguiente: “137. En el presente caso, no se presenta una situación similar a la del caso Kimel ya que era suficientemente previsible que ciertas expresiones y calificaciones utilizadas por los señores Mémoli (en las que acusan a los querellantes como posibles autores o encubridores del delito de estafa, los califican como ‘delincuentes’, ‘inescrupulosos’, ‘corruptos’ o que ‘se manejan con tretas y manganetas’, entre otras) podrían dar lugar a una acción judicial por alegada afectación al honor o la reputación de los querellantes”.[736]

El caso fue resuelto por cuatro votos a favor y tres en contra.[737] El criterio mayoritario de los jueces destacó que las informaciones contenidas en las expresiones de los señores Mémoli no eran de “interés público”, para ello se basaron en que no involucraban a funcionarios o figuras públicas[738] ni versaban sobre el funcionamiento de las instituciones

733 Tesis: 1a./J. 38/2013 (10a.). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro XIX. Abril de 2013. Tomo 1, p. 538.

734 Tesis: 1a. CXLVIII/2007. *Novena época. Semanario Judicial de la Federación y su Gaceta*. Tomo XXVI. Julio de 2007, p. 272.

735 Ficha técnica "Mémoli vs. Argentina". consultado el 21 de agosto de 2018, disponible en: http://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=375&lang=e

736 Corte IDH. Caso "Mémoli vs. Argentina" Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 22 de agosto de 2013. Serie C. No. 265, párr. 137.

737 Véase: Corte IDH. *El Voto conjunto parcialmente disidente de los jueces Manuel E. Ventura Robles, Eduardo Vío Grossi y Eduardo Ferrer Mac-Gregor Poisot*. Caso "Mémoli vs. Argentina". Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 22 de agosto de 2013. Serie C. No. 265.

738 Por ejemplo, en los casos de la CIDH: Caso *Herrera Ulloa vs. Costa Rica*, Serie C No. 107, párr. 124; Caso "Ricardo Canese vs. Paraguay", Serie C No. 111, párr. 91 a 94; Caso "Kimel vs. Argentina", Serie C No. 177, párr. 51; Caso "Tristán Donoso vs. Panamá", Serie C No. 193, párr. 93 y 115 y caso "Fontevecchia y D`Amico vs. Argentina", Serie C No. 238 párr. 62.

del Estado,[739] pues se habrían producido en el contexto de un conflicto entre personas particulares sobre asuntos que, eventualmente, solo afectarían a los miembros de una asociación mutual de carácter privado.[740]

En contraposición, el criterio minoritario consideró que "a fin de poder determinar si el caso en comento involucra o no un asunto de interés público, es indispensable considerar, no si el litigio interno era entre particulares, pues, prácticamente todos lo son, sino el contexto en que se emitieron las declaraciones en comento y, muy especialmente el lugar en que se dieron, es decir, San Andrés de Giles. Y es que a la fecha en que aquellas se emitieron, dicha localidad que tenía una población de alrededor de dieciocho mil habitantes y aproximadamente trescientos de ellos eran socios de la ya citada asociación italiana. Asimismo, procede valorar que los mencionados hechos se referían al ilícito contrato de nichos del cementerio municipal de tal pueblo o ciudad. Por tanto, lógicamente se concluye que resulta evidente que una proporción significativa de la población a la que estaban dirigidas las publicaciones en comento, tenía un legítimo interés de conocer las informaciones que contenían, puesto que no solo les concernían, sino que, además, porque se referían a un bien público o de la comunidad, de suyo muy relevante en su historia y en su conformación cultural como tal". En ese sentido, los jueces de la minoría consideraron que "sin la menor duda que tales informaciones trascendían a la citada asociación y, por lo tanto, eran de notorio o patente interés público".[741]

Partiendo de que la mayoría de las informaciones contenidas en las expresiones de los señores Mémoli no eran de interés público, en la sentencia se estima que:

> 143. Al respecto, la Corte toma nota de que las autoridades judiciales argentinas actuantes en el presente caso realizaron un examen de las expresiones de los señores Mémoli y su incidencia en el honor y la reputación de terceras personas. A juicio de este Tribunal, dicho examen constituyó una ponderación razonable y suficiente entre ambos derechos en conflicto, que justificaba el establecimiento de responsabilidades ulteriores en su perjuicio. Dada la naturaleza del procedimiento ante la Corte, los particulares cuyo honor y reputación habrían sido afectados no han tenido participación en el mismo. Por tanto, este Tribunal considera que en el presente caso las autoridades judiciales internas estaban en mejor posición para valorar el mayor grado de afectación en un derecho u otro. Este Tribunal resalta que las expresiones calificadas como injuriosas fueron publicadas en un medio que llegaba a muchas más personas que a los miembros de la Asociación Mutual, por lo cual el honor y la reputación de los querellantes se vio posiblemente afectado ante una audiencia mucho mayor a aquélla que podía verse beneficiada por dicha información. Además, teniendo en cuenta que las autoridades judiciales internas concluyeron que ciertos calificativos empleados por los señores Mémoli lesionaron innecesariamente la reputación de los querellantes, la Corte observa que el establecimiento de responsabilidades ulteriores en el presente caso constituye el cumplimiento por parte del Estado de la obligación establecida en el artículo 11.3 de la Convención, por la cual debe proteger a las personas contra ataques abusivos a su honra y su reputación (Sentencia de 22 de agosto de 2013. Serie C. No. 265. párr. 125 y 138).[742]

739 Tales como el Comité de Inversiones Extranjeras, en el Caso "Claude Reyes y otros vs. Chile". Fondo, reparaciones y costas. Sentencia de 19 de septiembre de 2006. Serie C No. 151, párr. 73, o las Fuerzas Armadas, en el Caso "Vélez Restrepo y Familiares vs. Colombia", Serie C No. 248, párr. 145.

740 Párrafos 145 a 149 de la Sentencia.

741 Véase: Corte IDH. *El Voto conjunto parcialmente disidente de los jueces Manuel E. Ventura Robles, Eduardo Vío Grossi y Eduardo Ferrer Mac-Gregor Poiso.* Caso "Mémoli vs. Argentina". Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 22 de agosto de 2013. Serie C. No. 265.

742 Corte IDH. Caso "Mémoli vs. Argentina". Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 22 de agosto de 2013. Serie C. No. 265, párr. 143.

En sentido contrario, el criterio minoritario estimó que "esa ponderación no es realizada de acuerdo con lo dispuesto en el artículo 13 de la Convención, sino evidentemente acorde al derecho interno del Estado". A este respecto, es necesario reiterar que el asunto a resolver en autos es si el juez penal nacional, al conocer y fallar en este asunto, realizó un correcto control de convencionalidad sobre la necesidad de las responsabilidades para asegurar el respeto a los derechos o a la reputación de los demás, es decir, no si se aplicó correctamente la sanción penal conforme al derecho interno del Estado, sino si lo hizo de acuerdo con lo previsto en el artículo 13 de la Convención. Y ello no ocurrió así.[743] La minoría consideró que "en realidad, el juez interno ni siquiera realizó una ponderación razonable y suficiente entre los derechos al honor y reputación de los querellantes y la libertad de expresión de los señores Mémoli, sino que sencillamente, considerando que "la libertad de prensa […] no puede amparar, […] a quienes la invocan y con su accionar lesionan derechos de terceros que también merecen amparos", dio preeminencia a los primeros por sobre la segunda, sin examinar las circunstancias particulares del caso ni fundamentar esa opción.[744]

Por último, debe destacarse el criterio de la SCJN en la tesis 1a./J. 32/2013 (10a.), donde la relación entre la libertad de expresión y los derechos de la personalidad como el honor, se complica cuando se ejerce para criticar a una persona de forma tal que ésta se sienta agraviada. La complejidad radica en que el Estado no puede privilegiar un determinado criterio de decencia, estética o decoro respecto a las expresiones que podrían ser bien recibidas, ya que no existen parámetros uniformemente aceptados que puedan delimitar el contenido de estas categorías y constituyen limitaciones demasiado vagas de la libertad de expresión como para ser constitucionalmente admisibles. De hecho, el debate en temas de interés público debe ser desinhibido, robusto, abierto y puede incluir ataques vehementes, cáusticos y desagradablemente mordaces sobre personajes públicos o, en general, ideas que puedan ser recibidas desfavorablemente por sus destinatarios y la opinión pública, de modo que no solo se encuentran protegidas las ideas que son recibidas favorablemente o las que son vistas como inofensivas o indiferentes. Estas son las demandas de una sociedad plural, tolerante y abierta, sin la cual no existe una verdadera democracia.[745]

Derecho al olvido

Isabel Davara Fernández de Marcos,
Gregorio Barco Vega y
Alexis Cervantes Padilla

En nuestro ordenamiento jurídico, el conocido comercialmente como derecho al olvido se consagra de dos maneras:

a) de manera genérica respecto de cualquier tipo de datos personales sobre los que el titular solicite el cese del tratamiento y[746]

743 Véase: Corte IDH. *El Voto conjunto parcialmente disidente de los jueces Manuel E. Ventura Robles, Eduardo Vío Grossi y Eduardo Ferrer Mac-Gregor Poisot. Caso Mémoli vs. Argentina. Excepciones preliminares, fondo, reparaciones y costas*. Sentencia de 22 de agosto de 2013. Serie C No. 265.

744 Véase: Corte IDH. *El Voto conjunto parcialmente disidente de los jueces Manuel E. Ventura Robles, Eduardo Vío Grossi y Eduardo Ferrer Mac-Gregor Poisot. Caso Mémoli vs. Argentina. Excepciones preliminares, fondo, reparaciones y costas*. Sentencia de 22 de agosto de 2013. Serie C. No. 265.

745 Tesis: 1a./J. 32/2013 (10a.). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro XIX. Abril de 2013. Tomo 1, p. 540.

746 Recomendamos consultar las definiciones de derecho de cancelación y derecho de oposición que forman parte de este *Diccionario de Protección de Datos Personales*.

b) de manera específica, para aquellos datos relacionados con el incumplimiento de obligaciones contractuales. El derecho al olvido aplicado a lo que en otras latitudes se conoce como "*habeas data* financiero" encuentra cabida en el tercer párrafo del artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que indica: "El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento".[747] En este mismo orden de ideas, la Ley para Regular las Sociedades de Información Crediticia proscribe que dichas instituciones inscriban créditos que tengan una antigüedad en cartera vencida mayor a 72 meses.[748] Conforme a lo anterior, puede decirse que la finalidad de este derecho, en el ámbito financiero, es establecer la obligación de los responsables de la base de datos de eliminar los datos personales después de un plazo razonable posterior a que se presente algún incumplimiento para reforzar el derecho a la intimidad y a la protección de datos personales.

Refiriéndonos a la faceta más moderna del derecho al olvido, debe decirse que esta variante jurídica surge como resultado de la necesidad de garantizar el derecho a la protección de datos personales frente a la existencia y difusión de información en internet que pudiera afectar al titular.

En concreto, esta denominación se ha asociado popularmente con los tratamientos de datos personales por motores de búsqueda en internet,[749] en particular cuando la información arrojada por esta poderosa herramienta resulta desactualizada, inexacta, no relevante y/o excesiva.

El derecho al olvido en internet adquirió notoriedad en el ámbito internacional a partir del llamado "caso Google" donde la sentencia C131/12[750] del Tribunal de Justicia de la Unión Europea (TJUE), entre otras cosas, consideró que la indexación[751] por medio de un algoritmo y bajo determinados criterios de búsqueda de información asociada con una persona física identificada o identificable, constituye un tratamiento de datos personales sujeto a la normatividad, reconociéndole a un ciudadano español el ejercicio de los derechos de oposición y cancelación de datos personales respecto a la indexación por su nombre en el motor de búsqueda Google.[752]

747 Artículo 11 de la ley Federal de Protección de Datos Personales en Posesión de los Particulares.

748 Artículo 20. La base de datos de las Sociedades se integrará con la información sobre operaciones crediticias y otras de naturaleza análoga que le sea proporcionada por los usuarios. Los usuarios que entreguen dicha información a las sociedades deberán hacerlo de manera completa y veraz; asimismo, estarán obligados a señalar expresamente la fecha de origen de los créditos que inscriban y la fecha del primer incumplimiento. Las sociedades no deberán inscribir por ningún motivo, créditos cuya fecha de origen no sea especificada por los usuarios, o cuando éste tenga una antigüedad en cartera vencida mayor a 72 meses. Lo anterior, de conformidad con lo establecido en los artículos 23 y 24 de esta Ley.

749 El Grupo de Trabajo del Artículo 29 ha estudiado el tema del tratamiento de datos personales por parte de motores de búsqueda en el dictamen 1/2008 emitido el 4 de abril de 2008, sobre cuestiones de protección de datos relacionadas con motores de búsqueda.

750 Costeja, M. (2014, mayo 13). *Sentencia del Tribunal de Justicia de la Unión Europea en el asunto C131/12.* Agencia Española de Protección de Datos. Recuperado de: https://www.abogacia.es/wp-content/uploads/2014/05/Sentencia-131-12-TJUE-derecho-al-olvido.pdf

751 La indexación puede definirse como la acción consistente en ordenar una serie de datos o informaciones de acuerdo con un criterio común a todos ellos, para facilitar su consulta y análisis.

752 En relación con la implementación de la sentencia C131/12 por parte de las autoridades de protección de datos europeas, se puede consultar el documento del Grupo de Trabajo del Artículo 29, *Guidelines on the implementation of the Court of Justice of the European Union judgment on "*Google Spain and inc. vs. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González", adoptado el 26 de noviembre de 2014.

Así, como decíamos, aunque ha cobrado popularidad el término, en realidad es importante señalar que en este caso —contrario al explicado en primer lugar respecto a la cancelación de los datos en un buró de crédito— los datos personales no son eliminados de su fuente original (la página o páginas web que contienen esa información y que el motor de búsqueda muestra en su listado de resultados). Es decir, el motor de búsqueda únicamente deja de indexar[753] dentro del listado de resultados aquellos datos que tengan que ver con el nombre de una persona física identificada o identificable. Es por esto que se habla del derecho a ser retirado del listado de resultados del buscador (*to delist* en inglés) o derecho a dejar de ser indexado.

En puridad, este derecho no es una novedad, ni autónomo, sino una manifestación de los derechos de oposición y cancelación, y en particular en ciertos proveedores de servicios de internet. Vale la pena destacar que, con base en la normatividad nacional que reconoce los derechos antes citados, puede ejercerse este derecho ante cualquier responsable que lleve a cabo el tratamiento de datos, incluyendo los motores de búsqueda y cualquier prestador de servicios de internet que se encuentren sujetos a la jurisdicción competente y ley aplicable.

Por esta razón, el Reglamento General de Protección de Datos (RGPD) titula su artículo 17 "Derecho de supresión" (el derecho al olvido) y lo individualiza,[754] pues si bien tiene un alcance bastante similar al que puede atribuirse a los derechos de cancelación y oposición en internet, comprende información desactualizada, inexacta, no relevante y excesiva cuya divulgación pudiera afectar los derechos subjetivos del titular de los datos, previendo los siguientes supuestos específicos:

a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados.
b) El titular retire el consentimiento en que se basa el tratamiento.
c) El titular se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento para fines de mercadotecnia directa.
d) Los datos personales hayan sido tratados ilícitamente.
e) Los datos personales deban suprimirse para el cumplimiento de una obligación legal.
f) Los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.

Por otro lado, el citado artículo 17 del Reglamento General de Protección de Datos (RGPD o GDPR por sus silgas en inglés) establece también que este derecho no procederá cuando

753 Según el *Diccionario de la Lengua Española*, la palabra indexar significa: registrar ordenadamente datos e informaciones, para elaborar su índice. *Vid*, *Diccionario de la Real Academia Española* en: http://dle.rae.es/?id=LNTIjYS

754 En este contexto, el considerando 65 del Reglamento General de Protección de Datos dispone lo siguiente:
"(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho, aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones".

el tratamiento sea necesario para ejercer el derecho a la libertad de expresión e información, el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, por razones de interés público, fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos en la medida en que el derecho indicado pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento y para la formulación, el ejercicio o la defensa de reclamaciones.[755]

En términos prácticos esta vertiente de este derecho ahora analizada encontrará cumplimiento cuando el responsable, una vez analizada la procedencia de la solicitud del titular, deje de indexar determinada información personal asociada con el titular. En términos del referido RGPD, además, los responsables que hayan hecho públicos los datos personales deberán adoptar medidas razonables, incluidas medidas técnicas para informar a los responsables que estén tratando los datos personales de la solicitud del titular de cualquier enlace a esos datos personales, copia o réplica de los mismos.[756]

Además, cualquiera que sea la causa para el ejercicio del derecho de supresión, el responsable debe cuidar que la retención de los datos personales sea lícita.[757] Esto es, que los datos personales sean conservados exclusivamente cuando dicha acción sea requerida para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica, fines estadísticos o para la formulación, el ejercicio o la defensa de reclamaciones.[758]

Concluimos esta breve exposición reiterando que este derecho solo afecta a los resultados obtenidos de búsquedas hechas con el nombre de la persona y no requiere la eliminación del enlace de los índices del motor de búsqueda completamente.[759] Además, reiteramos que la fuente no se borra, sino que se deja de "indexar" la información con el criterio de búsqueda de su nombre propio.

En definitiva, este derecho se refiere una aplicación concreta de las obligaciones de los ya tradicionales derechos de cancelación y oposición ante escenarios bastante específicos, por ejemplo, cuando se han extinguido las finalidades que justificaban su tratamiento (el caso de la información crediticia) o bien porque el titular ha revocado su consentimiento o ejercido su derecho de oposición (caso de proveedores de servicios de internet en particular).

755 Considerando 65 y artículo 17, apartado 2 del Reglamento General de Protección de Datos.

756 En este contexto, el considerando 66 del Reglamento General de Protección de Datos dispone lo siguiente:
"(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales".

757 Una situación particular que el RGPD regula es el ejercicio de este derecho cuando el titular de los datos dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. De este modo, se dispone que el titular se encuentra facultado para poder ejercer este derecho, aunque ya no sea un niño. *Vid*. Considerando 65 del Reglamento General de Protección de Datos.

758 Considerando 65 del Reglamento General de Protección de Datos.

759 Aunque todavía hay algunas dudas al respecto, si bien puede entenderse como procedente en el dominio referente al país de origen, en la práctica podría incluir también todos los dominios relevantes, incluyendo .com.

Derechos ARCO

Sofía Gómez Ruano

Son aquellos derechos referidos en algunos países de habla hispana (entre ellos México y España) con el acrónimo ARCO y que corresponde a los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.[760] Los derechos ARCO son una garantía del derecho de autodeterminación de las personas como titulares de datos personales que les permite mantener el control y disponer de sus datos personales frente a los responsables pertenecientes al sector público y al privado.

En México, los derechos ARCO son reconocidos como una garantía individual en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) que dispone: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, […]." El marco normativo aplicable al sector público que es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LFPDPPSO)[761] y el correspondiente al sector privado que es la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[762] establecen la forma, los requisitos, los medios y los procedimientos a través de los cuales se pueden ejercer los derechos ARCO. Derivan del derecho humano a la protección de los datos personales, por lo que comparten con éste las características de ser intransferibles, irrenunciables y universales.

Estos derechos no son los únicos de los titulares de datos personales. La LGPDPPSO les reconoce también el derecho de portabilidad de datos personales, el cual se estima en un futuro cercano sea también contemplado por la legislación aplicable al sector privado.

En el ámbito internacional, instrumentos como los Estándares Iberoamericanos de Protección de Datos (Estándares Iberoamericanos) y el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) reconocen también los derechos de acceso, rectificación, cancelación y oposición sobre el tratamiento de los datos personales con ciertas particularidades.

Los Estándares Iberoamericanos reconocen, adicionalmente, el derecho de portabilidad, el derecho de no ser objeto de decisiones individuales automatizadas y el de limitación del tratamiento de los datos personales. Mientras que el RGPD buscó ampliar los derechos con los que cuentan los titulares por lo que prevé derechos más amplios, entre los que están el derecho a la portabilidad de los datos, el derecho de limitación del tratamiento, equiparable al derecho de cancelación y dentro del que se incluye el derecho al olvido y a no ser sujeto de decisiones individuales incluida la elaboración de perfiles. El Convenio 108, por su parte, considera a los derechos ARCO como garantías complementarias para la persona. Por tanto, el Consejo Consultivo del Convenio 108 revisó que los derechos ARCO estuvieran contemplados por la legislación mexicana para invitar a México a ser parte de esa convención.

Los responsables de los datos personales deben prepararse para estar en posibilidad de atender las solicitudes de derechos ARCO. Dentro de las acciones que deben realizar están, entre

760 De esa manera define el término "derechos ARCO" la LGPDPPSO (artículo 3 fracción XI) y el Reglamento de la LFPDPPP (artículo 2 fracción II).

761 La LGPDPSO (título tercero) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (título tercero).

762 Artículo 22 de la LFPDPPP y su reglamento (capítulo VII).

otras, almacenar y organizar los datos personales, así como establecer procesos que les permita responder a las solicitudes ARCO en los plazos previstos por la normativa mexicana.

1. El carácter personalísimo de los derechos ARCO

Los derechos ARCO son personalísimos por lo que por regla general, únicamente pueden ejercerse por la persona a quien le conciernen los datos personales, ya sea directamente o a través de un representante. Para el ejercicio de los derechos ARCO es necesario que el titular de los datos personales acredite su identidad, así como, de ser el caso, la identidad y personalidad de su representante. Para tal efecto, es obligación del responsable informar a los titulares a través de su aviso de privacidad los medios para el ejercicio de los derechos ARCO, mismos que según lo previsto por los Lineamientos del Aviso de Privacidad[763] incluyen los mecanismos de acreditación de la identidad del titular y la personalidad de su representante, así como la información o documentación que el titular y/o su representante deben acompañar a la solicitud.

La identidad del titular se puede acreditar de las siguientes maneras: (i) presentando copia de su documento de identificación habiendo exhibido el original para su cotejo,[764] (ii) a través de instrumentos electrónicos por los cuales sea posible identificarlo fehacientemente o (iii) a través de otros mecanismos de autenticación permitidos por las disposiciones legales o que hayan sido establecidos por el responsable. En caso de que el titular utilice su firma electrónica avanzada o el instrumento electrónico que la sustituya, no será necesario que presente alguna otra identificación.

Si la solicitud se presenta a través de un representante legal, éste tendrá la obligación de acreditar (i) la identidad del titular, (ii) su identidad y (iii) el mandato que se le ha otorgado mediante instrumento público, carta poder firmada ante dos testigos[765] o la declaración en comparecencia personal del titular.

El ejercicio de los derechos ARCO por parte de menores de edad y personas en estado de interdicción o incapacidad debe realizarse teniendo en cuenta las reglas de representación previstas en la legislación civil y la demás que resulte aplicable. En el caso de personas fallecidas, la normativa mexicana para el sector privado es omisa, mientras que la LGPDPPSO dispone que podrá ejercer los derechos ARCO "la persona que acredite tener un interés jurídico, […], siempre que el titular de los derechos haya expresado fehacientemente su voluntad en tal sentido o exista un mandato judicial para dicho efecto. En caso de que la persona fallecida no hubiere expresado fehacientemente su voluntad […] bastará que quien pretende ejercer los derechos ARCO acredite su interés jurídico […]".[766]

763 Artículo 28.

764 El artículo 76 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público establece que la identificación deberá ser oficial.

765 Según lo dispuesto por los Lineamientos Generales de Protección de Datos Personales para el Sector Público habrá también que anexar copia simple de las identificaciones de quienes suscriban la carta poder.

766 Los Lineamientos Generales Para el Sector Público (artículo 75) definen el interés jurídico como: "Aquél que tiene una persona física que, con motivo del fallecimiento del titular, pretende ejercer los derechos ARCO de éste, para el reconocimiento de derechos sucesorios, atendiendo a la relación de parentesco por consanguinidad o afinidad que haya tenido con el titular, el cual se acreditará en términos de las disposiciones legales aplicables. Puede alegar interés jurídico, de manera enunciativa mas no limitativa, el albacea, herederos, legatarios, familiares en línea recta sin limitación de grado y en línea colateral hasta el cuarto grado, lo que se acreditará con copia simple del documento delegatorio, pasado ante la fe de notario público o suscrito ante dos testigos. En el supuesto de que el titular sea un menor de edad, el interés jurídico se acreditará con la copia del acta de defunción del menor, el acta de nacimiento o identificación del menor, así como la identificación de quien ejercía la patria potestad y/o tutela. En el supuesto de que el titular sea una persona en estado de interdicción o incapacidad declarada por ley o por autoridad judicial, el interés jurídico se acreditará con la copia de su acta de defunción, el documento de su identificación oficial y de quien ejercía la tutela, así como el instrumento legal de designación del tutor".

Los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) detallan la documentación que se deberá presentar en cada caso para acreditar la identidad y personalidad del representante.[767]

La necesidad de identificar al titular para el ejercicio de sus derechos, es también un requerimiento presente en el RGPD que exige a los responsables utilizar todos los medios razonables para verificar la identidad del titular. Si el responsable tiene dudas razonables sobre la identidad, puede solicitar al titular información adicional. Este ordenamiento prevé también un supuesto diferente, que se presenta cuando, en razón de los fines para los cuales se realiza el tratamiento de los datos personales, el responsable no ha tenido que mantener, obtener o tratar información adicional del titular para identificarlo, y consecuentemente no está en condiciones de identificarlo. En esos casos será necesario que el titular presente información adicional para su identificación.[768]

2. Los derechos ARCO son independientes y pueden ejercerse en cualquier momento

Los titulares de los datos personales tienen el derecho fundamental a ejercer sus derechos ARCO en cualquier momento, sin que el ejercicio de cualquiera de estos sea requisito previo, impida o excluya la posibilidad del ejercicio de otro de los derechos ARCO, por tratarse de derechos independientes. Así se reconoce en el marco jurídico nacional para el sector privado y para el sector público, y a nivel internacional.[769]

3. Gratuidad del ejercicio de los derechos ARCO

Por regla general, el ejercicio de los derechos ARCO es gratuito. El carácter gratuito es aplicable a la presentación de las solicitudes de derechos ARCO, la comunicación de la respuesta a esas solicitudes por parte del responsable y a las acciones necesarias para hacer efectiva la determinación que el responsable haya tomado en la respuesta, es decir, en general a todo el procedimiento de atención de derechos ARCO. Sin embargo, existen ciertos supuestos en los que se autoriza al responsable de los datos personales a realizar un cobro por algunos de esos conceptos.

Por lo que hace a la presentación de las solicitudes de derechos, en el sector privado, se otorga al responsable la posibilidad de establecer servicios o medios con costo para la presentación de las solicitudes de derechos ARCO, siempre y cuando no sean los únicos, es decir, el responsable ofrezca también algún servicio o medio gratuito.[770] Adicionalmente, el responsable tiene la posibilidad de fijar un costo para el ejercicio de los derechos ARCO en caso de que el titular reitere su solicitud respecto a los mismos datos en un periodo menor a 12 meses, siempre que no existan modificaciones sustanciales en el tratamiento que motiven la nueva solicitud y sujeto a que esos costos no rebasen tres veces el salario mínimo general vigente.

En el sector público, por el contrario, existe una prohibición expresa para establecer algún servicio o medio para el ejercicio de los derechos ARCO que implique un costo para el titular.[771]

En cuanto a las acciones que deberá emprender el responsable para hacer efectivo el derecho solicitado, la normativa pública y privada coinciden en permitirle el cobro al

767 Artículos 78, 79, 80, 81 y 82 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

768 Artículo 11 y 12.6 del Reglamento General de Protección de Datos Personales.

769 Artículo 22 de la LFPDPPP, artículo 87 del Reglamento de la LFPDPPP, artículo 43 de la LGPDPPSO y el artículo 24 de los Estándares Iberoamericanos de Protección de Datos.

770 Artículo 93 del Reglamento de la LFPDPPP.

771 Artículo 50 de la LGPDPPSO.

titular para recobrar gastos por concepto de reproducción, certificación y envío[772] de la información solicitada. En el sector privado, los costos de reproducción están limitados al costo de recuperación del material correspondiente[773] mientras que la normativa del sector público remite a las leyes que resulten aplicables, con la salvedad de que no existirá costo cuando (i) la entrega no implique más de 20 hojas simples o por las primeras 20 hojas en caso de ser un documento más extenso,[774] (ii) las unidades de transparencia exceptúen el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular considerando lo manifestado por el titular en su solicitud o (iii) en caso de que el titular haya proporcionado el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales.[775] En el sector público, los responsables deberán dar a conocer al titular los costos de reproducción, certificación y/o envío así como el plazo para su pago en la respuesta a la solicitud.[776]

4. El obligado a atender las solicitudes de derechos ARCO

El responsable del tratamiento de los datos personales es el obligado a atender las solicitudes de derechos ARCO. Para tal efecto, el responsable, si se trata de un particular, debe designar a una persona o departamento de datos personales para dar trámite a las solicitudes de derechos ARCO. Lo anterior, en el entendido de que el marco normativo mexicano para el sector privado,[777] permite que el responsable tercerice esta función a través de un encargado debiendo documentar la relación entre ambos de tal manera que sea posible acreditar la existencia, alcance y contenido de la misma.

En caso de que el responsable sea un sujeto obligado, éste deberá tramitar las solicitudes de derechos ARCO a través de su unidad de transparencia. La LGPDPPSO prevé la posibilidad de que los responsables designen a un oficial de protección de datos personales, especializado en la materia, que forme parte de esa unidad de transparencia y quien, dentro de otras funciones, gestione las solicitudes de ejercicio de los derechos ARCO. [778]

En cumplimiento del principio de información, el responsable debe dar a conocer al titular los medios para el ejercicio de los derechos ARCO.[779] El responsable del tratamiento

772 Artículo 50 de la LGPDPPSO.

773 Artículo 93 del Reglamento de la LFPDPPP.

774 Artículo 89 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

775 Artículo 50 de la LGPDPPSO.

776 Artículo 90 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

777 Artículo 30 de la LFPDPPP:

778 Artículo 85 de la LGPDPPSO.

779 Los Lineamientos del Aviso de Privacidad, artículo vigésimo octavo: "De acuerdo con lo previsto en los artículos 16, fracción IV y 33 de la Ley, y 90 y 102 de su Reglamento, el aviso de privacidad deberá informar al titular sobre:
I. Los medios habilitados por el responsable para atender las solicitudes de ejercicio de derechos ARCO, los cuales deberán implementarse de forma tal que no se limite el ejercicio de estos derechos por parte de los titulares; [...]
II. Los procedimientos establecidos para el ejercicio de los derechos ARCO; o bien, los medios a través de los cuales el titular podrá conocer dichos procedimientos, los cuales deberán ser de fácil acceso para los titulares y con la mayor cobertura posible, considerando su perfil y la forma en que mantienen contacto cotidiano o común con el responsable; gratuitos; que estén debidamente habilitados, y que hagan sencillo el acceso a la información. Los datos de identificación y contacto de la persona o departamento de datos personales que dará trámite a las solicitudes de los titulares para el ejercicio de los derechos ARCO, al que refiere el artículo 30 de la Ley.
Los procedimientos a los que refiere la fracción II del presente lineamiento deberán incluir, al menos, lo siguiente:
a) Los requisitos, entre ellos, los mecanismos de acreditación de la identidad del titular y la personalidad de su representante, y la información o documentación que se deberá acompañar a la solicitud;
b) Los plazos dentro del procedimiento;

tendrá en todo momento la carga de la prueba del cumplimiento de la obligación de responder tanto en el sector privado, en caso de iniciarse un procedimiento de protección de derechos, como en el sector público, de presentarse un recurso de revisión, por lo que es aconsejable conserve la evidencia que lo acredite.[780]

5. El procedimiento y los requisitos para el ejercicio de los derechos ARCO

Los requisitos de las solicitudes de derechos ARCO: el responsable debe dar a conocer al titular de los datos personales los requisititos mínimos que debe cumplir una solicitud de derechos ARCO (solicitudes ARCO) en el aviso de privacidad, pudiendo poner a disposición de los titulares formularios, sistemas u otros métodos simplificados para facilitar al titular el ejercicio de sus derechos en tiempo, forma y fondo.

La LFPDPPP[781] y la LGPDPPSO[782] establecen los siguientes requisitos que deberán reunir las solicitudes ARCO, así como la documentación que se deberá acompañar a las mismas:

(i) el nombre del titular, que permite identificar a la persona que ejerce el derecho y quien en consecuencia tendrá que acreditar su identidad;

(ii) el domicilio u otro medio para que el responsable pueda comunicar la respuesta al titular, siendo común que los responsables soliciten una dirección de correo electrónico para economizar y hacer más eficiente la comunicación;

(iii) los documentos que acrediten la identidad del titular[783] y que permitirán al responsable cumplir con su obligación de cerciorarse de la identidad del titular. En caso de presentar la solicitud a través de un representante legal, los documentos que acrediten su personalidad. Como se señaló anteriormente, en los casos en que los titulares sean menores de edad o personas en estado de interdicción o incapacidad, para su representación se estará a lo previsto por la legislación civil y la demás que resulte aplicable. Por otra parte, cuando la solicitud de derechos ARCO concierna a una persona fallecida, el solicitante deberá acreditar tener interés jurídico siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto. Los Lineamientos Generales de Protección de Datos Personales para el Sector Público prevén a detalle esos supuestos;[784]

(iv) En caso de que el responsable sea un sujeto obligado, de conformidad con la LGPDPPSO, de ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;

(v) la descripción clara y precisa de los datos personales respecto de los que se busca ejercer el derecho, salvo que se trate del derecho de acceso y

---

c) Los medios para dar respuesta;
d) La modalidad o medio de reproducción mediante la cual el titular podrá obtener la información o datos personales solicitados a través del ejercicio del derecho de acceso, es decir, copias simples, documentos electrónicos o cualquier otro medio, y
e) Los formularios, sistemas y otros métodos simplificados que, en su caso, el responsable haya implementado para facilitar al titular el ejercicio de los derechos ARCO".

780 Al respecto ver artículo 107 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

781 Artículo 29 de la LFPDPPP.

782 Artículo 52 de la LGPDPPSO.

783 *La Guía Práctica para la Atención de las Solicitudes de Ejercicio de los Derechos ARCO* del INAI establece la posibilidad de presentar cualquiera de las siguientes identificaciones: (a) credencial del Instituto Nacional Electoral, (b) pasaporte, (c) cartilla del servicio militar nacional, (d) cédula profesional, (e) cartilla de identidad postal (expedida por Sepomex), (f) certificado o constancia de estudios, (g) constancia de residencia, (h) credencial de afiliación al IMSS, (i) credencial de afiliación al ISSTE y (j) documento migratorio que constate la legal existencia en el país.

784 Artículos 78, 79, 80, 81 y 82 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

(vi) señalar y/o acompañar cualquier otro elemento o documento que facilite la localización de los datos personales.

Adicionalmente, los Lineamientos Generales establecen que en caso de que el titular no pueda cubrir los costos de reproducción y/o envío de sus datos personales en virtud de su situación económica deberá manifestar dicha circunstancia en su solicitud. Lo anterior con la intención de que el responsable, a través de la unidad de transparencia, determine si es procedente excusar al titular del costo por dichos conceptos.[785]

La LFPDPPP establece que se tendrá por no presentada aquella solicitud ARCO que (i) no incluya un domicilio o cualquier otro medio para que sea notificada la respuesta al titular o a su representante, debiendo el responsable dejar constancia de la omisión[786] y (ii) haya sido presentada con información insuficiente o errónea, o sin acompañar la documentación necesaria, no obstante, el requerimiento de información adicional que le haya realizado el responsable.[787]

Los medios para el ejercicio de los derechos ARCO: las solicitudes de derechos ARCO deben presentarse ante el responsable. Para tal efecto, el responsable debe informar a los titulares en el aviso de privacidad[788] los medios habilitados para atender las solicitudes, pudiendo establecer medios de atención física o local (por ejemplo, ventanillas de atención) y/o remotos o a distancia, además de poner a disposición de los titulares formularios, sistemas u otros métodos que le simplifiquen la presentación de las solicitudes.[789]

En cualquier caso, el procedimiento debe ser sencillo y claro, tomando en cuenta el perfil de los titulares y la forma en que mantiene contacto cotidiano o común con el responsable, siempre siguiendo los ejes rectores previstos por la normativa y que son coincidentes en la LFPDPPP y la LGPDPPSO. Lo anterior sin perjuicio de que en caso de que las disposiciones aplicables a determinadas bases de datos o tratamientos establezcan un procedimiento específico para solicitar el ejercicio de los derechos ARCO, se estará a lo dispuesto en los que ofrezcan mayores garantías al titular, siempre y cuando no contravengan la ley.[790]

Cuando los responsables del sector privado tengan en operación servicios de atención al público y de reclamaciones pueden atender las solicitudes ARCO a través los mismos, sujeto a que los plazos de respuesta no sean mayores a los previstos por la normativa mexicana. En esos casos, la identidad del titular se considerará acreditada por los mismos medios establecidos por el responsable para la identificación de titulares en la prestación de sus servicios o contratación de sus productos, siempre que a través de dichos medios se garantice la identidad del titular.

En el sector público, las solicitudes de derechos ARCO deben presentarse ante la unidad de transparencia del responsable que el titular considere competente, mediante un escrito libre, o los formatos, medios electrónicos o cualquier otro medio que al efecto establezca el INAI o los organismos garantes. La unidad de transparencia debe auxiliar y orientar al titular en la elaboración de las solicitudes para el ejercicio de los derechos ARCO, particularmente en aquellos casos en que los titulares sean personas que no saben leer o escribir, hablen una lengua indígena o tengan alguna discapacidad.[791]

785 Artículo 83 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

786 Artículo 94 del Reglamento de la LFPDPPP.

787 Artículo 96 del Reglamento de la LFPDPPP.

788 Artículo 28 de la LGPDPPSO y artículo 16 de la LFPDPPP.

789 Según lo dispuesto por la LFPDPPP los responsables y/o encargados pueden también implementar esquemas de autorregulación vinculante para adecuar y armonizar las disposiciones previstas en la normativa mexicana a la realidad de sectores específicos, incluyendo el desarrollar e implementar procedimientos específicos para la atención de los derechos de acceso, rectificación, cancelación y oposición que sean acorde a la normativa mexicana y las buenas prácticas.

790 Artículo 92 del Reglamento de la LFPDPPP.

791 Artículo 84 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

La respuesta a las solicitudes ARCO: el acuse de recibo bajo la normativa aplicable al sector público, existe una clara obligación del responsable de acusar recibo de las solicitudes ARCO dejando constancia de la fecha de su recepción. Mientras que en el sector privado, si bien la redacción de la normativa no es muy afortunada, el responsable también está obligado a anotar en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.[792]

La obligación de responder a toda solicitud: el responsable debe dar respuesta a toda solicitud ARCO. Esta obligación es aplicable aún en aquellos casos en que el responsable considere que no es procedente la solicitud ARCO debido a que (i) no ha tenido relación alguna con el titular, (ii) no cuenta con datos personales del titular o (iii) cualquier otra causa. El incumplimiento a la obligación de dar respuesta puede actualizar, entre otros, los siguientes supuestos de infracciones previstos en la normativa mexicana para el sector privado: (i) no cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de datos personales sin razón fundada y (ii) actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

La obligación de dar respuesta a las solicitudes de derechos ARCO según lo previsto por la LFPDPPP para el sector privado, se circunscribe a contestar referente a los derechos sobre los cuales el titular expresamente ejercitó su derecho, debiendo las respuestas presentarse en un formato legible, comprensible y de fácil acceso, en que de negarse la solicitud se justifique la respuesta y se informe al titular de su derecho de iniciar un procedimiento de protección de derechos ante el INAI.[793]

La normativa aplicable al sector público establece que el responsable deberá señalar en su respuesta, (i) de ser el caso, el costo de reproducción, certificación y/o envío de los datos personales o de las constancias que acrediten el ejercicio efectivo de los derechos ARCO, (ii) el plazo con que cuenta el titular para realizar el pago correspondiente y (iii) el derecho que le asiste al titular de interponer un recurso de revisión ante el INAI en caso de no estar conforme con la respuesta recibida.[794]

El RGPD también obliga a los responsables a dar una respuesta a los titulares. En atención al derecho de transparencia en la información y comunicaciones reconocido por este ordenamiento,[795] las respuestas deberán ser concisas, transparentes, inteligibles, de fácil acceso y utilizando un lenguaje claro y simple, debiendo el responsable tener un especial cuidado cuando sean comunicaciones dirigidas a menores.

La notificación sobre la falta de competencia o la existencia de procedimientos específicos: para el sector público, la LGPDPPSO fija un plazo de tres días siguientes a la presentación de la solicitud, para que el responsable notifique al titular que no es competente para atender la solicitud ARCO, y en caso de poderlo determinar, oriente al titular sobre el responsable competente. Si el responsable fuera competente para atender parcialmente la solicitud, deberá dar respuesta sobre aquello que esté bajo su respectiva competencia.[796]

Adicionalmente, la mencionada ley prevé que de existir un trámite o procedimiento específico para solicitar el ejercicio del derecho ARCO, el responsable deberá informar al

792 Artículo 95 del Reglamento de la LFPDPPP y el artículo 52 de la LGPDPPSO.

793 Artículo 100 LFPDPPP.

794 Artículo 90 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

795 Artículo 12 del Reglamento General de Protección de Datos.

796 Artículo 100 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

respecto al titular para que éste decida si utiliza ese trámite o procedimiento específico o el procedimiento de derechos ARCO general institucionalizado. En caso de que el titular no realice manifestación alguna, conforme a lo previsto por los Lineamientos Generales,[797] se entenderá que ha elegido el procedimiento general de atención de derechos ARCO.

El requerimiento o prevención de información adicional: En caso de que la información proporcionada por el titular o su representante en la solicitud sea (i) insuficiente, (ii) errónea, (iii) poco claro (iv) no se acompañen los documentos necesarios para dar trámite a la misma, el responsable podrá requerir al titular o a su representante, dentro de los cinco días hábiles siguientes a la recepción de la solicitud, por una única vez, que aporte los elementos o documentos necesarios para dar trámite a la misma. El titular o su representante tendrán un plazo de 10 días hábiles, contados a partir del día siguiente de la recepción del requerimiento, para dar respuesta. En caso de que el titular no dé respuesta al responsable en el plazo antes señalado, o no presente la información o documentación que le haya sido requerida, su solicitud se tendrá por no presentada.

El plazo para responder a las solicitudes ARCO: la respuesta a la solicitud ARCO deberá ser comunicada al titular o a su representante, en un plazo no mayor a 20 días hábiles contados a partir de la recepción de la solicitud según la normativa del sector privado y contados a partir del día siguiente a la recepción de la solicitud conforme a la LGPDPPSO. La normativa del sector privado autoriza a los responsables a prorrogar ese plazo por un plazo igual debiendo notificar la justificación de la misma al titular dentro del plazo original para dar respuesta.[798] Los responsables del sector público, por su parte, únicamente pueden prorrogar el plazo por 10 días hábiles, es decir, la mitad de la duración del plazo original.[799]

En caso de haberle solicitado al titular información o documentos adicionales, el responsable del sector privado contará con un nuevo plazo de hasta 20 días hábiles contados a partir del día siguiente a la presentación de la respuesta al requerimiento por parte del titular o su representante, para responder a la solicitud ARCO. Lo anterior a diferencia de lo previsto para el sector público, en el que la prevención únicamente interrumpirá el plazo con que cuenta el responsable para dar respuesta.[800]

Por su parte, el Reglamento General de Protección de Datos Personales establece un plazo de un mes para que los responsables den respuesta a una solicitud. Dicho plazo puede prorrogarse hasta por dos meses más en ciertos casos.

La denegación o desestimación de las solicitudes ARCO: las normativas en materia de datos personales aplicable al sector privado[801] y la aplicable al sector público[802] establecen ciertos supuestos en los que el responsable puede negar, parcial o totalmente, la solicitud de derechos ARCO. La LFPDPPP[803] prevé las siguientes:

(i) en caso de que el solicitante no sea el titular de los datos personales o no acredite su identidad, o el representante no esté debidamente acreditado para ello;

797 Artículo 103 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

798 Artículo 97 del Reglamento de la LFPDPPP.

799 Artículo 51 de la LGPDPPSO.

800 Artículo 52 LGPDPPSO.

801 Artículo 34 de la LFPDPPP.

802 Artículo 55 de la LGPDPPSO.

803 Artículo 34 de la LFPDPPP.

(ii) en aquellos casos en que el responsable no cuente con datos personales del solicitante en las bases de datos, registros y archivos del responsable, o sus encargados;

(iii) si estima que la solicitud podría lesionar los derechos de un tercero;

(iv) cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos y

(v) en aquellos casos en que la rectificación, cancelación u oposición haya sido previamente realizada.

La LGPDPPSO,[804] por su parte, señala los únicos supuestos en los que es improcedente la solicitud del ejercicio de los derechos ARCO, que son cuando:

(i) el titular o su representante no estén debidamente acreditados para ello;

(ii) los datos personales no se encuentren en posesión del responsable;

(iii) exista un impedimento legal;

(iv) se lesionen los derechos de un tercero;

(v) se obstaculicen actuaciones judiciales o administrativas;

(vi) exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;

(vii) la cancelación u oposición haya sido previamente realizada;

(viii) el responsable no sea competente;

(ix) sean necesarios para proteger intereses jurídicamente tutelados del titular;

(x) sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;

(xi) en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano o

(xii) los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

De ser negada la solicitud ARCO, el responsable deberá comunicar al titular o a su representante, dentro del plazo de 20 días hábiles contados a partir de la recepción de la solicitud, la determinación informando y justificando el motivo de la decisión a través del mismo medio por el que se llevó a cabo la solicitud y acompañando, en su caso, las pruebas que resulten pertinentes. En el caso de responsables del sector público, la denegación del ejercicio deberá constar en una resolución de su comité de transparencia que confirme la improcedencia de la solicitud.[805] En aquellos casos en que la improcedencia derive de la inexistencia de los datos personales la resolución del comité de transparencia deberá contener elementos que permitan al titular tener la certeza de que los datos se buscaron.[806] Asimismo, informará al titular el derecho que le asiste para presentar una solicitud de protección de derechos ante el INAI si el responsable es un particular, o un recurso de revisión en caso de que el responsable sea un sujeto obligado.

804 Artículo 55 de la LGPDPPSO.

805 Artículo 99 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

806 Artículo 101 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

El plazo para hacer efectiva la determinación: En caso de ser procedente la solicitud ARCO, el responsable debe hacer efectiva la determinación alcanzada dentro de un plazo no mayor a 15 días hábiles que son contados conforme a la LFPDPPP, a partir del día de que se comunique la respuesta al titular o a su representante y conforme a la LGPDPPSO a partir del día siguiente a que se le haya comunicado la respuesta. Tratándose de solicitudes ARCO sobre el derecho de acceso a datos personales, la entrega se hará previa acreditación de la identidad del titular o su representante y, en su caso, el pago de los costos correspondientes.

El plazo para hacer efectiva la determinación es conforme a la normativa para el sector público un plazo único sin que los sujetos obligados tengan la posibilidad de prorrogarlo. Por el contrario, en el sector privado la LFPDPPP brinda a los responsables la posibilidad de ampliar ese plazo hasta por un plazo igual, si las circunstancias lo justifican y sujeto a que se informe al titular al respecto dentro del plazo original.

6. Las restricciones al ejercicio de los derechos ARCO

Los derechos ARCO no son absolutos. La LFPDPPP establece las siguientes limitaciones al ejercicio de los derechos ARCO: razones de seguridad nacional, disposiciones públicas, seguridad y salud públicas o la protección de derechos de terceras personas, en los casos y conforme al alcance previstos en las leyes aplicables, o según se determine en la resolución debidamente fundada y motivada de una autoridad competente.

7. La tutela del Estado sobre el ejercicio de los derechos ARCO

El marco jurídico nacional brinda a los titulares de los datos personales, tanto en el sector privado como en el público, procedimientos para la protección del ejercicio de sus derechos ARCO. En el sector privado, los titulares tienen la posibilidad de iniciar un procedimiento de protección de derechos ante el INAI en caso de que el responsable de los datos personales (i) no brinde al titular una respuesta, (ii) no entregue al titular los datos personales solicitados o lo haga en un formato incomprensible, (iii) se niegue a hacer modificaciones o correcciones de los datos personales o (iv) la información entregada no sea de conformidad del titular por considerar éste que es incompleta o no corresponde a la información requerida. Este procedimiento debe iniciarse dentro de los 15 días hábiles siguientes a que el titular haya recibido o debiera haber recibido una respuesta a su solicitud ARCO.

En el sector público, el titular podrá presentar un recurso de revisión ante la falta de respuesta a una solicitud o en caso de no estar conforme con la respuesta recibida dentro de los 15 días hábiles contados a partir del día siguiente a la fecha de notificación de la respuesta.[807]

A) Derecho de acceso

El derecho de acceso es uno de los derechos que se reconocen a los titulares de datos personales. La LFPDPPP lo define como "el derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el aviso de privacidad al que está sujeto el tratamiento".[808] Más adelante, en el reglamento de la mencionada ley, se determinó que se trataba de un "derecho a obtener del responsable sus datos personales, así como información relativa

807 Artículo 56 de la LGPDPPSO.

808 Artículo 23 de la LFPDPPP.

a las condiciones y generalidades del tratamiento".[809] Finalmente, la LGPDPPSO combinó las definiciones anteriores para establecer que el derecho de acceso es el "derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento".[810]

Consecuentemente, el derecho de acceso es muy amplio y obliga al responsable a permitir al titular a acceder a todos sus datos personales en posesión o poder del responsable, brindarle información sobre el efectivo tratamiento al que son sujetos sus datos personales y conocer las circunstancias de ese tratamiento, por ejemplo: el tipo de datos que trata, las finalidades del tratamiento, las personas que intervienen en el tratamiento, la existencia de encargados, la existencia de transferencias, los destinatarios de las transferencias, las finalidades de las transferencias y los datos transferidos, entre otra información que el titular esté interesado en conocer. Gran parte de esa información debiera darse a conocer al titular desde el aviso de privacidad en cumplimiento del principio de información.

En la LFPDPPP se trata también de forma particular la posibilidad que tiene el titular de ejercer su derecho de acceso para conocer los datos personales que trata un responsable como parte de la toma de decisiones sin la intervención humana. Lo anterior con objeto de permitir al titular, en su caso, solicitar la rectificación y la reconsideración de la decisión tomada.

A nivel internacional, los Estándares Iberoamericanos reconocen el derecho de acceso en términos similares a la ley mexicana, mientras que el RGPD otorga al derecho de acceso un contenido muy puntual. La información que el responsable debe dar a conocer al titular, parte de la confirmación de que el responsable está tratando los datos que conciernen al titular y, de ser el caso, el acceso a los mismos, incluyendo lo siguiente:

> a) los fines del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de los destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo; e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; f) el derecho a presentar una reclamación ante una autoridad de control; g) cuando los datos no se hayan obtenido del interesado, cualquier información disponible sobre su origen; h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, […] y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado[811]

El ejercicio del derecho de acceso puede significar una carga administrativa para el responsable por lo que es conveniente establezca procesos que le permitan hacer efectivo ese derecho cuando se presente una solicitud.

I. El ejercicio del derecho de acceso

Los requisitos particulares de las solicitudes de acceso: el titular, directamente o a través de un representante, debe presentar la solicitud de ejercicio del derecho de acceso ante el responsable de los datos personales de conformidad con los requisitos y a través de los medios que se le den a conocer a través del aviso de privacidad y la legislación aplicable (ver definición de derechos ARCO).

809 Artículo 101 del Reglamento de la LFPDPPP.

810 Artículo 44 de la LGPDPPSO.

811 Artículo 15, UE RGDP, "Derecho de acceso del interesado". Disponible en: http://www.privacy-regulation.eu/es/15.htm

En la solicitud de acceso, el titular debe indicar el objeto de su solicitud para cumplir con el requisito previsto por la LFPDPPP en cuanto a que se proporcione una descripción clara y precisa de la solicitud.

Según lo dispuesto por la LGPDPPSO, en los casos en que el titular realice una solicitud de derecho de acceso deberá también señalar la modalidad de entrega y/o reproducción en la que prefiere que los datos se reproduzcan y podrá, en su caso, manifestar su imposibilidad de cubrir los costos de reproducción de la información en virtud de su situación socioeconómica.[812] La mencionada ley y los Lineamientos Generales de Protección de Datos Personales para el Sector Público brindan también al titular la oportunidad de acompañar a su solicitud algún medio magnético, electrónico o el mecanismo a través del cual requiere su reproducción para recibir la información con la intención de poder evitar que su entrega represente un costo para el titular.

Los medios para el otorgamiento del acceso: conforme a lo previsto por la legislación del sector privado, el responsable debe informar a los titulares en el aviso de privacidad los medios por los que dará acceso a sus datos personales. Cuando el responsable lo considere conveniente, podrá independientemente de lo que haya sido previsto en el aviso de privacidad, acordar con el titular la modalidad de entrega o reproducción de los datos. En cualquier caso, el acceso a los datos debe ser en formatos legibles o comprensibles para el titular y empleando un lenguaje sencillo y claro, de manera que no dejen duda sobre el contenido.

En el sector público, el responsable debe atender a la modalidad en la que el titular haya manifestado prefiera recibir la información. Si se presentara una imposibilidad física o jurídica que limite al responsable a cumplir con esa preferencia, según lo previsto por la LGPDPPSO, deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.

Para la elección de los medios para el otorgamiento del acceso tanto el responsable como el titular deberán tomar en consideración la seguridad de la información.

II. El otorgamiento del acceso

El responsable perteneciente al sector privado deberá dar respuesta a la solicitud de ejercicio del derecho de acceso en un plazo no mayor a 20 días hábiles contados a partir de la recepción de la solicitud, o en caso de haberse solicitado información o documentos adicionales, en un plazo no mayor a 20 días hábiles contados a partir del día siguiente a la presentación de la respuesta a ese requerimiento por parte del titular o su representante.

Adicionalmente, para otorgar el acceso el responsable contará con un plazo de 15 días hábiles contados a partir de que se haya comunicado la respuesta al titular de los datos o su representante.

Según lo previsto por la legislación aplicable al sector público, el responsable tendrá un plazo no mayor a 20 días hábiles contados a partir del día siguiente a la recepción de la solicitud para contestar. Plazo que se interrumpirá en caso de que exista una prevención. El plazo para contestar la solicitud de acceso podrá ser prorrogado únicamente por un plazo de 10 días hábiles siempre que exista causa justificada y se informe al titular de la ampliación dentro del plazo original.

812 Artículo 52 de la LGPDPPSO y artículo 83 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

El acceso se dará por cumplido una vez acreditada la identidad del titular o identidad y personalidad de su representante, así como, en su caso, el pago del costo correspondiente, cuando el responsable:

(i) ponga a disposición del titular los datos personales en sitio. En este caso, el responsable deberá determinar el periodo durante el cual el titular podrá presentarse a consultarlos, mismo que no podrá ser menor a 15 días hábiles. Los Lineamientos Generales de Protección de Datos Personales para el Sector Público establecen que el plazo máximo durante el cual el responsable deberá poner a disposición del titular la información solicitada es de 60 días hábiles contados a partir del día siguiente en que se hubiera notificado la respuesta de procedencia al titular. Una vez transcurrido dicho plazo sin que el titular haya acudido a tener acceso a sus datos personales,[813] será necesaria la presentación de una nueva solicitud;

(ii) expida copias simples o certificadas o

(iii) haga disponibles los datos personales cuyo acceso se solicitó a través de medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad.

Es interesante tener en cuenta que a nivel internacional, instrumentos como el Reglamento General de Protección de Datos abren la posibilidad a que el derecho de acceso se brinde verbalmente al titular, cuando éste lo solicite previa acreditación de su identidad. Lo anterior, sin duda, reduce el tiempo de respuesta por parte del responsable. Sin embargo, el responsable deberá tener en cuenta que la carga de la prueba del cumplimiento de la obligación siempre recae en la figura del responsable.

III. La denegación del acceso

El responsable puede desestimar una solicitud de acceso conforme a las causas generales previstas en la normativa en materia de datos personales. La LFPDPPP[814] prevé las siguientes:

(i) en caso de que el solicitante no sea el titular de los datos personales o no acredite su identidad, o el representante no esté debidamente acreditado para ello;

(ii) en aquellos casos en que el responsable no cuente con datos personales del solicitante en las bases de datos, registros y archivos del responsable, o sus encargados;

(iii) si estima que la solicitud podría lesionar los derechos de un tercero;

(iv) cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos y

(v) en aquellos casos en que la rectificación, cancelación u oposición haya sido previamente realizada.

La LGPDPPSO,[815] por su parte, señala los únicos supuestos en los que es improcedente la solicitud de ejercicios de derechos ARCO frente a responsables del sector público, que son cuando:

(i) el titular o su representante no estén debidamente acreditados para ello;

(ii) los datos personales no se encuentren en posesión del responsable;

(iii) exista un impedimento legal;

813 Los Lineamientos Generales de Protección de Datos Personales para el Sector Público (artículo 98) señalan que la información deberá ser destruida.

814 Artículo 34 de la LFPDPPP.

815 Artículo 55 de la LGPDPPSO.

(iv) se lesionen los derechos de un tercero;

(v) se obstaculicen actuaciones judiciales o administrativas;

(vi) exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;

(vii) la cancelación u oposición haya sido previamente realizada;

(viii) el responsable no sea competente;

(ix) sean necesarios para proteger intereses jurídicamente tutelados del titular;

(x) sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;

(xi) en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano o

(xii) los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En caso de no ser estimada la solicitud, el responsable deberá responder al titular dentro del plazo de 20 días hábiles previsto, informando la determinación alcanzada y justificando el motivo de la decisión. En el caso de responsables del sector público, la denegación del ejercicio deberá constar en una resolución de su comité de transparencia que confirme la improcedencia de la solicitud.[816] En aquellos casos en que la improcedencia derive de la inexistencia de los datos personales la resolución del comité de transparencia deberá contener elementos que permitan al titular tener la certeza de que los datos se buscaron.[817]

Así mismo, deberá informar al titular del derecho que le asiste para presentar una solicitud de protección de derechos ante el INAI, en caso de ser el responsable un particular, o un recurso de revisión en caso de tratarse de un sujeto obligado.

B) Derecho de rectificación

El derecho de rectificación es el derecho fundamental del titular de datos personales que según lo dispuesto por la LFPDPPP[818] consiste en poder solicitar, en todo momento, la rectificación de sus datos personales cuando sean inexactos o incompletos. Conforme a lo previsto por la LGPDPPSO,[819] la corrección de los datos personales también es procedente en caso de que los datos personales no estén actualizados.

A nivel internacional, los Estándares Iberoamericanos de Protección de Datos[820] prevén estos mismos tres supuestos en los que es procedente la rectificación: datos inexactos, incompletos o desactualizados. El Reglamento General de Protección de Datos Personales sigue esa misma tendencia y brinda a los responsables la posibilidad de rectificar los datos mediante una declaración adicional.[821]

816 Artículo 99 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

817 Artículo 101 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

818 Artículo 24 de la LFPDPPP.

819 Artículo 45 de la LGPDPPSO.

820 Artículo 26 de los Estándares Iberoamericanos de Protección de Datos.

821 Artículos 16 del Reglamento General de Protección de Datos.

I. El derecho de rectificación y su relación con el principio de calidad

El derecho de rectificación tiene una estrecha relación con el principio de calidad de los datos personales. El principio de calidad se cumple cuando los datos personales tratados son exactos, completos, pertinentes, correctos y actualizados.

En aquellos casos en que el titular proporciona directamente sus datos, se considera que los mismos cumplen con el principio de calidad, hasta en tanto el titular manifieste y acredite lo contrario o el responsable cuente con evidencia objetiva que lo contradiga.

Consecuentemente, es en beneficio tanto del responsable como del titular que los datos se rectifiquen cuando sea procedente.

II. El ejercicio del derecho de rectificación

Los requisitos particulares de las solicitudes de rectificación: El titular de datos personales, directamente o a través de un representante, debe presentar la solicitud de ejercicio del derecho de rectificación ante el responsable de los datos personales de conformidad con los requisitos y a través de los medios que se dan a conocer a través del aviso de privacidad y la legislación aplicable (ver definición de derechos ARCO).

En el caso específico de una solicitud de esta naturaleza, en adición a los requisitos que debe reunir toda solicitud ARCO, es indispensable que el titular especifique en su solicitud:

(i) los datos personales que desea rectificar;

(ii) la corrección o modificación que solicita se realice y

(iii) acompañe la documentación que soporte la procedencia de su solicitud.

Lo anterior se relaciona directamente con el requisito de que las solicitudes de derechos ARCO incluyan una descripción clara y precisa de lo solicitado.[822]

En la LFPDPPP se trata también, de forma particular, el caso en que el tratamiento de datos personales se realice sin la intervención humana y establece el derecho que tiene el titular de solicitar la rectificación sobre los datos personales que se hayan utilizado como parte de la toma de decisiones. Lo anterior con la intención de darle la posibilidad al titular, de así desearlo, de solicitar la reconsideración de la decisión tomada.

Los medios para presentar la solicitud de rectificación: el responsable debe informar a los titulares en el aviso de privacidad los medios habilitados para atender las solicitudes. La normativa nacional en materia de datos personales hace especial mención de la plena libertad que se otorga a los responsables para habilitar mecanismos que faciliten a los titulares el ejercicio del derecho de rectificación. La única restricción que se impone a los responsables es que los mecanismos favorezcan al titular.

III. La rectificación de los datos

El responsable perteneciente al sector privado deberá dar respuesta a la solicitud de ejercicio del derecho de rectificación en un plazo no mayor a 20 días hábiles contados a partir de la recepción de la solicitud, o en caso de haberse solicitado información o documentos adicionales, en un plazo no mayor a 20 días hábiles contados a partir del día siguiente a la presentación de la respuesta a ese requerimiento por parte del titular o su representante.

Adicionalmente, el responsable contará con un plazo de 15 días hábiles contados a partir de que se haya comunicado la respuesta al titular de los datos o a su representante, para realizar la rectificación.

822 Artículo 29 fracción III de la LFPDPPP.

Según lo previsto por la legislación aplicable al sector público, el responsable tendrá un plazo no mayor a 20 días hábiles contados a partir del día siguiente a la recepción de la solicitud para contestar. Plazo que se interrumpirá en caso de que exista una prevención. El plazo para contestar la solicitud podrá ser prorrogado únicamente por un plazo de 10 días hábiles siempre que exista causa justificada y se informe al titular de la ampliación dentro del plazo original.

De ser procedente, la obligación de rectificación se dará por cumplida cuando el responsable modifique aquellos datos personales que eran incompletos, inexactos o desactualizados. Al respecto, es importante tener en cuenta que la rectificación deberá realizarse para todos los tratamientos que se realicen de ese dato, lo que puede significar que la rectificación en una sola base de datos no sea suficiente.

En aquellos casos en que la información a rectificar haya sido remitida o transferida a terceros nacionales o extranjeros con anterioridad, el responsable deberá informar a estos de tal situación para que procedan a efectuar la corrección correspondiente.

IV. La denegación de la solicitud de rectificación

La normativa permite al responsable negar la solicitud de rectificación conforme a las causas generales previstas en la LFPDPPP:[823]

(i) en caso de que el solicitante no sea el titular de los datos personales o no acredite su identidad, o el representante no esté debidamente acreditado para ello;

(ii) en aquellos casos en que el responsable no cuente con datos personales del solicitante en las bases de datos, registros y archivos del responsable, o sus encargados;

(iii) si estima que la solicitud podría lesionar los derechos de un tercero;

(iv) cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y

(v) en aquellos casos en que la rectificación, cancelación u oposición haya sido previamente realizada.

La LGPDPPSO,[824] por su parte, señala los únicos supuestos en los que es improcedente la solicitud de ejercicios de derechos ARCO frente a responsables del sector público, que son cuando:

(i) el titular o su representante no estén debidamente acreditados para ello;

(ii) los datos personales no se encuentren en posesión del responsable;

(iii) exista un impedimento legal;

(iv) se lesionen los derechos de un tercero;

(v) se obstaculicen actuaciones judiciales o administrativas;

(vi) exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;

(vii) la cancelación u oposición haya sido previamente realizada;

(viii) el responsable no sea competente;

(ix) sean necesarios para proteger intereses jurídicamente tutelados del titular;

823 Artículo 34 de la LFPDPPP.

824 Artículo 55 de la LGPDPPSO.

(x) sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;

(xi) en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano o

(xii) los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En caso de no ser estimada la solicitud, el responsable deberá responder al titular dentro del plazo de 20 días hábiles previsto, informando la determinación alcanzada y justificando el motivo de la decisión. En el caso de responsables del sector público, la denegación del ejercicio deberá constar en una resolución de su comité de transparencia que confirme la improcedencia de la solicitud.[825] En cualquier caso, deberá informar al titular del derecho que le asiste para presentar una solicitud de protección de derechos ante el INAI, en caso de ser el responsable un particular, o un recurso de revisión en caso de tratarse de un sujeto obligado.

C) Derecho de cancelación

El derecho de cancelación es el derecho fundamental reconocido al titular de los datos personales por el cual la LFPDPPP[826] dispone que tiene, en todo momento, la prerrogativa de solicitar que todos o parte de sus datos personales se supriman o eliminen para que no estén en posesión del responsable y dejen de ser tratados.

La solicitud de cancelación deriva de que el titular considera que sus datos personales no están siendo tratados conforme a los principios y deberes previstos en el marco normativo aplicable en materia de protección de datos personales.

Al respecto, la LGPDPPSO,[827] además de reconocer a los titulares ese derecho, hace un listado de los medios de almacenamiento en los que pudieran encontrarse los datos personales que han de suprimirse, entre ellos, los archivos, los registros, los expedientes y los sistemas del responsable.

De conformidad con lo dispuesto por la LFPDPPP y la LGPDPPSO, la cancelación de los datos personales no se lleva a cabo de forma dinmediata, sino que en muchos casos debe ser precedida por un periodo de bloqueo. El responsable de los datos personales debe establecer y documentar los procedimientos para la conservación, bloqueo —y en su caso— supresión de los datos personales.

El Reglamento General de Protección de Datos reconoce el derecho de supresión, y dentro del mismo, el derecho al olvido.[828] Uno de los aspectos que este ordenamiento prevé —y que está pendiente de regular en el marco jurídico mexicano— es la excepción a la supresión de los datos personales por razones de libertad de expresión e información. Lo anterior fue una de las observaciones realizadas por el Comité Consultivo del Convenio 108 al marco jurídico mexicano.

825 Artículo 99 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

826 Artículo 25 de la LFPDPPP.

827 Artículo 46 de la LGPDPPSO.

828 Artículo 17 del Reglamento General de Protección de Datos Personales.

I. El ejercicio del derecho de cancelación

Los requisitos particulares de las solicitudes de cancelación: el titular de datos personales, directamente o a través de un representante, debe presentar la solicitud de cancelación ante el responsable de los datos personales de conformidad con los requisitos y a través de los medios que se dan a conocer a través del aviso de privacidad y la legislación aplicable (ver definición de "derechos ARCO").

En adición a los demás requisitos previstos para una solicitud de derechos ARCO, atendiendo al requisito general de que la solicitud contenga una descripción sea clara y precisa, en la solicitud de cancelación el titular debe identificar los datos personales que desea cancelar. La LGPDPPSO obliga además al titular a señalar las causas que lo motivaron a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable.

II. La cancelación de los datos personales

La respuesta a la solicitud de cancelación e inicio del periodo de bloqueo: El responsable perteneciente al sector privado tendrá, como en todos los casos de ejercicio de derechos ARCO, un plazo de 20 días hábiles a partir de que el titular de los datos haya presentado su solicitud, para darle respuesta, o en caso de haberse solicitado información o documentos adicionales, en un plazo no mayor a 20 días hábiles contados a partir del día siguiente a la presentación de la respuesta a ese requerimiento por parte del titular o a su representante.

Según lo previsto por la legislación aplicable al sector público, el responsable tendrá un plazo no mayor a 20 días hábiles contados a partir del día siguiente a la recepción de la solicitud para contestar. Plazo que se interrumpirá en caso de que exista una prevención. El plazo para contestar la solicitud podrá ser prorrogado únicamente por 10 días hábiles, siempre que exista causa justificada y se informe al titular de la ampliación dentro del plazo original.

En caso de resolver que la cancelación es procedente, el responsable deberá establecer un periodo de bloqueo y las medidas de seguridad que impidan se lleven a cabo otros tratamientos de los datos personales.

El responsable contará con un plazo de 15 días hábiles a partir de la fecha en que notificó su respuesta al titular, para operativamente llevar a cabo el bloqueo de los datos personales que trate, directamente o a través de sus encargados. Los responsables del sector público deberán, dentro de ese mismo plazo de 15 días hábiles, notificar al titular o a su representante una constancia que señale: (i) los documentos, bases de datos, archivos, registros, expedientes y/o sistemas de tratamiento en los que se encuentre los datos personales objeto de la cancelación; (ii) el periodo de bloqueo, en su caso, (iii) las medidas de seguridad de carácter administrativo, físico y técnico implementadas durante el periodo de bloqueo, en su caso, y (iv) las políticas, métodos y técnicas utilizadas para la supresión definitiva de los datos personales. Dichas constancias podrán recogerse en la unidad de transparencia del responsable en donde estarán disponibles hasta por 60 días hábiles contados a partir del día siguiente a que su hubiera notificado la procedencia de la oposición al titular. El envío de estas constancias se podrá realizar por correo certificado o medios electrónicos en aquellos casos en que el titular haya comparecido personalmente ante el responsable, siempre que no se trate de menores de edad.[829]

829 Artículo 96 y 97 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

El periodo de bloqueo: el bloqueo de los datos personales debe distinguirse de la cancelación. El bloqueo es periodo durante el cual, una vez identificados los datos personales sobre los que procede la cancelación, estos se reservan con la única finalidad de enfrentar posibles responsabilidades derivadas del tratamiento. Por esa razón, el periodo de bloqueo es equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica de la que deviene el tratamiento. Durante el periodo de bloqueo, los datos personales permanecen almacenados sin que deba permitirse ningún otro tratamiento, salvo que alguna disposición legal prevea lo contrario.

Una vez concluido el periodo de bloqueo, los datos personales serán cancelados, es decir, eliminados.

La supresión de los datos personales: transcurrido el periodo de bloqueo, se da paso a la cancelación de los datos personales, es decir, a su supresión definitiva. Para tal efecto, el responsable y sus encargados deben tomar las medidas de seguridad pertinentes. La supresión debe realizarse de tal manera que no permita la recuperación de la información bajo ninguna técnica. Al respecto, es recomendable tener en cuenta la *Guía para el Borrado Seguro de Datos Personales* publicada por el INAI. Una vez suprimidos los datos, el responsable deberá dar aviso al titular

III. La denegación del derecho de cancelación

El derecho de cancelación no es absoluto. El responsable puede desestimar una solicitud de cancelación conforme a las causas generales previstas en la LFPDPPP.[830]

(i) en caso de que el solicitante no sea el titular de los datos personales o no acredite su identidad, o el representante no esté debidamente acreditado para ello;

(ii) en aquellos casos en que el responsable no cuente con datos personales del solicitante en las bases de datos, registros y archivos del responsable, o sus encargados;

(iii) si estima que la solicitud podría lesionar los derechos de un tercero;

(iv) cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y

(v) en aquellos casos en que la rectificación, cancelación u oposición haya sido previamente realizada.

Adicionalmente, la LFPDPPP establece las siguientes excepciones al ejercicio del derecho de cancelación, algunas de las cuales entran dentro de las causas generales:[831]

(i) cuando la cancelación se refiera a los datos personales de las partes de un contrato privado, social o administrativo que el responsable tenga celebrado con el titular, y los datos sean necesarios para su desarrollo y cumplimiento;

(ii) en caso de que los datos deban ser tratados por disposición legal;

(iii) cuando la eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos, o la actualización de sanciones administrativas;

(iv) en caso de que los datos personales sean necesarios para proteger los intereses jurídicamente tutelados por el titular;

830 Artículo 34 de la LFPDPPP.

831 Artículo 26 de la Ley Federal de Protección de Datos Personales.

(v) cuando los datos personales sean necesarios para realizar una función del interés público;

(vi) en caso de que los datos personales sean necesarios para cumplir con una obligación legalmente adquirida por el titular; y

(vii) en aquellos casos en que los datos personales sean objeto de tratamiento para la prevención, el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional sujeto a un deber de secreto.

La LGPDPPSO,[832] por su parte, señala los únicos supuestos en los que es improcedente la solicitud de ejercicios de derechos ARCO frente a responsables del sector público, que son cuando:

(i) el titular o su representante no estén debidamente acreditados para ello;

(ii) los datos personales no se encuentren en posesión del responsable;

(iii) exista un impedimento legal;

(iv) se lesionen los derechos de un tercero;

(v) se obstaculicen actuaciones judiciales o administrativas;

(vi) exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;

(vii) la cancelación u oposición haya sido previamente realizada;

(viii) el responsable no sea competente;

(ix) sean necesarios para proteger intereses jurídicamente tutelados del titular;

(x) sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;

(xi) en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o

(xii) los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En caso de que el responsable resuelva que no procede la cancelación, deberá notificarlo al titular y/o su representante, justificando su decisión en un plazo de 20 días hábiles a partir de que el titular de los datos haya presentado su solicitud. En el caso de responsables del sector público, la denegación del ejercicio deberá constar en una resolución de su comité de transparencia que confirme la improcedencia de la solicitud.[833] En aquellos casos en que la improcedencia derive de la inexistencia de los datos personales la resolución del comité de transparencia deberá contener elementos que permitan al titular tener la certeza de que los datos se buscaron.[834]

D) Derecho de oposición

El derecho de oposición es la prerrogativa con que cuenta el titular de los datos personales para, en todo momento y por causa legítima, oponerse al tratamiento de sus datos perso-

832 Artículo 55 de la LGPDPPSO.

833 Artículo 99 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

834 Artículo 101 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

nales según lo dispuesto por la LFPDPPP[835] o exigir el cese del tratamiento de sus datos personales para determinadas finalidades conforme a lo que adiciona la LGPDPPSO.[836]

El derecho de oposición no es absoluto. La solicitud de oposición no procederá cuando, entre otras causas, los datos personales sean necesarios para las finalidades esenciales de la relación jurídica entre las partes, como por ejemplo, el cumplimiento de una obligación contractual o una disposición legal.

De resultar procedente el derecho de oposición, el responsable no podrá tratar los datos personales sobre los que el titular haya ejercido ese derecho para las finalidades que el titular haya especificado. Lo anterior, sin afectar el tratamiento de los datos personales por parte del responsable para las demás finalidades previstas en el aviso de privacidad que no hayan sido objetadas.

La normativa en materia de protección de datos personales, tanto en el sector privado como en el público, prevé diferentes supuestos en los que puede proceder la oposición. Existe una relación entre el derecho de oposición y el principio de consentimiento. El primero (previsto para ambos sectores) se presenta cuando un responsable está haciendo un tratamiento lícito de los datos, sin embargo, existe una causa legítima y la situación específica del titular justifica que éste solicite el cese de dicho tratamiento a fin de evitar que se le cause un daño o perjuicio, según dispone la LGPDPPSO, o un perjuicio según lo dispuesto por la LFPDPPP.

El segundo caso se presenta cuando el titular requiere manifestar su oposición para el tratamiento de sus datos personales con objeto de que su información personal no sea utilizada para ciertas finalidades, por ejemplo, en el sector privado pueden ser fines de prospección comercial o publicitarios.

Finalmente, en el sector público se prevé un supuesto adicional, que se presenta cuando el titular se opone o solicita el cese del tratamiento automatizado de sus datos personales para evaluar, sin intervención humana, determinados aspectos de su persona o analizar o predecir su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento, dado que le está produciendo efectos jurídicos no deseados o que afectan de manera significativa sus intereses, derechos o libertades.

A nivel internacional, los Estándares Iberoamericanos van en la misma línea que la legislación mexicana. Sin embargo, el RGPD reconoce también el derecho de objetar el tratamiento de datos personales con la particularidad de que incluye expresamente, como un derecho por separado, el derecho a no ser sujeto a un tratamiento automatizado de datos personales para la creación de perfiles. Adicionalmente, el reglamento prevé también un derecho a la limitación del tratamiento de los datos personales y prevé situaciones distintas en las que procede. La primera, cuando el titular impugna la exactitud de los datos personales. En este supuesto se limitará el tratamiento de los datos personales hasta que se resuelva la exactitud de los mismos. La segunda situación se presenta cuando, siendo el tratamiento que se realiza de los datos personales lícito, el titular se opone a la supresión de sus datos y en su lugar solicita la limitación de uso de los mismos, y finalmente, una tercera situación, por la cual el responsable ya no necesite los datos personales para las finalidades del tratamiento, pero el titular los necesita para la formulación, ejercicio o defensa de sus reclamaciones.

835 Artículo 27 de la LFPDPPP.

836 Artículo 47 de la LGPSPPSO.

I. El ejercicio del derecho de oposición

Los requisitos particulares de las solicitudes de oposición: el titular de datos personales, directamente o a través de un representante, debe presentar la solicitud de oposición ante el responsable de los datos personales de conformidad con los requisitos y a través de los medios que se dan a conocer a través del aviso de privacidad y la legislación aplicable (ver definición derechos ARCO).

La solicitud de oposición en el sector privado, en adición a los demás requisitos que debe contener una solicitud de derechos ARCO, es conveniente que especifique la finalidad o finalidades, tratamiento o tratamientos para los cuales existe oposición. Así mismo, cuando el tratamiento pueda llegar a causar un daño o perjuicio al titular, deberá señalarlo, sin importar que el tratamiento sea legítimo. Este elemento permite al responsable valorar la solicitud de oposición y fortalecerla. Adicionalmente, en caso de que no sea aceptada por el responsable, podrá ser de ayuda en la evaluación del asunto que realice el INAI dentro de un procedimiento de protección de derechos.

En el sector público, para el caso en que el titular presente una solicitud de oposición, la LGPDPPSO establece una clara obligación de: (i) manifestar las causas legítimas o la situación específica que lo llevaron a solicitar el cese del tratamiento y (ii) el daño o perjuicio que le causaría la persistencia del tratamiento o las finalidades específicas respecto a las cuales quiere ejercer el derecho de oposición.

II. La exclusión o cese del tratamiento de los datos

El responsable del sector privado deberá dar respuesta a la solicitud de oposición en un plazo no mayor a 20 días hábiles contados a partir de la recepción de la solicitud, o en caso de haberse solicitado información o documentos adicionales, en un plazo de hasta 20 días hábiles contados a partir del día siguiente a la presentación de la respuesta al requerimiento por parte del titular o su representante.

Según lo previsto por la legislación aplicable al sector público, el responsable tendrá un plazo no mayor a 20 días hábiles contados a partir del día siguiente a la recepción de la solicitud para contestar. Plazo que se interrumpirá en caso de que exista una prevención. El plazo para contestar la solicitud podrá ser prorrogado únicamente por un plazo de 10 días hábiles siempre que exista causa justificada y se informe al titular de la ampliación dentro del plazo original.

De ser procedente la oposición, el responsable deberá excluir o cesar el tratamiento de los datos personales del titular.

Los responsables del sector público deberán, además, notificar al titular o a su representante una constancia que señale el cese del tratamiento dentro del plazo de 15 días hábiles previsto para hacer efectiva la determinación del responsable. Dichas constancias podrán recogerse en la unidad de transparencia del responsable en donde estarán disponibles hasta por 60 días hábiles contados a partir del día siguiente a que su hubiera notificado la procedencia de la oposición al titular. El envío de estas constancias se podrá realizar por correo certificado o medios electrónicos, en aquellos casos en que el titular haya comparecido personalmente ante el responsable, siempre que no se trate de menores de edad.[837]

Para hacer efectivo el derecho de oposición, los responsables del sector privado pueden también gestionar listados de exclusión propios en los que incluyan los datos de las per-

837 Artículo 96 y 97 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

sonas que manifiesten su negativa a que se traten sus datos personales. Estos listados pueden ser comunes por sectores o generales. La inscripción debe ser gratuita y deberá proporcionarse al titular una constancia de su inscripción.

Lo anterior debe realizarse sin perjuicio de las obligaciones que tienen los responsables en el sector privado de no tratar los datos personales de aquellos titulares inscritos tanto en el Registro Público de Consumidores previsto en la Ley Federal de Protección al Consumidor como en el Registro Público de Usuarios a que hace referencia la Ley de Protección y Defensa al Usuario de Servicios Financieros.[838]

Los responsables deben incluir en sus avisos de privacidad las medidas que tienen implementadas para limitar el tratamiento de los datos personales, como los listados de exclusión propios.

III. La denegación del derecho de oposición

El responsable puede negar una solicitud de oposición con fundamento en las siguientes causas generales previstas por la normativa en materia de datos personales para el sector privado:[839]

(i) en caso de que el solicitante no sea el titular de los datos personales o no acredite su identidad, o el representante no esté debidamente acreditado para ello;

(ii) en aquellos casos en que el responsable no cuente con datos personales del solicitante en las bases de datos, registros y archivos del responsable, o sus encargados;

(iii) si estima que la solicitud podría lesionar los derechos de un tercero;

(iv) cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos y

(v) en aquellos casos en que la rectificación, cancelación u oposición haya sido previamente realizada.

En adición a las causas generales por las que se puede desestimar una solicitud de derechos ARCO (ver definición derechos ARCO en este diccionario), la LFPDPPP[840] también señala que el derecho de oposición no será procedente cuando el tratamiento de los datos personales que realice el responsable, ya sea directamente o a través de un encargado, sea necesario para el cumplimiento de una obligación legal a cargo del titular de los datos personales.

La LGPDPPSO,[841] por su parte, señala los únicos supuestos en los que es improcedente la solicitud de ejercicios de derechos ARCO frente a responsables del sector público, que son cuando:

(i) el titular o su representante no estén debidamente acreditados para ello;

(ii) los datos personales no se encuentren en posesión del responsable;

(iii) exista un impedimento legal;

(iv) se lesionen los derechos de un tercero;

(v) se obstaculicen actuaciones judiciales o administrativas;

(vi) exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;

838 Artículo 111 del Reglamento de la LFPDPPP.

839 Artículo 34 de la LFPDPPP.

840 Artículo 109 del Reglamento de la LFPDPPP.

841 Artículo 55 de la LGPDPPSO.

(vii) la cancelación u oposición haya sido previamente realizada;

(viii) el responsable no sea competente;

(ix) sean necesarios para proteger intereses jurídicamente tutelados del titular;

(x) sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;

(xi) en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano o

(xii) los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En el caso de responsables del sector público, la denegación del ejercicio deberá constar en una resolución de su comité de transparencia que confirme la improcedencia de la solicitud.[842] En aquellos casos en que la improcedencia derive de la inexistencia de los datos personales la resolución del comité de transparencia deberá contener elementos que permitan al titular tener la certeza de que los datos se buscaron.[843]

Derecho humano

Miguel Carbonell Sánchez

En términos generales, puede decirse que los derechos humanos son considerados como tales en la medida en que constituyen instrumentos de protección de los intereses más importantes de las personas, puesto que preservan los bienes básicos necesarios para poder desarrollar cualquier plan de vida de manera digna. Siguiendo a Ernesto Garzón Valdés podemos entender por bienes básicos aquellos que son condición necesaria para la realización de cualquier plan de vida, es decir, para la actuación del individuo como agente moral.[844]

Lo anterior significa que una persona puede no necesitar que el derecho a fumar sea un derecho humano ya que fumando o no, es posible que, en términos generales, pueda desarrollar de forma autónoma su plan de vida, pudiéndolo trazar por sí mismo y contando para tal efecto con un amplio abanico de posibilidades. Pero ese plan de vida y la capacidad de un individuo para llevarlo a la práctica se verán claramente afectados si el ordenamiento no contempla la libertad de tránsito o el derecho a la integridad física, ya que en ese caso la persona puede verse impedida de viajar a donde quiera o puede ser torturado o mutilado.

Hay que enfatizar que cuando hablamos de derechos humanos estamos hablando de la protección de los intereses más vitales de toda persona, con independencia de sus gustos personales, de sus preferencias o de cualquier otra circunstancia que pueda caracterizar su existencia. Por eso se puede decir, como se va a explicar más adelante, que los derechos fundamentales deben ser universales porque protegen bienes con los que deben contar toda persona con independencia del lugar en el que haya nacido, de su nivel de ingresos o de sus características físicas.

842 Artículo 99 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

843 Artículo 101 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

844 Garzón, E. (1990). *Derecho, ética y política*. Madrid. CEC, p. 531. Ver también, sobre el mismo tema, las reflexiones de Nino, C. (s.f.). "Autonomía y necesidades básicas". *Doxa*, número 7. Alicante, pp. 21 y ss.

Para entender el concepto de los derechos humanos es importante referirnos a la cuestión del fundamento de tales derechos. El análisis del fundamento de los derechos intenta responder a las siguientes preguntas ¿Por qué debemos proteger cierto bien como un derecho humano? ¿Qué es lo que debemos tomar en cuenta para decidir qué bienes deben tener el rango de derechos humanos y cuáles deben ser considerados como derechos secundarios, como derechos que pueden pactar entre sí los particulares o de simples aspiraciones sociales o morales no respaldadas por la fuerza del sistema jurídico?

Otro aspecto esencial en el tema que estamos analizando tiene que ver con la distinción entre los conceptos "derechos fundamentales", "garantías individuales y sociales" y "derechos humanos". Dichos términos no son equivalentes, ni se pueden utilizar indistintamente. Desde luego, es la Constitución la que utiliza, en el encabezado de su primera parte, el término "derechos humanos", en sustitución al de "garantías individuales" que durante muchos años figuró en nuestra Carta Magna y al que se apegaba la mayor parte de la doctrina constitucional mexicana.[845]

Representa un avance histórico el cambio de nombre que desde 2011 adopta la Constitución. El término "garantías individuales" no era el más adecuado, porque como ha demostrado en muchos de sus trabajos Héctor Fix Zamudio, el concepto de garantía no puede ser equivalente al de un derecho. La garantía es el medio, como su nombre lo indica, para garantizar algo, para hacerlo eficaz, para devolverlo a su estado original —en caso de que haya sido tergiversado, violado o no respetado. En sentido moderno una garantía constitucional tiene por objeto reparar las violaciones que se hayan producido a los principios, valores o disposiciones fundamentales.[846] Luigi Ferrajoli señala que: "Garantía es una expresión del léxico jurídico con la que se designa cualquier técnica normativa de tutela de un derecho subjetivo".[847]

Si quisiéramos utilizar un símil de derecho privado, podríamos decir que no es lo mismo el contenido de una obligación (por ejemplo, la obligación de entregar un bien objeto de un contrato de compra-venta) que la garantía mediante la cual las partes acuerdan hacer efectiva esa obligación en caso de incumplimiento. De hecho, en el derecho privado existen diversos tipos de garantías que se establecen para asegurar el cumplimiento de una obligación. Hay garantías reales (prenda, hipoteca) y garantías personales (fianza, aval).[848] Cuando llamamos garantías individuales a los derechos humanos es como si en el derecho privado se confundiera la obligación surgida del contrato con la hipoteca que se constituye para garantizar su cumplimiento.

Ha sido precisamente Luigi Ferrajoli quien con mayor agudeza ha explorado los alcances del concepto "garantía", partiendo de la idea de que no es lo mismo que un derecho fundamental. Para él, las garantías, en una primera acepción, son las obligaciones que derivan de los dere-

845 En la doctrina nacional hay algunas confusiones conceptuales cuando se intenta distinguir entre los términos citados. Me parece que es lo que sucede con la exposición que se hace en la obra Burgoa, I. (2002). *Las garantías individuales*. 35ª edición. México. Porrúa, pp. 177 y ss. Este autor afirma lo siguiente al intentar distinguir entre los derechos del hombre y las garantías individuales: "Los derechos del hombre se traducen substancialmente en potestades inseparables e inherentes a su personalidad; son elementos propios y consubstanciales de su naturaleza como ser racional, independientemente de la posición jurídico-positiva en que pudiera estar colocado ante el Estado y sus autoridades; en cambio, las garantías individuales equivalen a la consagración jurídico-positiva de esos elementos, en el sentido de investirlos de obligatoriedad e imperatividad para atribuirles respetabilidad por parte de las autoridades estatales y del Estado mismo. Por ende, los derechos del hombre constituyen, en términos generales, el contenido parcial de las garantías individuales, considerando a éstas como meras relaciones jurídicas entre los sujetos de que hemos hablado: gobernados, por un lado y Estado y autoridades, por el otro", p. 187.

846 Fix, H. (2003). "Breves reflexiones sobre el concepto y el contenido del derecho procesal constitucional", en Ferrer MacGregor, Eduardo (coordinador), *Derecho procesal constitucional*, 4ª edición. México. Porrúa. Tomo I, pp. 273 y 283, entre otras.

847 Ferrajoli, L. (2002, julio). "Garantías", en *Jueces para la democracia*. Número 38. Madrid, p. 39.

848 Ferrajoli, L. (2002, julio). "Garantías", en *Jueces para la democracia*. Número 38. Madrid, p. 39.

chos, de esta forma, puede haber garantías positivas y garantías negativas. Las negativas obligan a abstenciones por parte del Estado y de los particulares en respeto de algún derecho fundamental, mientras que las positivas generan obligaciones de actuar positivamente (es decir, de hacer cosas o realizar conductas) para cumplir con la expectativa que derive de algún derecho. Estos dos tipos de garantías pueden subsumirse en lo que el mismo autor llama "las garantías primarias o sustanciales", que son distintas de las "garantías secundarias o jurisdiccionales".

Las garantías primarias son precisamente las obligaciones o prohibiciones que corresponden a los derechos subjetivos establecidos en algún texto normativo; por su lado, las garantías secundarias son las obligaciones que tienen los órganos judiciales de aplicar la sanción o declarar la nulidad cuando constaten, en el primer caso, actos ilícitos y, en el segundo, actos no válidos que violen los derechos subjetivos y por tanto violen también las garantías primarias.[849]

Desde un punto de vista teórico, los derechos humanos no deberían ser confundidos con los derechos fundamentales, aunque en México dicha distinción se ha relativizado después de la reforma constitucional del 10 de junio de 2011. En general, podríamos decir que los derechos que están previstos en el texto constitucional y en los tratados internacionales son fundamentales.

El término "derechos fundamentales" aparece en Francia (*droits fondamentaux*) a finales del siglo XVIII, dentro del movimiento que culmina con la expedición de la Declaración de los Derechos del Hombre y del Ciudadano de 1789. En sentido moderno, toma relieve sobre todo en Alemania bajo la denominación de *grundrechte* adoptada por la constitución de ese país de 1949.[850]

Los derechos humanos son una categoría más amplia y que, en la práctica, se suele utilizar con menos rigor jurídico que la de derechos fundamentales. Muchas veces se hace referencia a los derechos humanos como expectativas que no están previstas de forma clara en alguna norma jurídica, con el objeto de señalar lo que a algunas personas les puede parecer una actuación indebida de las autoridades. Para algunos teóricos, que esgrimen muy buenas razones en su favor, serían también derechos humanos algunos derechos no jurídicos; se trataría, por ejemplo, de los llamados "derechos morales".[851] Como escribe Antonio E. Pérez Luño:[852]

> En los usos lingüísticos jurídicos, políticos e incluso comunes de nuestro tiempo, el término 'derechos humanos' aparece como un concepto de contornos más amplios e imprecisos que la noción de los 'derechos fundamentales'. Los **derechos humano**s suelen venir entendidos como **un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional.** En tanto que con la noción de los **derechos fundamentales** se tiende a aludir a **aquellos derechos humanos garantizados por el ordenamiento jurídico positivo, en la mayor parte de los casos en su normativa constitucional, y que suelen gozar de una tutela reforzada.** (Énfasis añadido).

Los derechos humanos aúnan —sigue diciendo Pérez Luño— a su significación descriptiva de aquellos derechos y libertades reconocidos en las declaraciones y convenios internacionales, una connotación prescriptiva o deontológica, al abarcar también aquellas exigencias más radicalmente vinculadas al sistema de necesidades humanas, y que debiendo

849 Ferrajoli, L. (2002, julio). "Garantías", en *Jueces para la democracia*. Número 38. Madrid, p. 39

850 Pérez, A. (1991). *Los derechos fundamentales*, 4ª edición. Madrid. Tecnos, p. 29. Ver también Cruz, P. "Formación y evolución de los derechos fundamentales" en su libro *La curiosidad del jurista persa, y otros escritos sobre la Constitución*. Madrid. CEPC, pp. 23-53.

851 Para un primer acercamiento al tema se recomienda: Cruz, J. (2001, octubre). "Derechos morales: concepto y relevancia", en *Isonomía*, número 15. México, pp. 55-79.

852 Pérez, A. (1991). *Los derechos fundamentales*, 4ª edición. Madrid. Tecnos, pp. 46-47.

ser objeto de positivación no lo han sido. Los derechos fundamentales poseen un sentido más preciso y estricto, ya que tan solo describen el conjunto de derechos y libertades jurídicas e institucionalmente reconocidas y garantizadas por el derecho positivo.

Las fronteras conceptuales de los derechos humanos son menos precisas que las que tienen los derechos fundamentales. Quizá por esa razón es por la que los sociólogos, los economistas, los politólogos, los filósofos, etcétera han escritos muchas páginas (algunas muy buenas) sobre los derechos humanos, pero sobre derechos fundamentales —hasta donde hay noticias— solamente escriben los juristas. Autores paradigmáticos en sus campos de conocimiento y con vasta influencia sobre la ciencia jurídica, como John Rawls o Jürgen Habermas, cuando hacen referencia en sus textos a libertades básicas, derechos o bienes primarios o derechos fundamentales, lo hacen sin tener en cuenta lo que efectivamente dice la constitución de su país o de cualquier otro Estado. Hacen bien, porque desde su perspectiva científica pueden adoptar enfoques más amplios que los que se utilizan desde la ciencia jurídica. Sus aportaciones son del mayor valor para quienes nos situamos en una óptica constitucional, pues con frecuencia someten nuestros razonamientos a fuertes presiones argumentativas y tenemos que redoblar o en su caso corregir nuestros puntos de vista.

Pese a todo, la distinción entre derechos fundamentales y derechos humanos no nos debe llevar a pensar que se trata de categorías separadas e incomunicadas. Todo lo contrario. De hecho, podríamos decir que todos los derechos fundamentales son derechos humanos constitucionalizados.

Pérez Luño pone un ejemplo que refleja con nitidez la diferencia entre el uso que le damos al concepto de derechos humanos y el que corresponde a la noción de derechos fundamentales: habría un amplio consenso en considerar que en el régimen del *apartheid* en Sudáfrica o en la dictadura de Pinochet en Chile se violaban derechos humanos; sin embargo, de acuerdo con el sistema jurídico de esos países, la detención sin causa o la segregación racial no eran actos violatorios de derechos fundamentales.[853] Esos dos regímenes (y muchos otros que se han visto y se siguen viendo en tantos países) podrían ser denunciados como violadores de derechos humanos, pero no como violadores de derechos fundamentales en tanto que sus ordenamientos jurídicos internos no reconocían como tales una serie de derechos que a nosotros nos pueden parecer esenciales desde cualquier punto de vista.

Lo anterior no significa, desde luego, que en el estudio de los derechos fundamentales los juristas no deban tener en cuenta las perspectivas y argumentos que ofrecen otras ciencias sociales; por el contrario, una perspectiva multidisciplinaria es muy recomendable para el estudio de los derechos fundamentales, siempre que se tenga presente que nuestra base metodológica tiene que partir de razonamientos y premisas estrictamente jurídicos.

¿Cómo definir un derecho humano o fundamental? (en adelante usaré como sinónimos las dos expresiones) No se trata, desde luego, de una cuestión sencilla. Como lo señala Carlos Bernal: "El concepto de derecho fundamental es una de las nociones más controvertidas en la doctrina constitucional europea de finales del segundo milenio y comienzos del tercero. Este concepto ha sido objeto de un sinnúmero de definiciones, acuñadas a partir de una gran variedad de perspectivas, cada una de las cuales acentúa ciertos rasgos específicos o enfatiza determinados matices o singularidades de esta figura jurídica".[854]

853 Pérez Luño, Pérez, A. (1991). *Los derechos fundamentales*, 4ª edición. Madrid. Tecnos, pp. 47-48.

854 Bernal, C. (2003). *El principio de proporcionalidad y los derechos fundamentales*. Madrid. CEPC, p. 75.

Todo derecho fundamental está recogido en una disposición de derecho fundamental, que es un enunciado previsto en la Constitución o en los tratados internacionales que tipifican un derecho fundamental.[855] Las disposiciones de derecho fundamental están previstas en normas de derecho fundamental, que son significados prescriptivos por medio de los cuales se señala que algo está ordenado, prohibido o permitido, o que atribuyen a un sujeto una competencia de derecho fundamental.[856] Para decirlo en otras palabras, la disposición es un texto normativo que todavía no ha sido dotado de sentido y que todavía no ha sido interpretado, mientras que la norma es el resultado de la interpretación del texto, que nos permite saber qué conductas están ordenadas, prohibidas o permitidas.

En términos generales, podemos decir que a partir de una norma de derecho fundamental se crea una relación jurídica compuesta por tres elementos: un sujeto activo, un sujeto pasivo y un objeto de la relación. La calidad de los sujetos vendrá dada, por un lado, por la titularidad de derechos que asigne una norma, por ejemplo, podrá ser sujeto activo del derecho a la educación toda persona, pero solamente lo será del derecho al voto quien sea mayor de 18 años y además posea la ciudadanía del estado en el que reside habitualmente. Por otro lado, la calidad de sujeto vendrá determinada también por el tipo de enunciado que la norma de derecho fundamental contenga; así, por ejemplo, el derecho a la vida podrá oponerse frente a todas las demás personas, con independencia de que sean particulares o autoridades, pero el derecho a un proceso judicial sin dilaciones, solamente podrá oponerse a una autoridad, en tanto que los particulares no administran justicia.

También podrá resultar variable el tipo de relación jurídica de derecho fundamental dependiendo del objeto que busque proteger un derecho fundamental, así, por ejemplo, si el objeto es la libertad del sujeto activo, es probable que la relación jurídica implique para el sujeto pasivo un deber de abstención, una conducta omisiva, que no lesione la libertad del sujeto activo. Puede resultar también que, si el objeto del derecho es la igualdad, se requiera del sujeto pasivo una conducta activa, por ejemplo para prestar el servicio público de salud, para construir viviendas o para impedir que unos particulares discriminen a otros en el acceso al transporte por carretera.

Tomando en cuenta lo anterior y considerando la pluralidad de conceptos y definiciones que existen de los derechos fundamentales, quizá lo mejor sea ofrecer solamente una de ellas, que nos permita comprender después el significado de los derechos dentro del sistema jurídico mexicano. Una de las mejores definiciones que se han realizado de los derechos fundamentales es la de Luigi Ferrajoli pues tiene la ventaja de que, al tratarse de un concepto construido desde premisas de teoría del derecho, puede ser aplicable a cualquier ordenamiento jurídico positivo, y además resulta útil para comenzar a plantear algunos de los problemas que, ya no en la teoría sino en la práctica, tienen actualmente los derechos (por ejemplo, en cuanto a su titularidad).

Luigi Ferrajoli sostiene que los derechos fundamentales son "todos aquellos derechos subjetivos que corresponden universalmente a 'todos' los seres humanos en cuanto dotados del *status* de personas, de ciudadanos o de personas con capacidad de obrar".[857] El propio autor aclara que por derecho subjetivo debe entenderse "cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones) adscrita a un sujeto por una

855 Alexy, R. (2002). *Teoría de los derechos fundamentales*, traducción de Ernesto Garzón Valdés. Madrid. (3ª reimpresión), p. 63.

856 Bernal, C. (2003). *El principio de proporcionalidad y los derechos fundamentales*. Madrid. CEPC, p. 77. La distinción entre "disposición" y "norma" puede verse en Guastini, R. (1992). *Dalle fonti alle norme*. Turín. Giappichelli, pp. 15 y ss.

857 Ferrajoli, L. (1999). *Derechos y garantías. La ley del más débil*. Madrid. Trotta, p. 37.

norma jurídica", mientras que por *status* debemos entender "la condición de un sujeto, prevista asimismo por una norma jurídica positiva, como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de éstas".

De esta definición conviene destacar tres elementos clave: se trata de a) derechos subjetivos; b) que son universalmente adscritos a todos en cuanto personas y c) que pueden estar restringidos por no contar con el *status* de ciudadano o de persona con capacidad de obrar.

Desde luego, el lector debe tener en cuenta que la definición de Ferrajoli toma como punto de vista el de la teoría general del derecho y en esa medida, deberá ser complementada con los datos que proporciona la dogmática jurídica para estar en condiciones de saber, dentro de un ordenamiento constitucional determinado, cuáles son —en concreto— los derechos fundamentales.

Es importante tener presente lo anterior porque el concepto de Ferrajoli hace referencia de lo que podríamos llamar "el contenido" de los derechos (un derecho subjetivo, su asignación universal, su restricción en algunos casos para los no ciudadanos o para quienes no tienen capacidad de obrar, etcétera), pero no nos señala que el carácter de fundamental de un derecho proviene —desde el punto de vista de la dogmática jurídica— también de la fuente jurídica que lo establece (normalmente la Constitución o los tratados internacionales), lo cual tiene importantes repercusiones prácticas para su tratamiento normativo (por ejemplo, los derechos participan de la supremacía constitucional, no son disponibles para el legislador, requieren de una especial forma de interpretación constitucional, están sujetos a un cierto procedimiento especial de protección, etcétera) y también, desde luego, para su análisis teórico.

Ferrajoli defiende el sentido de su definición argumentando —desde mi punto de vista con toda razón— que se trata de una definición realizada a partir de las premisas de la teoría del derecho y que, por lo tanto, se trata: a) de una definición estipulativa, ni verdadera ni falsa como tal, sino solamente más o menos adecuada a la finalidad explicativa de la teoría en relación con cualquier ordenamiento, cualesquiera que sean los derechos allí tutelados como fundamentales y b) de una definición formal, esto es, dirigida a identificar los rasgos estructurales que, en función de dicha finalidad, convenimos en asociar a esta expresión, y que determinan la extensión de la clase de derechos denotados por ella, cualesquiera que sean sus contenidos.[858]

Un aspecto central del concepto de Ferrajoli tiene que ver con la universalidad de los derechos, característica que además nos permite distinguir a los derechos humanos de otro tipo de derechos.

La universalidad de los derechos fundamentales puede ser estudiada desde dos distintos puntos de vista. Desde la teoría del derecho y atendiendo a la definición que nos ofrece Ferrajoli de derecho fundamental, la universalidad tendría que ver con la forma en que están redactados los preceptos que contienen derechos. Si su forma de redacción permite concluir que un cierto derecho se adscribe universalmente a todos los sujetos de una determinada clase (menores de edad, trabajadores, campesinos, ciudadanos, mujeres, indígenas: lo importante es que esté adscrito a todas las personas que tengan la calidad establecida por la norma), entonces estamos ante un derecho fundamental. Si, por el contrario, una norma jurídica adscribe un derecho solamente a una parte de los miembros de un grupo, entonces no estamos frente a un derecho fundamental, sino ante un derecho de otro tipo.

858 Pérez, A. (1991). *Los derechos fundamentales*, 4ª edición. Madrid. Tecnos, pp. 29 y 290.

A partir de esa distinta forma de asignación del derecho, el propio Ferrajoli distingue entre los derechos fundamentales (asignados universalmente a todos los sujetos de una determinada clase) y los derechos patrimoniales (asignados a una persona con exclusión de los demás), por ejemplo, la libertad de expresión, al ser reconocida constitucionalmente como un derecho de toda persona, sería un derecho fundamental, mientras que el derecho patrimonial sobre mi coche (derecho que comprende la posibilidad de usarlo, venderlo, agotarlo y destruirlo) excluye de su titularidad a cualquier otra persona.[859] En palabras del autor:[860]

> Los derechos fundamentales —tanto los derechos de libertad como el derecho a la vida, y los derechos civiles, incluidos los de adquirir y disponer de los bienes objeto de propiedad, del mismo modo que los derechos políticos y los derechos sociales— son derechos 'universales' (*omnium*), en el sentido lógico de la cuantificación universal de la clase de sujetos que son sus titulares; mientras los derechos patrimoniales —del derecho de propiedad a los demás derechos reales y también los derechos de crédito— son derechos singulares (*singuli*), en el sentido asimismo lógico de que para cada uno de ellos existe un titular determinado (o varios cotitulares, como en la copropiedad) con exclusión de todos los demás... Unos son inclusivos y forman la base de la igualdad jurídica... Los otros son exclusivos, es decir, *excludendi alios*, y por ello están en la base de la desigualdad jurídica.

Siguiendo la misma perspectiva de teoría del derecho hay que distinguir, como lo ha explicado Robert Alexy, entre la universalidad con respecto a los titulares y la universalidad respecto a los destinatarios (obligados) de los derechos.[861] La primera consiste "en que los derechos humanos son derechos que corresponden a todos los seres humanos", con independencia de un título adquisitivo.[862] Los destinatarios (en cuanto que obligados por los derechos) serían no solamente los seres humanos en lo individual sino también los grupos y los Estados. En este último caso, de acuerdo con Alexy, hay que diferenciar entre los derechos humanos absolutos de los derechos humanos relativos, los primeros se pueden oponer frente a todos los seres humanos, a todos los grupos y a todos los Estados, mientras que los segundos —los relativos— solamente son oponibles a, por lo menos, un ser humano, un grupo o un Estado.

Alexy pone como ejemplo de derechos humanos absolutos al derecho a la vida, que debe respetarse por todos. Un ejemplo de derecho humano relativo frente al Estado sería el derecho al voto, el cual debe ser respetado por el Estado del cual el individuo forma parte, y un ejemplo de derecho humano relativo frente a un grupo sería el derecho de los niños a que sus familias les proporcionen asistencia y educación.

Aparte de la perspectiva de la teoría del derecho, que es la que se acaba de explicar de forma muy resumida, la universalidad de los derechos también debe ser contemplada desde una óptica política, a partir de la cual dicha característica supondría la idea de que todos los habitantes del planeta, con independencia del país en el que hayan nacido y del lugar del globo en el que se encuentren deberían tener al menos el mismo núcleo básico de

859 Ferrajoli, L. (1999). *Derechos y garantías. La ley del más débil*. Madrid. Trotta, pp. 45 y ss.

860 Ferrajoli, L. (1999). *Derechos y garantías. La ley del más débil*. Madrid. Trotta, p. 46.

861 Alexy, Robert, "La institucionalización de los derechos humanos en el Estado constitucional democrático", *Derechos y libertades*, número 8, Madrid, enero-junio de 2000, pp. 24-26.

862 Alexy no acepta que puedan haber derechos de grupo, es decir, derechos que no sean asignados a cada uno de los seres humanos en lo individual, si bien reconoce que pueden existir derechos de comunidades o de Estados (derechos de tercera generación, derecho al desarrollo); tales derechos, sin embargo, no serían derechos humanos, con lo cual —reconoce el autor— se perdería la carga valorativo-positiva que tiene el término, pero se obtendría la ventaja "de aguzar la vista para que estos derechos no devengan en derechos de funcionarios", Alexy, R., "La institucionalización de los derechos humanos en el Estado constitucional democrático", *Derechos y libertades*, número 8, Madrid, enero-junio de 2000, p. 25.

derechos fundamentales, los cuales, además tendrían que ser respetados por todos los gobiernos. Desde luego, la forma en que ese núcleo básico podría plasmarse en los distintos ordenamientos jurídicos no tiene que ser uniforme para ser acorde con los principios de justicia; la historia, cultura y pensamiento de cada pueblo o comunidad puede agregar, y de hecho históricamente han agregado, una multiplicidad de matices y diferencias al conjunto de derechos fundamentales que establece su respectiva Constitución. En palabras de Konrad Hesse, "...la validez universal de los derechos fundamentales no supone uniformidad... el contenido concreto y la significación de los derechos fundamentales para un Estado dependen de numerosos factores extrajurídicos, especialmente de la idiosincrasia, de la cultura y de la historia de los pueblos".[863]

La caracterización de los derechos fundamentales como derechos universales no solamente sirve para extenderlos sin distinción a todos los seres humanos y a todos los rincones del planeta, sino que también es útil para deducir su inalienabilidad y su no negociabilidad. En palabras del propio Ferrajoli, si tales derechos "son normativamente de 'todos' (los miembros de una determinada clase de sujetos), no son alienables o negociables, sino que corresponden, por decirlo de algún modo, a prerrogativas no contingentes e inalterables de sus titulares y a otros tantos límites y vínculos insalvables para todos los poderes, tanto públicos como privados".[864] Que no sean alienables o negociables significa, en otras palabras, que los derechos fundamentales no son disponibles. Su no disponibilidad es tanto activa (puesto que no son disponibles por el sujeto que es su titular), como pasiva (puesto no son disponibles, expropiables o puestos a disposición de otros sujetos, incluyendo sobre todo al Estado).[865]

La no disponibilidad activa solamente supone que el sujeto mismo no puede, por su propia voluntad, dejar de ser titular de los derechos, lo cual no implica que se le impida renunciar a ejercer uno o varios derechos de los que es titular o que no pueda renunciar a utilizar los medios de protección que el ordenamiento jurídico pone a su alcance para protegerlos cuando hayan sido violados.

Es decir, un sujeto puede perfectamente renunciar a ejercer su libertad de expresión y quedarse callado durante toda su vida, de la misma forma que puede renunciar a su derecho a la intimidad y aparecer en televisión contando toda clase de sucesos pertenecientes a su vida privada (como suele pasar en la actualidad con muchas personas que buscan de esa manera sus quince minutos de celebridad), pero esas renuncias no significan, sin embargo, que una persona deje de ser titular del derecho, ya que esa capacidad de ser titular la asigna incondicionalmente el ordenamiento jurídico y no se puede renunciar a ella.

Por otro lado, tampoco se resquebraja la no disponibilidad activa por el hecho de que una persona decida, frente a la violación de uno de sus derechos fundamentales, no ejercer ninguno de los medios de tutela que establece el sistema jurídico para reparar esa violación. La violación puede permanecer, incluso con el concurso de la voluntad del afectado, sin que por ello sufra una merma la no disponibilidad activa del derecho fundamental.

863 Hesse, K. (1996). "Significado de los derechos fundamentales", en Benda, Maihofer, Vogel, Hesse, Heyde, *Manual de derecho constitucional.* Madrid. IVAP-Marcial Pons, p. 85.

864 Ferrajoli, L. (1999). *Derechos y garantías. La ley del más débil*. Madrid. Trotta, p. 39. El autor afirma que "...en caso de que se quiera tutelar un derecho como 'fundamental', es preciso sustraerlo, de un lado, al intercambio mercantil, confiriéndolo igualmente mediante su enunciación en forma de una regla general y, de otro, a la arbitrariedad política del legislador ordinario mediante la estipulación de tal regla en una norma constitucional colocada por encima del mismo".

865 Ferrajoli, L. Ferrajoli, L. (1999). *Derechos y garantías. La ley del más débil*. Madrid. Trotta, p. 47. Ver, en referencia al criterio de no disponibilidad de los derechos fundamentales de Ferrajoli, las observaciones de Guastini, Riccardo, "Tres problemas para Luigi Ferrajoli", en Ferrajoli, Luigi y otros, Pérez, A. (1991). *Los derechos fundamentales*, 4ª edición. Madrid. Tecnos

En los tiempos actuales, las características mencionadas de no negociabilidad y no alienabilidad son muy importantes, pues sirven, entre otras cosas, para poner a los derechos fuera del alcance de la lógica neo-absolutista del "mercado" que todo lo traduce en términos de productividad y ganancia; al no ser alienables ni disponibles los derechos se convierten en un verdadero coto vedado, para usar la expresión de Ernesto Garzón Valdés.[866] Lo anterior implica, por ejemplo, que no se puede vender la propia libertad de tránsito o las garantías que tiene todo individuo en el proceso penal.

Los derechos fundamentales, tomando en cuenta tanto su universalidad como su protección constitucional, se sitúan fuera del mercado y de los alcances de la política ordinaria. Esto significa que no puede existir una justificación colectiva que derrote la exigencia que se puede derivar de un derecho fundamental. Para decirlo en palabras de Ronald Dworkin, "los derechos individuales son triunfos políticos en manos de los individuos. Los individuos tienen derechos cuando, por alguna razón, una meta colectiva no es justificación suficiente para negarles lo que, en cuanto individuos, desean tener o hacer, o cuando no justifica suficientemente que se les imponga una pérdida o un perjuicio".[867]

En el mismo sentido, Robert Alexy señala que "el sentido de los derechos fundamentales consiste justamente en no dejar en manos de la mayoría parlamentaria la decisión sobre determinadas posiciones del individuo, es decir, en delimitar el campo de decisión de aquella...".[868] Esto significa que frente a un derecho fundamental no pueden oponerse conceptos como "bien común", "seguridad nacional", "interés público", "moral ciudadana", etcétera. Ninguno de esos conceptos tiene la entidad suficiente para derrotar argumentativamente a un derecho fundamental. En todas las situaciones en las que se pretenda enfrentar a un derecho fundamental con alguno de ellos el derecho tiene inexorablemente que vencer, si en verdad se trata de un derecho fundamental.

Ni siquiera el consenso unánime de los integrantes de una comunidad puede servir como instrumentos de legitimación para violar un derecho fundamental, pues como señala Ferrajoli, "ni siquiera por unanimidad puede un pueblo decidir (o consentir que se decida) que un hombre muera o sea privado sin culpa de su libertad, que piense o escriba, o no piense o no escriba, de determinada manera, que no se reúna o no se asocie con otros, que se case o no se case con cierta persona o permanezca indisolublemente ligado a ella, que tenga o no tenga hijos, que haga o no haga tal trabajo u otras cosas por el estilo. La garantía de estos derechos vitales es la condición indispensable de la convivencia pacífica. Por ello, su lesión por parte del Estado justifica no simplemente la crítica o el disenso, como para las cuestiones no vitales en las que vale la regla de la mayoría, sino la resistencia a la opresión hasta la guerra civil".[869]

La base normativa de la universalidad de los derechos humanos se encuentra, además de lo ya dicho, en los diversos pactos, tratados y convenciones internacionales que existen sobre la materia. El punto de partida de todas esas disposiciones —en sentido conceptual, no temporal— se encuentra en la Declaración Universal de los Derechos del Hombre de 1948. Dicha Declaración, junto con la Carta de la ONU, supone el embrión de un verda-

866 Valdés, G. (1993). "Representación y democracia". *Derecho, ética y política*. Madrid. CEC, pp. 644 y ss. del mismo autor, es importante consultar también su obra *Instituciones suicidas. Estudios de ética y política*. México. Paidós. UNAM. 2000.

867 Dworkin, R. (1993). *Los derechos en serio*. Barcelona. Planeta-Agostini, p. 37.

868 Alexy, R. (2002). *Teoría de los derechos fundamentales*, traducción de Ernesto Garzón Valdés. Madrid. (3ª reimpresión) p. 412.

869 Ferrajoli, L. (1995). *Derechos y razón. Teoría del garantismo penal.* Editorial Trotta. México, p. 859.

dero constitucionalismo global.[870] Como recuerda Bobbio, "con la Declaración de 1948 se inicia una fase importante en la evolución de los derechos: la de su universalización y positivación, haciéndolos pasar de derechos de los ciudadanos a verdaderos derechos de (todos) los hombres, o al menos derechos del ciudadano de esa ciudad que no conoce fronteras, porque comprende a toda la humanidad".[871]

A partir de la Declaración de 1948 los derechos dejan de ser una cuestión interna de la incumbencia exclusiva de los Estados y saltan por completo al terreno del derecho y las relaciones internacionales. Los particulares se convierten en sujetos de ese nuevo derecho, antes reservado solamente a la actuación de los Estados y no de los individuos, en la medida en que tienen asegurado un estatus jurídico supranacional; incluso, bajo ciertas circunstancias, pueden acceder a una jurisdicción internacional para el caso de que consideren violados sus derechos. Los tribunales nacionales empiezan a aplicar las normas jurídicas internacionales y los problemas antes considerados como exclusivamente domésticos adquieren relevancia internacional; podemos afirmar, en consecuencia, que también en materia de derechos humanos —como en tantos otros aspectos— vivimos en la era de la interdependencia.

Derechos morales

Kiyoshi Tsuru Alberú y
Patricio González Granados

El concepto de derechos morales está inexorablemente condicionado a ser la contraposición de los derechos económicos o patrimoniales. Su razón de ser es la necesidad de diferenciación de las prerrogativas y derechos que se traducen en valor patrimonial, para tener un foco de atención a aquellos derechos que derivan de valores no tasables como la personalidad, la dignidad, la intimidad, el honor o la reputación.

El derecho autoral es la rama del derecho, en la legislación mexicana, en la que se reconoce y desarrolla el concepto de derechos morales, se les define como los derechos de autor y son las prerrogativas y privilegios de carácter exclusivo y personal que se otorgan en favor de todo creador de obras literarias y artísticas.[872] Estos derechos buscan proteger la personalidad del autor a través de la obra y tienen el fin de tutelar su dignidad intelectual. En su origen subyace la idea de que el autor guarda un vínculo creativo e indestructible con su obra. De ahí que los derechos morales constituyan un derecho personalísimo, inalienable, imprescriptible, inembargable e irrenunciable.

El ordenamiento que sienta la base a nivel nacional de la normativa autoral es el Convenio de Berna para la Protección de las Obras Literarias y Artísticas, de 1886, el cual establece que el autor conservará el derecho de reivindicar la paternidad de la obra y de oponerse a cualquier deformación, mutilación u otra modificación de la misma o a cualquier atentado a la misma que cause perjuicio a su honor o a su reputación.[873]

Volviendo a la legislación nacional, nuestra Ley Federal del Derecho de Autor dispone que el autor es el único, primigenio y perpetuo titular de los derechos morales sobre las

870 Ferrajoli, L. (2002). "Más allá de la soberanía y la ciudadanía: un constitucionalismo global", en Carbonell, Miguel (compilador), *Teoría de la Constitución. Ensayos escogidos*. 2ª edición. México. IIJ-UNAM. Porrúa, pp. 397 y ss.

871 Bobbio, N. (1997). *L'eta dei diritti*. Turín. Einaudi, pp. 23-24.

872 Artículo 11 de la Ley Federal del Derecho de Autor.

873 Artículo 6 Bis 1 del Convenio de Berna.

obras de su creación. Esto implica que el derecho moral se considera unido al autor y es inalienable, imprescriptible, irrenunciable e inembargable. Si bien esta dicotomía de derechos morales y patrimoniales no ha sido extensamente desarrollada por nuestros tribunales, la Primera Sala de la Suprema Corte de Justicia de la Nación ha delineado las dos dimensiones del derecho de autor en los términos siguientes:

> …De tal suerte, corresponde al autor una dualidad de derechos en relación a su carácter subjetivo y otro atendiendo a la cuestión objetiva en la que se plasma su idea creativa de manera tangible; contando así, por un lado, con derechos patrimoniales, a través de los cuales puede obtener beneficios de naturaleza económica, como la cesión de derechos por su reproducción; a obtener regalías o por su venta como un bien material; así como derechos de naturaleza moral, tales como la integridad y paternidad de la obra y de oponerse a cualquier deformación, mutilación u otra modificación, o a cualquier atentado a la misma que cause perjuicio a su honor o a su reputación como artista, derivados de la integridad de la obra.[874]

En el ámbito civil no existe una definición legal de derechos morales. Sin embargo, sí se establece el contenido material que éstos protegen a través de la definición de daño moral prevista en el artículo 1916 del Código Civil Federal (CCF), a saber, la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, o bien en la consideración que de sí misma tienen los demás, o el menoscabo ilegítimo a la libertad o la integridad física o psíquica de las personas.

En materia de datos personales, los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) establecen que, de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), el responsable del tratamiento de los datos personales deberá notificar al titular y al Instituto en caso de que ocurran vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular. Para tales efectos, y siguiendo puntualmente lo previsto en la legislación civil federal, los Lineamientos precisan que se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relacionada —de manera enunciativa más no limitativa— con sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, consideración que de sí mismo tienen los demás, o cuando se menoscabe ilegítimamente la libertad o la integridad física o psíquica de éste.

A final de cuentas, puede observarse que tanto las prerrogativas otorgadas por el derecho autoral, como los bienes jurídicos tutelados por la legislación civil y la de datos personales, a pesar de tener distintas materializaciones y efectos jurídicos, derivan de los derechos de la personalidad y la dignidad inherentes a la persona.

874 Tesis 1a. CCVIII/2012 (10a.) de la Primera Sala de la Suprema Corte de Justicia de la Nación, publicada en la página 504 del *Semanario Judicial de la Federación y su Gaceta*. Décima época. Libro XII. septiembre de 2012. Tomo 1.

Derecho de portabilidad

Isabel Davara Fernández de Marcos,
Gregorio Barco Vega y
Alexis Cervantes Padilla

El derecho a la portabilidad de datos personales es una prerrogativa de los titulares de datos personales que les permite, bajo las condiciones establecidas en la normatividad aplicable, recibir los datos personales que han proporcionado a un responsable del tratamiento en un formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable del tratamiento sin impedimentos.[875]

En el ámbito nacional, el derecho a la portabilidad de datos personales se encuentra exclusivamente reconocido y regulado en la normatividad de datos personales aplicable al sector público. Es decir, al día de hoy, en el sector privado dicho derecho no figura en el catálogo de prerrogativas que tienen los titulares de datos personales respecto de su información personal, y si bien en muchas ocasiones se puede considerar como una modalidad más sofisticada del derecho de acceso o cancelación, lo cierto es que sus características, y en especial su importancia en la práctica para la efectividad de los derechos para los titulares, hacen que sea muy relevante su individualización.

En cuanto a la definición de este derecho, los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales (Lineamientos de Portabilidad)[876] señalan, en la fracción V de su artículo 3, que este derecho es la "prerrogativa del titular a que se refiere el artículo 57 de la Ley General o los que correspondan en las legislaciones estatales en la materia".[877]

En este orden de ideas, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) indica que "cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. Asimismo se añade que, cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales".[878]

Asimismo, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) indican, en su artículo 30.1, que "cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera".

875 Grupo de Trabajo del Artículo 29. *Directrices sobre el derecho a la portabilidad de los datos,* WP 242, adoptadas el 13 de diciembre de 2016. Revisadas por última vez y adoptadas el 5 de abril de 2017.

876 Lineamientos publicados en el *Diario Oficial de la Federación* el 12 de febrero de 2018.

877 Artículo 2 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

878 Artículo 57 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Finalmente, el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) dispone, en el apartado 1 del artículo 20, que "el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado".

1. Objeto de la portabilidad de datos personales

El Grupo de Trabajo del Artículo 29 (GTA29)[879] sostiene que el derecho a la portabilidad de datos personales tiene por objeto facultar a los titulares para tener control sobre el uso y destino de sus datos personales, ya que mejora su capacidad de trasladar, copiar o transmitir datos personales fácilmente de un entorno informático a otro (ya sea a sus propios sistemas, a los sistemas de terceros de confianza o a los de otros responsables del tratamiento).[880]

En el ámbito nacional, el artículo 7 de los Lineamientos de Portabilidad destaca que la portabilidad tiene por objeto que el titular solicite a) una copia de sus datos personales que hubiere facilitado directamente al responsable, en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos y, en su caso, entregarlos a otro responsable para su reutilización y aprovechamiento en un nuevo tratamiento, sin que lo impida el responsable al que el titular hubiere facilitado los datos personales y b) la transmisión de sus datos personales a un responsable receptor, siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos personales al responsable transmisor y el tratamiento de éstos se base en su consentimiento o en la suscripción de un contrato.

2. Procedencia

De acuerdo con lo previsto por los Lineamientos de Portabilidad, el derecho a la portabilidad de datos personales resulta procedente cuando los datos personales se encuentren en un formato estructurado y comúnmente utilizado y se actualicen cada una de las siguientes condiciones:

a) el tratamiento se efectúe por medios automatizados o electrónicos y en un formato estructurado y comúnmente utilizado;[881]

b) los datos personales del titular se encuentren en posesión del responsable o sus encargados. En este sentido, el derecho de portabilidad incluye los datos personales que incumban a la persona en cuestión y que ésta haya facilitado a un responsable del tratamiento;

c) los datos personales conciernan al titular, o bien, a personas físicas vinculadas a un fallecido que tengan un interés jurídico;

d) el titular hubiere proporcionado directamente al responsable sus datos personales, de forma activa y consciente, lo cual incluye los datos personales obtenidos en el contexto del uso, la prestación de un servicio o la realización de un trámite, o bien, aquellos proporcionados por el titular a través de un dispositivo tecnológico;

879 Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

880 Grupo de Trabajo del Artículo 29, *Directrices sobre el derecho a la portabilidad de los datos,* WP 242, adoptadas el 13 de diciembre de 2016 Revisadas por última vez y adoptadas el 5 de abril de 2017.

881 En este sentido los Lineamientos de Portabilidad prevén lo siguiente:
Artículo 6 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

e) la portabilidad de los datos personales no afecte los derechos y libertades de terceros;
f) exista una relación jurídica entre el responsable receptor y el titular;
g) se dé cumplimiento a una disposición legal y
h) el titular pretenda ejercer algún derecho.

Por otro lado, los Estándares Iberoamericanos prevén que el derecho de portabilidad se podrá ejercer cuando se traten por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.

El RGPD señala, en su artículo 20, apartado 1, letra a, con el fin de que se incluyan en el ámbito de aplicación de la portabilidad de datos, que las operaciones de tratamiento deben basarse en el consentimiento del interesado (con arreglo al artículo 6, apartado 1, letra a, o con arreglo al artículo 9, apartado 2, letra a, en el caso de categorías especiales de datos personales) o en un contrato del que el interesado es parte, de conformidad con el artículo 6, apartado 1, letra b.

3. Características

En cuanto a sus rasgos esenciales, desde el ámbito de las obligaciones impuestas al responsable, podemos señalar que el derecho a la portabilidad de datos personales impone la obligación al responsable de procesar, filtrar, seleccionar, extraer y diferenciar los datos personales que son objeto de portabilidad de aquella que no queda comprendida por ésta.[882]

Respecto de las características de este derecho, es importante señalar también que, en términos de lo señalado por el artículo noveno de los Lineamientos de Portabilidad, no se incluye la siguiente información:

A. Aquella inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos personales proporcionados directamente por el titular, como es el caso de los datos que hubieren sido sometidos a un proceso de personalización, recomendación, categorización, creación de perfiles u otros procesos similares o análogos.
B. Los pseudónimos, salvo que éstos se encuentren claramente vinculados al titular y puedan identificarlo o lo hagan identificable cuando el responsable cuente con información adicional que permita su individualización e identificación.
C. Los datos personales sujetos a un proceso de disociación, de tal manera que no puedan asociarse al titular ni permitir la identificación del mismo, es decir, que ya no serían considerados como tales, porque serían anónimos, salvo aquellos datos personales que por medio de un procedimiento posterior se puedan asociar de nuevo al titular y, por lo tanto, en puridad sería un proceso que habría dado lugar a la seudonimización y no a la anonimización.

Otro rasgo importante del derecho de portabilidad es que éste último no impone obligación alguna al responsable de almacenar, preservar, guardar, mantener o conservar todos los datos personales en su posesión en un formato estructurado y comúnmente utilizado, solo para efecto de garantizarla.[883]

882 Artículo 9 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

883 Artículo 10 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Al igual que los tradicionales derechos ARCO, el derecho de portabilidad es gratuito, salvo el costo razonable del medio de almacenamiento a través del cual se entregue la copia de los datos personales en un formato estructurado y comúnmente utilizado al titular.[884]

Finalmente conviene precisar que el derecho de portabilidad no implica el cese o la conclusión de la relación jurídica con el responsable, por lo que el titular podrá seguir utilizando o beneficiándose del servicio o programa proporcionado por el responsable al que hubiere facilitado los datos personales.[885]

4. Ejercicio del derecho de portabilidad

Los Lineamientos de Portabilidad establecen reglas muy precisas para el ejercicio del derecho de portabilidad como son los requisitos de la solicitud de portabilidad, interpretación, respuesta, presentación o costo para hacer efectivo el derecho, plazos, improcedencia y medios de impugnación aplicables.

De forma esquemática, en la siguiente tabla se resumen cada uno de los aspectos referidos:

Reglas para el ejercicio del derecho de portabilidad		
Elemento	Descripción	Fundamento
Solicitud para la portabilidad de datos personales	La petición de solicitar una copia de los datos personales en un formato estructurado y comúnmente utilizado, o bien, transmitir sus datos personales al responsable receptor. La explicación general de la situación de emergencia en la que se encuentra el titular, a efecto de que los plazos de respuesta sobre la procedencia o improcedencia de su solicitud y, en su caso, para hacer efectiva la portabilidad de sus datos personales sean menores. La denominación del responsable receptor y el documento que acredite la relación jurídica entre el responsable y el titular, el cumplimiento de una disposición legal o el derecho que pretende ejercer, en caso de que el titular solicite la transmisión de sus datos personales.	Artículo 52 de la LGPDPPSO y artículo 15 de los Lineamientos de Portabilidad.
Interpretación	El responsable deberá privilegiar la interpretación más amplia sobre los datos personales que conciernen al titular, salvo que se actualice alguno de los supuestos previstos en el artículo 9 de los Lineamientos de Portabilidad.	Artículo 17 de los Lineamientos de Portabilidad.
Metadatos	El responsable deberá entregar al titular o transmitir al responsable receptor, en la medida de lo posible, el mayor número de metadatos que se hubieren generado y obtenido a partir del tratamiento de los datos personales proporcionados directamente por el titular.	Artículo 18 de los Lineamientos de Portabilidad.

884 Artículo 16 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

885 Artículo 12 de los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales.

Respuesta del responsable y plazo para emitirla en situación de emergencia	El plazo a que se refiere el artículo 51, párrafo primero de la LGPDPPSO[315] o los que correspondan en las legislaciones estatales en la materia, no deberá exceder de 10 días contados a partir del día siguiente de la recepción de la solicitud, sin ampliación del mismo.	Artículo 51 de la LGPDPPSO y artículo 19 de los Lineamientos de Portabilidad.
Presentación o costo del medio de almacenamiento	El responsable deberá informar: El plazo que tiene el titular para que pueda presentar el medio de almacenamiento para la elaboración de la copia de sus datos personales en un formato estructurado y comúnmente utilizado, el cual no podrá exceder de tres días contados a partir del día siguiente en que se hubiere notificado la respuesta al titular. El costo del medio de almacenamiento para la elaboración de la copia de los datos personales en un formato estructurado y comúnmente utilizado que, en su caso corresponda, siempre y cuando no lo proporcione.	Artículo 20 de los Lineamientos de Portabilidad.
Plazo para hacer efectiva la portabilidad de datos personales en situación de emergencia	La transmisión no deberá exceder de siete días.	Artículo 21 de los Lineamientos de Portabilidad.
Efectividad de la portabilidad	Cuando el titular o en su caso, su representante reciba copia de sus datos personales en un formato estructurado y comúnmente utilizado, que le permita seguir utilizándolos, previo pago del costo del medio de almacenamiento que en su caso corresponda. Cuando el titular o en su caso, su representante hubiere sido notificado que el responsable transmisor ante el cual ejerció la portabilidad de sus datos personales transmitió éstos al responsable receptor conforme a sus instrucciones.	Artículo 22 de los Lineamientos de Portabilidad.
Improcedencia de la portabilidad de datos personales	Cuando se trate de información a que se refiere el artículo 9 de los presentes Lineamientos.	Artículo 23 de los Lineamientos de Portabilidad.

5. Normas técnicas y procedimiento para la transmisión de datos personales

Dado el carácter técnico del derecho a la portabilidad de datos personales, el artículo 25 de los Lineamientos de Portabilidad establece que los responsables del tratamiento deben observar las siguientes normas técnicas específicas:

a) Implementar mecanismos, medios y procedimientos idóneos que permitan al titular obtener sus datos personales, sea de manera personal, por vía electrónica, a través de opciones de descarga establecidas en sus páginas oficiales de internet, o por cualquier otra tecnología que considere pertinente.

b) Informar al titular sobre el o los tipos de formatos estructurados y comúnmente utilizados disponibles, a través de los cuales podrá entregar o transmitir los datos personales al responsable receptor, en función de la naturaleza de los datos personales y la viabilidad para ser objeto de portabilidad.

c) Garantizar, siempre y cuando sea técnicamente posible, la interoperabilidad del formato estructurado y comúnmente utilizado en el que se entreguen los datos personales al titular o los transmita a otros sistemas y bases de datos en posesión del responsable receptor, con la finalidad de que los datos personales puedan ser comunicados y reutilizados de manera uniforme y eficiente.

d) Procurar que los servicios y sistemas electrónicos en su posesión mantengan la capacidad de interoperar con otros sistemas, como una cualidad integral desde su diseño y a lo largo de su ciclo de vida, adoptando protocolos y estándares que permitan el intercambio de datos personales entre diversos sistemas o plataformas tecnológicas, con independencia del lenguaje de programación o plataforma en la que fueron desarrollados.

Asimismo, resulta necesario señalar que, además de las normas técnicas anteriores, los responsables que realicen la portabilidad de datos personales deberán observar las condiciones técnicas prevista en el artículo 26 de los Lineamientos de Portabilidad, así como cumplir con el procedimiento de transmisión de datos personales identificado en el artículo 27 de los Lineamientos de Portabilidad que señala lo siguiente:

a) La unidad de transparencia (UT) del responsable transmisor deberá dar respuesta al titular sobre la procedencia jurídica y técnica de la transmisión de sus datos personales en el plazo de 20 días contados a partir del día siguiente a la recepción de la solicitud, salvo que el titular se encuentre en una situación de emergencia.

b) El responsable transmisor deberá transmitir los datos personales —en un formato estructurado y comúnmente utilizado— al responsable receptor dentro del plazo referido en el numeral anterior.

c) El responsable transmisor deberá enviar los datos personales —en un formato estructurado y comúnmente utilizado— al responsable receptor, previa acreditación de la identidad del titular y, en su caso, la identidad y personalidad de su representante.

d) El responsable transmisor deberá cifrar los datos personales —en un formato estructurado y comúnmente utilizado— durante su envío al sistema o plataforma electrónica del responsable receptor.

e) El responsable transmisor y el responsable receptor deberán autorizar a una persona que se encargue de vigilar que en la transmisión de los datos personales se observen las condiciones, normas, procedimientos y obligaciones técnicas previstas en los Lineamientos de Portabilidad.

f) La UT del responsable transmisor y la UT del responsable receptor coadyuvarán, en el ámbito de sus respectivas competencias, con la persona a que se refiere la fracción anterior del presente artículo para vigilar el cumplimiento de los presentes Lineamientos en la transmisión de los datos personales.

g) La UT del responsable receptor deberá notificar a la UT del responsable transmisor y al titular la recepción de los datos personales —en un formato estructurado y comúnmente utilizado— a más tardar al día siguiente de la recepción de éstos.

h) Las UT del responsable transmisor y del responsable receptor deberán coordinar la atención de las solicitudes de portabilidad de datos personales, sin que ello implique realizar o intervenir en el desarrollo de actividades de índole técnico propias de las unidades administrativas competentes.

En definitiva, se puede señalar que el derecho de portabilidad habilita al titular de los datos a recibir un subconjunto de datos personales que le conciernen en un determinado formato, procesados por un responsable del tratamiento, y a almacenar dichos datos para un uso personal posterior, ya sea en un dispositivo privado o en una nube privada, sin tener que transmitir necesariamente los datos a otro responsable del tratamiento.[886]

Derechos patrimoniales

Kiyoshi Tsuru Alberú y
Patricio González Granados

Los derechos patrimoniales, entendidos en un sentido amplio, son todos aquellos derechos subjetivos oponibles a terceros que otorgan a su titular la facultad de exigir una determinada conducta de dar, hacer o no hacer que impacta de manera positiva a su patrimonio.

Bajo este marco general, encontramos en nuestra legislación nacional un concepto específico en la Ley Federal del Derecho de Autor, en la cual se contemplan los derechos patrimoniales como uno de los dos tipos de derechos que integran los derechos de autor. En nuestro orden jurídico, estos derechos están reconocidos a nivel constitucional en el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) de forma negativa, al incluirse en el apartado que establece las conductas que no serán consideradas monopólicas.[887]

El concepto normativo que establece la legislación mexicana de los derechos de autor es binario, en el sentido de que establece que son el reconocimiento que hace el Estado en favor de todo creador de obras literarias y artísticas, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial. Las prerrogativas y privilegios que tienen valor económico y generan ingresos son los que integran los derechos patrimoniales.

En materia de protección de datos personales, este concepto cobra relevancia en los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) emitidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en relación con la obligación de informar a los titulares en caso de que hubiere una vulneración. Los Lineamientos Generales establecen que, en términos de lo dispuesto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), el responsable del tratamiento de datos personales deberá notificar al titular y al INAI en caso de que ocurran vulneraciones de seguridad que de forma significativa afecten los derechos patrimoniales o morales del titular. Para tales efectos, los Lineamientos Generales disponen que se considerará que se afectan derechos patrimoniales cuando la vulneración esté relacionada —de manera enunciativa más no limitativa— con sus bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados o las cantidades o porcentajes relacionados con la situación económica del titular.

886 Grupo de Trabajo del Artículo 29, *Directrices sobre el derecho a la portabilidad de los datos,* WP 242. Adoptadas el 13 de diciembre de 2016 y revisadas por última vez y adoptadas el 5 de abril de 2017.

887 Artículo 28…
Tampoco constituyen monopolios los privilegios que por determinado tiempo se concedan a los autores y artistas para la producción de sus obras y los que, para el uso exclusivo de sus inventos, se otorguen a los inventores y perfeccionadores de alguna mejora.

De este enunciado normativo se advierte que el concepto de derechos patrimoniales que aplica en la rama de protección de datos personales es amplio, en el sentido de incluir, no solamente la información económica o financiera del titular afectado, sino también la que de alguna manera incida o permita desprender más datos, directos o indirectos sobre su patrimonio y obligaciones contractuales.

Desechamiento de la denuncia

Isabel Davara Fernández de Marcos,
Gregorio Barco Vega y
Alexis Cervantes Padilla

Es un acto jurídico de carácter procesal que pueden realizar el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y/o los organismos garantes en el ámbito de sus respectivas competencias, dentro del procedimiento de investigación (PI)[888] como resultado del análisis de la denuncia presentada por el titular de los datos, determinando desestimar la misma por no reunir los requisitos legales previstos en la normatividad de datos personales.

El desechamiento de la denuncia es un acto procesal que se produce dentro del PI y/o en su caso dentro de las investigaciones que son competencia del INAI y/o los organismos garantes locales, según corresponda, como consecuencia del análisis de la denuncia presentada por el titular de los datos ante la autoridad garante competente.

Por medio de este acto jurídico procesal, la autoridad garante en turno determina desestimar los elementos de fondo de la denuncia que ha presentado el titular, por razón de que la misma no cumple con los elementos formales y materiales previstos en la normatividad aplicable. Con base en ello, el desechamiento tendrá como consecuencia que el PI no subsista y se decrete la conclusión de este.

De esta manera, respecto de la figura del desechamiento de la denuncia podemos distinguir su adopción de en dos facetas normativas diferenciadas, de un lado en la normatividad aplicable al sector privado, y por el otro, en la normatividad del sector público, con bastantes similitudes en ambos sectores de actividad, pero con determinadas concreciones legales que a continuación se explican.

1. Desechamiento de la denuncia en el sector privado

El desechamiento de la denuncia se produce como un acto que se da dentro del PI regulado en los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de los Procedimientos) como resultado del análisis de la admisibilidad de la denuncia formulada por el titular de los datos personales. En particular, a partir de su estudio, el INAI, a través de la Dirección General de Investigación y Verificación para el Sector Privado (DGIV) determina si la misma resulta admisible al actualizarse los elementos formales y materiales establecidos en el artículo 151 de los Lineamientos de los Procedimientos y 131 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) o es preciso adoptar una determinación distinta respecto del contenido de esta.

888 Se recomienda consultar la definición de "procedimiento de investigación", prevista en este *Diccionario de Protección de Datos Personales.*

Con base en ello, la DGIV del INAI al realizar un estudio y análisis de la descripción de los hechos en que se funda la denuncia, así como a partir de la información presentada por el denunciante, podrá realizar las siguientes acciones:

a) Reconducir la denuncia. La denuncia se reconducirá en un plazo no mayor a 10 días hábiles a partir de que se tuvo por presentada la denuncia cuando los hechos en que se funda ésta última se refieran a alguno de los supuestos para el inicio del Procedimiento de Protección de Derechos (PPD).[889]

b) Orientar al denunciante sobre las instancias legales a las que puede acudir en defensa de sus derechos, en un plazo no mayor a 10 días hábiles a partir de que se haya tenido por presentada la denuncia.

c) Prevenir al denunciante, en caso de que su denuncia no sea clara, o bien, no cumpla con los elementos que señala el artículo 51 los Lineamientos de los Procedimientos previamente aludidos. En el supuesto de que el titular no responda la prevención formulada en un plazo de cinco días hábiles, se tendrá por desechada la denuncia. En esta etapa es precisamente en la que el INAI habrá analizado, si la denuncia reúne los siguientes elementos formales:

    1. Nombre completo del denunciante y domicilio o medio, ya sea electrónico o algún otro, para recibir notificaciones.
    2. Descripción de hechos precisos en los que basa su denuncia y los elementos o documentos con que cuenta para probar su dicho.
    3. Nombre y domicilio del denunciado o, en su caso, datos para su ubicación.
    4. Firma autógrafa de quien promueve, para lo cual se deberá observar lo siguiente: 1) si la denuncia se presentó por escrito, ésta deberá tener su firma autógrafa a menos que no sepa o no pueda firmar, caso en el cual, se imprimirá su huella digital y 2) si la denuncia se presentó por medios electrónicos, ésta deberá incluir el documento digitalizado que contenga su firma autógrafa, o bien, que contenga su firma electrónica avanzada (FIEL).

Con base en lo anterior, en el caso de que el denunciante no haya atendido en tiempo y forma la prevención que le formule la DGIV respecto del contenido de su denuncia, se procederá a desechar la misma, y en consecuencia el PI no dará inicio.

2. Desechamiento de la denuncia en el sector público

En un sentido similar al procedimiento de desechamiento de la denuncia del sector privado, los Lineamientos Generales de Protección de Datos Personales del Sector Público (Lineamientos Generales) establecen, en su artículo 194, segundo párrafo, que el INAI, a

889 Los supuestos previstos en el artículo 115 del RLFPDPPP que son las causales de procedencia del procedimiento de protección de derechos, son los siguientes:
a) que el titular no haya recibido respuesta por parte del responsable;
b) que el responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
c) que el responsable se niegue a efectuar las rectificaciones a los datos personales;
d) que el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;
e) que el responsable se niegue a cancelar los datos personales;
f) que el responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición y
g) por otras causas que a juicio del Instituto sean procedentes conforme a la Ley o al presente Reglamento.

través de su unidad administrativa competente (Dirección General de Investigación y Verificación para el Sector Público (DGIVSP), y derivado del estudio y análisis de los hechos manifestados en la denuncia, podrá desechar la misma, en el supuesto de que el denunciante no hubiere atendido la prevención que le haya formulado el INAI y/o el organismo garante que conozca de las investigaciones previas.[890]

Consecuentemente, el organismo garante competente, ya sea en el orden federal y/o local, al recibir la denuncia presentada[891] por el titular de los datos, realizará estudio y análisis de la denuncia misma para determinar si ésta resulta materia de un procedimiento de verificación o si reúne los siguientes elementos formales:

a) el nombre de la persona que denuncia, o en su caso, de su representante;
b) el domicilio o medio para recibir notificaciones de la persona que denuncia;
c) la relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho;
d) el responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación, y
e) La firma del denunciante, o en su caso, de su representante. En caso de que el titular no sepa firmar, bastará la huella digital.

Derivado de dicho análisis, la DGIVSP podrá realizar cualquiera de las siguientes acciones:

a) Reconducir la denuncia. Cuando ésta se ubique en uno de los supuestos de procedencia del Recurso de Revisión previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados LGPDPPSO. Lo anterior ocurrirá en un plazo no mayor a cinco días contados a partir de que se presentó la misma.
b) Orientar al denunciante. Lo orientará sobre las instancias legales a las que puede acudir en defensa de sus derechos en un plazo no mayor a 10 días hábiles a partir de que se haya tenido por presentada la denuncia.
c) Prevenir al denunciante. En caso de que su denuncia no sea clara, o bien, no cumpla con los elementos que señala el artículo 148 de la LGPDPPSO y 192 de los Lineamientos Generales en un plazo no mayor a cinco días a partir de la presentación de la denuncia. La falta de respuesta a la prevención tendrá como consecuencia el desechamiento de la denuncia.

Es decir, con base en la prevención que el INAI y/o el organismo garante competente realice dentro de las investigaciones previas para atender los requisitos de fondo y forma de la denuncia, cuando el titular hubiere sido omiso en facilitar, dentro del plazo legalmente requerido, la totalidad de la información necesaria para la admisibilidad de ésta última se decretará el desechamiento de la misma y, en consecuencia, el PI quedará sin materia para su tramitación legal.

890 Se recomienda consultar la definición de "investigaciones previas" en el presente diccionario.

891 De acuerdo con el artículo 192 de los Lineamientos Generales, la denuncia podrá presentarse por escrito libre, o a través de los formatos, medios electrónicos o cualquier otro medio que al efecto establezca el INAI o los organismos garantes. Las denuncias que se hayan presentado por escrito deberán contener la firma autógrafa del denunciante a menos que no sepa o no pueda firmar, en cuyo caso se imprimirá su huella digital, y en el caso de las presentadas por medios electrónicos, se deberá incluir el documento digitalizado que contenga la firma autógrafa, o bien, la firma electrónica avanzada del denunciante o del instrumento que lo sustituya.

Dignidad humana

Miguel Carbonell Sánchez

Antes de la reforma constitucional de junio de 2011, el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) señalaba que era precisamente la CPEUM la que otorgaba los derechos humanos (llamados "garantías" por el texto de la Carta Magna). La reforma del 10 de junio de 2011 establece que lo que la Constitución hace es simplemente "reconocer". Esa es, desde mi punto de vista, la clave para entender en México la concepción jurídica del principio de dignidad humana.

En distintos documentos que fueron redactados por las Cámaras del Congreso de la Unión como parte del procedimiento de reforma constitucional se hace referencia precisamente a este tema. Por ejemplo, en el dictamen de la Cámara de Senadores del mes de abril de 2010 se menciona que con la modificación que estamos analizando "…se reconocerán explícitamente los derechos humanos como derechos inherentes al ser humano, diferenciados y anteriores al Estado….", con lo cual se pretende romper "…con la antigua filosofía positivista en boga en el siglo XIX… bajo esta concepción, solo el Estado podía otorgar las garantías en una especie de concesión graciosa, y también podía, por esa misma concesión, revocar o limitar las garantías… el cambio que estamos planteando es de filosofía constitucional".

Lo cierto es que, más allá del debate entre iuspositivismo e iusnaturalismo (tema en el que ahora no es posible detenernos), a partir de la segunda posguerra mundial se afirma una corriente de pensamiento que sitúa a la dignidad humana en el centro del discurso jurídico, pero concibiéndola más allá de las normas.[892] Se parte de la idea de que la dignidad humana es previa y superior al ordenamiento jurídico, de modo que ninguna disposición del mismo puede desaparecerla. En buena medida se trata de decir "nunca más" a la barbarie del nazismo y del fascismo en Alemania y en Italia.[893]

En el ámbito internacional también la Convención Americana de Derechos Humanos se refiere a los "derechos inherentes al ser humano", los cuales pueden no estar enunciados en un texto jurídico (artículo 29 de la Convención). Se trata, en buena medida, de lo que se conoce como "derechos implícitos".

En el derecho comparado también encontramos distintas referencias a la dignidad humana como límite a la capacidad de disposición del ordenamiento jurídico. En este sentido podemos citar el artículo 1.1. de la constitución alemana de 1949, el artículo 3 de la constitución italiana de 1947 y al artículo 10 de la constitución española de 1978, por mencionar los más conocidos.

En el ámbito de América Latina, hay disposiciones parecidas en la constitución de Brasil (artículo 1 fracción III), de Costa Rica (artículo 33) y de Colombia (artículo 1, inspirado en buena medida en las constituciones alemana y española ya citadas), entre otras.

En la jurisprudencia mexicana, el principio de dignidad humana se ha ido abriendo camino de forma paulatina, aunque tímida si lo comparamos con lo que ha sucedido en otros países. Entre los pronunciamientos más interesantes cabe citar por ejemplo los siguientes:

892 Un amplio repaso a lo que significa la dignidad humana puede verse en Garzón, E. (2011). "¿Cuál es la relevancia moral del concepto de dignidad humana?". En *Propuestas*. Madrid. Trotta, pp. 35 y ss.

893 Carbonell, M. (2008). *La libertad. Dilemas, retos y tensiones*. México. UNAM-CNDH, pp. 220 y ss.

DERECHO AL LIBRE DESARROLLO DE LA PERSONALIDAD. ASPECTOS QUE COMPRENDE. De la dignidad humana, como derecho fundamental superior reconocido por el orden jurídico mexicano, deriva, entre otros derechos personalísimos, el de todo individuo a elegir en forma libre y autónoma su proyecto de vida. Así, acorde a la doctrina y jurisprudencia comparadas, tal derecho es el reconocimiento del Estado sobre la facultad natural de toda persona a ser individualmente como quiere ser, sin coacción ni controles injustificados, con el fin de cumplir las metas u objetivos que se ha fijado, de acuerdo con sus valores, ideas, expectativas, gustos, etcétera. Por tanto, el libre desarrollo de la personalidad comprende, entre otras expresiones, la libertad de contraer matrimonio o no hacerlo; de procrear hijos y cuántos, o bien, decidir no tenerlos; de escoger su apariencia personal; su profesión o actividad laboral, así como la libre opción sexual, en tanto que todos estos aspectos son parte de la forma en que una persona desea proyectarse y vivir su vida y que, por tanto, solo a ella corresponde decidir autónomamente.[894]

DIGNIDAD HUMANA. EL ORDEN JURÍDICO MEXICANO LA RECONOCE COMO CONDICIÓN Y BASE DE LOS DEMÁS DERECHOS FUNDAMENTALES. El artículo 1 de la Constitución Política de los Estados Unidos Mexicanos establece que todas las personas son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razones étnicas o de nacionalidad, raza, sexo, religión o cualquier otra condición o circunstancia personal o social que atente contra la dignidad humana y que, junto con los instrumentos internacionales en materia de derechos humanos suscritos por México, reconocen el valor superior de la dignidad humana, es decir, que en el ser humano hay una dignidad que debe ser respetada en todo caso, constituyéndose como un derecho absolutamente fundamental, base y condición de todos los demás, el derecho a ser reconocido y a vivir en y con la dignidad de la persona humana, y del cual se desprenden todos los demás derechos, en cuanto son necesarios para que los individuos desarrollen integralmente su personalidad, dentro de los que se encuentran, entre otros, el derecho a la vida, a la integridad física y psíquica, al honor, a la privacidad, al nombre, a la propia imagen, al libre desarrollo de la personalidad, al estado civil y el propio derecho a la dignidad personal. Además, aun cuando estos derechos personalísimos no se enuncian expresamente en la Constitución General de la República, están implícitos en los tratados internacionales suscritos por México y, en todo caso, deben entenderse como derechos derivados del reconocimiento al derecho a la dignidad humana, pues solo a través de su pleno respeto podrá hablarse de un ser humano en toda su dignidad.[895]

DIGNIDAD HUMANA. SU NATURALEZA Y CONCEPTO. La dignidad humana es un valor supremo establecido en el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, en virtud del cual se reconoce una calidad única y excepcional a todo ser humano por el simple hecho de serlo, cuya plena eficacia debe ser respetada y protegida integralmente sin excepción alguna.[896]

894 Novena época. Pleno. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXX. Diciembre de 2009, p. 7, aislada, Civil, Constitucional. P. LXVI/2009

895 Novena época. Pleno. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXX. Diciembre de 2009, p. 8, aislada, constitucional. P. LXV/2009.

896 Décima época. Tribunales Colegiados de Circuito. *Semanario Judicial de la Federación y su Gaceta*. Libro I. Octubre de 2011. Tomo 3, p. 1529, jurisprudencia, civil. I.5o.C. J/31 (9a.).

Quizá lo interesante de la modificación al artículo 1, realizada en junio del 2011, consista en proporcionarnos una llamada de atención sobre los límites que deben observar los poderes públicos, incluyendo al poder encargado de reformar la Constitución. Lo que nos afirma la CPEUM es que ningún ordenamiento jurídico puede jugar con la dignidad humana, concepto absolutamente no negociable en el desarrollo de los pueblos y naciones.

Se puede o no estar de acuerdo con el enfoque iusnaturalista adoptado por la Constitución mexicana, pero lo cierto es que la evidencia histórica nos demuestra que nunca sobra estar advertidos de los peligros que se corren cuando los poderes públicos (a veces incluso con la activa participación de los ciudadanos) pasan por alto la dignidad humana y cometen indecibles atropellos.

Una expresión concreta, de entre las muchas que se podrían citar, de la dignidad humana en el texto constitucional mexicano se establece a través de la prohibición de toda forma de esclavitud, contemplada en el artículo 1 de la Carta Magna. La prohibición de la esclavitud va de la mano con la concepción kantiana del ser humano como un fin en sí mismo, que nunca puede ser utilizado como un medio para fines que le sean ajenos. El ser humano, considerado en su totalidad, no es un bien que pueda formar parte del mercado: no se puede comprar o vender una vida.

Así parecía entenderlo, ya desde los inicios del Estado constitucional, el artículo 18 de la Declaración de los Derechos del Hombre y del Ciudadano del 24 de junio de 1793, cuyo texto dispuso: "Cualquiera puede contratar sus servicios y su tiempo, pero no puede venderse ni ser vendido; su persona no es una propiedad alienable. La ley no admite la esclavitud; no puede existir más que un compromiso de servicios y retribución entre el hombre que trabaja y el que le da empleo".

Y lo mismo parece desprenderse de la filosofía, como queda claro en el siguiente párrafo del ensayo *On Liberty* de John S. Mill:

> En este, como en los más de los países civilizados, un compromiso por el cual una persona se vendiera, o consintiera en ser vendido, como esclavo, sería nulo y sin valor; ni la ley ni la opinión le impondría. El fundamento de una tal limitación del poder de voluntaria disposición del individuo sobre sí mismo es evidente, y se ve con toda claridad en este caso. El motivo para no intervenir, sino en beneficio de los demás, en los actos voluntarios de una persona, es el respeto a su libertad. Su voluntaria elección es garantía bastante de que lo que elige es deseable, o cuando menos soportable para él, y su beneficio está, en general, mejor asegurado, dejándole procurarse sus propios medios para conseguirlo. Pero vendiéndose como esclavo abdica de su libertad; abandona todo el uso futuro de ella para después de este único acto. Destruye, por consiguiente, en su propio caso, la razón que justifica el que se le permita disponer de sí mismo. Deja de ser libre; y, en adelante, su posición es tal que no admite en su favor la presunción de que permanece voluntariamente en ella. El principio de libertad no puede exigir que una persona sea libre de no ser libre. No es libertad el poder de renunciar a la libertad.[897]

Otro ejemplo de enorme relevancia para entender los contenidos concretos de la dignidad humana puede verse en la cláusula que prohíbe la discriminación. El ahora párrafo quinto del artículo 1 de la CPEUM dispone lo siguiente: "[q]ueda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas".

897 Stuart. J. (2014). *Sobre la libertad.* Editorial Akal. Madrid.

Del párrafo recién trascrito conviene subrayar varios aspectos. En primer lugar, la notable ambigüedad con que se recogen algunos de los conceptos empleados; en segundo término, es importante mencionar que el propio artículo expresamente señala que la lista de cualidades que enuncia no es limitativa, de forma que podrá haber otras que también estén prohibidas si atentan contra la dignidad humana y tienen por objeto anular o menoscabar los derechos y libertades de las personas.[898]

Para comprender las posibilidades interpretativas que genera la apertura que propicia la última parte del artículo 1 constitucional transcrito, en el sentido de que aparte de los criterios mencionados por ese precepto son también discriminatorias otras causas que puedan atentar contra la dignidad humana siempre que tengan por objeto anular o menoscabar los derechos y libertades de las personas, conviene acudir, entre otras fuentes, a la jurisprudencia de la corte constitucional colombiana, que sostiene que son potencialmente discriminatorias aquellas diferenciaciones que: "1) se funden en rasgos permanentes de las personas de los cuales éstas no puedan prescindir por voluntad propia a riesgo de perder su identidad; 2) aquellas que afecten a grupos históricamente sometidos a menosprecio y prácticas discriminatorias y 3) aquellas que se funden en criterios que por sí mismos no posibiliten efectuar una distribución o reparto racional y equitativo de bienes, derechos o cargas sociales" (Sentencias C-371 de 2000 y C-93 de 2001).[899] Esa es, desde mi punto de vista, una excelente forma de entender y aplicar con sentido práctico el concepto de dignidad humana.

En todo caso, lo cierto es que la dignidad humana es, hoy en día, un referente propiamente normativo y no solamente ideológico del Estado constitucional de derecho. Su adecuada comprensión nos permite resolver problemas prácticos y, sobre todo, poner al ser humano en el centro del debate jurídico, evitando su instrumentalización.

Directrices de la OCDE sobre protección de datos y flujos transfronterizos

Jacobo Esquenazi Franco

A finales de los setenta, el tema de privacidad y protección de datos tomó relevancia en la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Los trabajos en la materia se cristalizaron en la Declaración del Consejo sobre la Protección de la Privacidad y el Flujo Transfronterizo de Datos,[900] aprobada el 23 de septiembre de 1980, y que contiene como anexo a los Lineamientos de Privacidad de la OCDE).[901] Los trabajos de la OCDE en torno a la privacidad han continuado y siguen hasta la fecha con importantes aportaciones en este campo.[902]

898 Courtis, Ch. (2009). *El mundo prometido. Escritos sobre derechos sociales y derechos humanos*. México. Fontamara, pp. 175 y ss.

899 Bernal, C. (2005) "El juicio de la igualdad en la jurisprudencia de la Corte Constitucional colombiana". En *El derecho de los derechos. Estudios sobre la aplicación de los derechos fundamentales*. Bogotá. Universidad del Externado de Colombia, pp. 255 y ss.

900 OECD. (s.f.) *Recommendation of the Council Concerning Guidelines Governing. The Protection of Privacy and Transborder Flows of Personal Data*. Disponible en: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

901 Anexo a la recomendación del Consejo se encuentran los lineamientos que gobiernan la protección de la privacidad y el flujo transfronterizo de datos personales. Consultados en: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

902 Sería imposible cubrir las aportaciones de la OCDE en la materia dentro de esta sección, pero para una visión de la evolución de la privacidad y las aportaciones de la OCDE se puede consultar: OECD. "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines", en *OECD Digital Economy Papers*. No. 176. Paris. OECD Publishing. Disponible en: http://dx.doi.org/10.1787/5kgf09z90c31-en

Los Lineamientos, como lo establece la declaración, buscan "permitir el avance del libre flujo transfronterizo de datos entre los países miembros y evitar la creación de obstáculos injustificados al desarrollo de las relaciones económicas y sociales".[903] Para ello desarrollan una serie de principios fundamentales para la protección de los datos personales, buscando que los países miembros incorporen dichos principios en sus marcos regulatorios nacionales, al mismo tiempo que buscan que dicha protección no establezca "obstáculos injustificados a los flujos transfronterizos de datos personales".[904]

1. Estructura

Las Lineamientos de la Privacidad constan de cinco partes y un memorando explicativo. El contenido de las partes centrales incluye:

a) Definiciones

La primera parte de las Lineamientos incluye 3 definiciones básicas:[905]

- responsable de datos personales
- dato personal
- flujo transfronterizo de datos personales

2. Alcance

Las Lineamientos especifican su aplicabilidad en los sectores público y privado, siempre que, por su utilización, contexto o forma de procesamiento pudieran causar un daño a la libertad y privacidad individuales. Sin embargo, reconoce que distintas categorías de datos personales podrían requerir de niveles de protección diferenciados, lo que les merecería establecer medidas especiales en las legislaciones nacionales y que los Lineamientos se aplicaran solamente al procesamiento automatizado de datos.

También se establece que las limitaciones a los principios contenidos en los Lineamientos, sobre todo aquellas que se establecen por motivos de soberanía y seguridad nacionales y mantenimiento del orden público, deben ser las menores posibles y públicas.

3. Principios básicos y de aplicación nacional[906]

La tercera parte contiene los siguientes principios básicos:[907]

1. Principio de limitación de la recolección (*Collection Limitation Principle*): se deben establecer límites a la recolección de datos personales, los cuales se deben obtener de manera justa y legal, y cuando sea apropiado, con el conocimiento y consentimiento del titular de los datos.[908]

903 OECD. (s.f.) *Recommendation of the Council Concerning Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data*. Disponible en: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

904 OECD. (s.f.) *Recommendation of the Council Concerning Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data*. Disponible en: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

905 Por cuestiones de espacio se listan pero no se incluyen las definiciones. Estas pueden encontrarse en: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

906 Los principios se toman directamente del documento de las Lineamientos. Disponibles en: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

907 A fin de presentar los principios de la manera más fidedigna posible, se ha optado por la traducción literal de los principios de la OCDE en lugar de utilizar la terminología más común utilizada hoy en día en distintas legislaciones como la mexicana.

908 Algunas legislaciones de protección de datos personales incorporan este principio como "proporcionalidad".

2. Principio de calidad: los datos personales deben ser relevantes al propósito para el que fueron recolectados y en la medida de lo necesario, deben ser precisos, completos y actualizados.
3. Especificación del propósito (*Purpose Specification Principle*): los propósitos para los cuales se recolectan los datos personales deben ser especificados a más tardar al momento de la recolección, y su uso subsecuente debe limitarse al cumplimiento de esos propósitos u otros que no sean incompatibles con los que se han especificado en cada cambio de propósito.[909]
4. Limitación del uso (*Use limitation Principle*): los datos personales no deben ser comunicados, facilitados o utilizados de forma distinta a los propósitos con los que se recolectaron (en el principio de especificación de propósito) salvo con las siguientes excepciones:
   a. con el consentimiento del titular de los datos, y
   b. bajo autorización de ley.
5. Principio de seguridad (*Secirity Safeguards Principle*): la información personal debe ser protegida con medidas razonables de seguridad que eviten los riesgos de acceso, destrucción, uso o publicación no autorizados de los datos personales.
6. Principio de apertura (*Oppenness Principle*): debe establecerse una política general de apertura ante nuevos desarrollos, prácticas y políticas relacionados con los datos personales. Debe poderse determinar de manera sencilla la existencia y naturaleza de los datos personales, los propósitos del tratamiento, la identidad y localización habitual del responsable de los datos.
7. Participación individual (*Individual Participation Principle*): los individuos tienen derecho a:
   a. obtener del responsable de los datos personales, o de otra fuente, información sobre si el responsable cuenta con su información personal;
   b. obtener su información personal en un período prudencial con un costo, si lo hubiere, que no sea excesivo, de una manera razonable y en un formato que le sea comprensible;
   c. que se le provean razones por las cuales las solicitudes contenidas en (a) y (b) le sean negadas y tener un mecanismo para objetar esa negativa;
   d. a objetar cuando los datos relacionados con su persona no sean precisos y cuando la objeción sea correcta, que los datos sean borrados, rectificados, completados o enmendados.
8. Principio de responsabilidad demostrada (*Accountability Principle*): un responsable del tratamiento de datos personales debe poder demostrar el cumplimiento efectivo de los principios arriba descritos.[910]

4. Principios básicos y de aplicación internacional

Los Lineamientos de Privacidad de la OCDE establecen también una serie de principios de aplicación internacional. Entre ellos, la necesidad de tomar en consideración las implicaciones que las reglas nacionales pudieran tener para el procesamiento y reexportación de los datos en otros países miembros. Esto encierra tomar medidas apropiadas para que no se interrumpa el flujo transfronterizo de datos (incluido el tránsito por terceros países miembros) de manera segura, a menos que éstos no observen de manera substan-

909 Algunas legislaciones de protección de datos personales incorporan este principio como "finalidad".

910 Algunas legislaciones alrededor del mundo describen el concepto "*accountability*" en inglés como "responsabilidad proactiva" por ejemplo el Reglamento Europeo de Protección de Datos.

tiva los Lineamientos. Sin embargo, se plantea que se pudieren establecer restricciones específicas a ciertos tipos de datos para los cuales su legislación establezca impedimientos adicionales de forma doméstica.

Implementación nacional

Esta sección establece que para poder realizar la implementación nacional de los Lineamientos se requiere establecer instituciones que velen por la protección de la privacidad y las libertades individuales relacionadas con los datos personales. Estas medidas, además de la implementación de los principios en las legislaciones o regulaciones nacionales, incluyen el reconocimiento a otros mecanismos como la autorregulación y la necesidad de establecer sanciones y remedios adecuados, a fin de evitar la discriminación contra los titulares de los datos.

Cooperación internacional

Los Lineamientos establecen que los países miembros "deberían",[911] a petición de otros miembros, hacerles saber detalles del cumplimiento de los principios establecidos en los lineamientos, buscando que las medidas tomadas sean compatibles con las de los demás países miembros que cumplan con los Lineamientos. Establece también, que los miembros deberían establecer procedimientos para el intercambio de información y asistencia mutua en los procedimientos de investigación y de mecanismos que gobiernen el flujo transfronterizo de datos personales.

Memorándum explicativo

Adicional a las secciones anteriores que componen el cuerpo de los lineamientos, estos contienen un documento denominado memorándum explicativo. Este contiene una referencia histórica a las fuentes que dieron pie a los principios y recomendaciones contenidas en los Lineamientos, a nivel de los países miembros y en el contexto internacional. Se incluye también una reseña de los trabajos realizados en la OCDE desde 1969, así como un desarrollo "comentado" de los elementos contenidos en los lineamientos, a fin de poder establecer un contexto y desarrollo más completo, a fin que los miembros de la OCDE pudieran utilizarlos para establecer sus marcos regulatorios nacionales.

Global Privacy Enforcement Network (GPEN)

Los trabajos de la OCDE no terminaron con la emisión de los Lineamientos de Privacidad, en 1980, sino que continuaron a lo largo de los siguientes años y se mantienen hasta la actualidad. Un hito importante se dio en junio de 2007 con la adopción de las Recomendaciones de la OCDE sobre Cooperación Transfronteriza para el Cumplimiento de Leyes de Protección a la Privacidad.[912]

En parte, el desarrollo de estos trabajos dio pie al lanzamiento de la Red Global de Aplicación del Cumplimiento de la Privacidad (Global Privacy Enforcement Network o GPEN por sus siglas en inglés), espacio en el que las autoridades de protección de datos cooperan para el cumplimiento en temas transfronterizos de las legislaciones de protección de datos personales.[913]

---

911 Es importante notar que el documento usa la voz "deberían" (*should* en inglés) a manera de recomendación en lugar de "deberán" (*shall* en inglés) que implicaría un compromiso.

912 OCDE. *Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*. Consultado en: http://www.oecd.org/internet/ieconomy/38770483.pdf

913 La participación en GPEN no es limitada a los miembros de la OCDE, pero tiene, definitivamente, su génesis en los trabajos de la organización.

Actualización de los Lineamientos de la OCDE

A partir de 2010 algunos de los miembros de la OCDE plantearon la necesidad de actualizar los Lineamientos de Privacidad de la OCDE. Finalmente se decidió hacer una que no modificó los principios específicos, pero que se enfoca en la actualización del memorándum explicativo, que es parte de los Lineamientos. Finalmente, se aprobó, en 2013, una versión actualizada de los Lineamientos de Privacidad.[914]

La actualización, conocida como los Lineamientos de Privacidad de la OCDE (2013), incorporan dos temas principales: a) la implementación de protección de los datos con un enfoque basado en el manejo de riesgo y b) la necesidad de considerar la dimensión global de la protección de la privacidad por medio de la mejora en la interoperabilidad.

El grupo de expertos que desarrolló la actualización de los Lineamientos produjo un reporte que identificó varios retos pero que no se resolvieron del todo como parte de la actualización y que pudieran ser parte de futuros trabajos en el marco de la OCDE.[915]

Disociación

María Solange Maqueo Ramírez

Tanto el artículo 3, fracción VIII, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), como el artículo 3, fracción XIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) definen la disociación como "el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo". De esta forma, la disociación implica la separación de la identidad de una persona física del conjunto de los datos personales que están siendo tratados, a fin de que ésta no esté identificada ni sea identificable de manera definitiva e irreversible. En consecuencia, los datos personales que han pasado por un proceso adecuado de disociación dejan de ser considerados como tales y, por ende, quedan excluidos del ámbito de aplicación de las disposiciones jurídicas en materia de protección de datos de carácter personal.

En ese sentido, para que un procedimiento de disociación pueda ser considerado como adecuado debe garantizarse que resulta prácticamente imposible conocer los datos personales originales que dieron lugar a la generación de los datos disociados. La mera posibilidad de que se produzca una asociación entre los datos y la persona concernida, sea mediante métodos físicos o lógicos, implica que el procedimiento no fue adecuado y, en consecuencia, el responsable del tratamiento seguirá estando sujeto a los principios, deberes y procedimientos establecidos por la ley en la materia. Esta última posibilidad es la que permite diferenciar la disociación de ciertas prácticas o técnicas, tales como el uso de seudónimos o el cifrado, que permiten la identificación de la persona aunque con un mayor grado de dificultad.

Por todo lo anterior, es necesario que los procedimientos de disociación tengan un carácter dinámico que permita su adaptación a la constante evolución tecnológica y al surgimiento de nuevos y cada vez más sofisticados métodos de reidentificación o reversión de procesos. Ello explica por qué los métodos y técnicas de disociación no estén especi-

914 OCDE. (2013). *OECD Privacy Guidelines (2013)*. Consultado en: http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

915 OECD. (s/f). "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", en *OECD Digital Economy Papers*. No. 229. Consultado en: http://dx.doi.org/10.1787/5k3xz5zmj2mx-en

ficados a través de la ley, pues su propio dinamismo y pluralidad impide sujetarlos a los procesos de creación y reforma legislativa. De hecho, su elección e implementación se constituye en un campo natural para la adopción de esquemas de mejores prácticas.

1. Utilidad

Los beneficios que conlleva la disociación de los datos personales se relacionan con los propios beneficios de la conservación de información que pudiera tener un valor específico, sea en términos históricos, estadísticos o científicos, sin que rivalice con los derechos de privacidad y protección de los datos personales a los que están sujetos, tanto el sector público como el sector privado. De tal forma que aun cuando se hubieran cumplido las finalidades que dieron origen al tratamiento de los datos personales, su disociación abre la posibilidad de disponer de información agregada o anonimizada sin afectar estos derechos humanos.

En ese sentido, los procedimientos de disociación resultan benéficos tanto para la implementación de políticas públicas, el ejercicio de otros derechos, como para la toma de decisiones y la adopción de políticas empresariales, por citar unos cuantos, cuya base de elaboración e implementación es precisamente la información generada a lo largo del tiempo. De ahí que los procedimientos de disociación cobren una mayor relevancia a partir del reconocimiento del valor de la información.

2. Efectos

El procedimiento de disociación de datos personales implica un tratamiento al cual se someten dichos datos para que dejen de ser considerados como tales. En consecuencia, su tratamiento queda excluido del ámbito de aplicación de la legislación en materia de protección de datos personales. En congruencia con lo anterior, tanto el artículo 22 de la LGPDPPSO como el artículo 10 de la LFPDPPP establecen que no es necesario obtener el consentimiento del titular de los datos personales "cuando los datos personales se sometan a un procedimiento previo de disociación".

Finalmente, cabe decir que a pesar de que las disposiciones jurídicas relativas a la obligación de los responsables del tratamiento de datos personales de documentar ciertas actividades relacionadas con el propio tratamiento, tales como la conservación, supresión o, en su caso, el bloqueo de datos personales, no explicitan los procedimientos de disociación dentro del ámbito comprendido por esta obligación, éstos podrían ser considerados en tanto que producen, de manera análoga, los mismos efectos que el borrado, eliminación o destrucción de la información personal.

Disponibilidad de la información

Christian Paredes González

La expresión "disponibilidad" de acuerdo con el *Diccionario de la Real Academia Española* (DRAE) es la cualidad o condición de disponible. Por otro lado, la palabra "disponible" —de acuerdo con la citada fuente— es la característica de una cosa que implica que se pueda disponer libremente de ella o que esté lista para usarse o utilizarse. Entonces, tratándose de la información, se puede entender como la cualidad de que la misma esté disponible o lista para utilizarse en cualquier momento.

Por otra parte, en el terreno nacional, las Recomendaciones de Seguridad de Datos Personales,[916] la Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales, publicada en 2015[917] (GISGSDP) y las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales[918] definen "disponibilidad" como la propiedad de un activo[919] para ser accesible y utilizable cuando lo requieran personas, entidades o procesos autorizados.

Divulgación

Isabel Davara Fernández de Marcos, Gregorio Barco Vega y Alexis Cervantes Padilla

El término "divulgación" es empleado en la normatividad de protección de datos personales para referirse a una de las acciones que implican el tratamiento de los datos personales.[920] Sin embargo, dicho término no se encuentra legalmente definido ni tampoco se ha delimitado su alcance en las disposiciones secundarias emitidas por la autoridad reguladora en la materia.[921]

De esta forma, para entender el alcance de este concepto es preciso referirse, en primer lugar, a la definición genérica del mismo. En este contexto, el *Diccionario de la Real Academia de la Lengua Española* (DRAE) indica que la palabra "divulgar" tiene el siguiente significado: "publicar, extender y/o poner al alcance del público algo".[922]

De la definición anterior notamos que de ella se desprende que la acción de divulgar, entendida como "divulgación", involucra actuaciones positivas —que requieren una actividad— relacionadas con la difusión o publicidad de algo. Respecto de lo anterior, lo que se hace público entonces puede abarcar cualquier contenido, material o información, pues el pronombre "algo" es empleado para señalar a una realidad indeterminada cuya identidad no se conoce o no se específica[923] y que es susceptible de concretarse en cualquier elemento, pudiendo involucrar en consecuencia, información como los datos personales sujetos a un determinado tratamiento.

En materia de protección de datos personales se puede observar, como adelantábamos, que la divulgación forma parte de las acciones relacionadas con el tratamiento de los datos personales, puesto que la definición del mismo, tanto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) como en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), incluye cualquier acción relacionada con la divulgación de los datos personales:

916 Publicadas el 30 de octubre de 2013 en el *Diario Oficial de la Federación*.

917 INAI. (2015). *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

918 INAI. (2018). *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

919 En términos de los citados instrumentos, un activo es la información, el conocimiento sobre los procesos, el personal, hardware, software y cualquier otro recurso involucrado en el tratamiento de los datos personales que tenga valor para la organización.

920 En relación con este concepto se recomienda consultar también la definición de "Tratamiento" de datos personales que figura en este *Diccionario de Protección de Datos Personales*.

921 En el portal del INAI se puede consultar la normatividad emitida para tal efecto, incluyendo los instrumentos internacionales http://inicio.ifai.org.mx/SitePages/marcoNormativo.aspx

922 RAE. (2018). "Divulgar" en *Diccionario de la Lengua Española.* Disponible en: http://dle.rae.es/?id=E1q9Jgy

923 RAE. (2018). "Algo" en *Diccionario de la Lengua Española*. Disponible en: http://dle.rae.es/?id=1nUry2t

924 Vid. Artículo 3, fracción XVIII, de la LFPDPPP y artículo 3, fracción XXXIII, de la LGPDPPSO.

Definición de tratamiento (divulgación como acción relacionada con el tratamiento)[354]	
LFPDPPP	LGPDPPSO
La obtención, uso, **divulgación** o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.	Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, **divulgación,** transferencia o disposición de datos personales.

Considerando entonces a la divulgación como una manifestación del tratamiento de datos personales, podemos diferenciar el empleo de este término en la normatividad de datos personales en figuras como las comunicaciones de datos personales y las vulneraciones de seguridad.

Normativamente, el término de divulgación se emplea para referirse a los dos tipos de comunicaciones de datos personales reguladas por la normatividad, es decir, a la remisión y a la transferencia.[925] También la *Guía para la Implementación de un Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP)[926] publicada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en 2015 al hacer referencia a la divulgación como una fase en la que ocurre el tratamiento de los datos personales, escinde dicha figura en las figuras de la remisión y la transferencia. Esto es, tanto la normatividad de datos personales del sector público como la del sector privado, distingue estas dos figuras (transferencia[927] y remisión[928]), en las que la divulgación de datos personales se da cuando los datos personales se hacen del conocimiento de un sujeto interviniente en el tratamiento o de un tercero para que éste ejecute, ya sea por propia cuenta o a nombre del responsable, determinados tratamientos de datos personales.

Por otro lado, como decíamos, la divulgación de datos personales es un término que tiene notable relevancia en un ámbito totalmente distinto, el de la seguridad ya que se considera una vulneración de seguridad el tratamiento de datos personales no autorizado, por lo que debe entenderse entonces que cualquier tipo de acción que resulte en que un tercero no autorizado acceda a datos personales, implicará una afectación del deber de seguridad y por lo tanto se considerará como una vulneración sujeta a las reglas previstas en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) y en la LGPDPPSO:

925 En relación con estas figuras, recomendamos consultar las definiciones de "remisión" y "transferencia" presentes en este *Diccionario de Protección de Datos Personales*.

926 INAI. (2015, junio). *Guía para la Implementación de un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf Fecha de consulta: 18 de octubre de 2018.

927 *Vid.* Artículo 3, fracción IXIX de la LFPDPPP y artículo 3, fracción XXXII de la LGPDPPSO.

928 *Vid.* Artículo 2, fracción IX del Reglamento de la LFPDPPP y artículo 3, fracción XXVII de la LGPDPPSO.

Definición de vulneración (tratamiento no autorizado)	
Reglamento de la LFPDPPP (artículo 63)	LGPDPPSO (artículo 38)
Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son: I. La pérdida o destrucción no autorizada; II. el robo, extravío o copia no autorizada; III. el uso, acceso o **tratamiento no autorizado** o IV. el daño, la alteración o modificación no autorizada.	Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes: I. La pérdida o destrucción no autorizada; II. el robo, extravío o copia no autorizada; el uso, acceso o **tratamiento no autorizado** o IV. el daño, la alteración o modificación no autorizada.

De acuerdo con lo anterior, puede afirmarse que una divulgación no autorizada de datos personales constituye una vulneración de datos en términos legales. No obstante, debe aclararse que, según la citada prescripción normativa, dicha acción solo podrá ser considerada como vulneración cuando se haya ejecutado sin la autorización del titular o del responsable del tratamiento, de ahí que se aluda a la vulneración como una conducta no controlada ni consensuada que puede poner en riesgo los derechos patrimoniales o morales del titular de los datos.

Documento de seguridad

Uciel Fragoso Rodríguez

La Real Academia de la Lengua Española (RAE)[929] define "documento" como:

> 1. m. Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos.
>
> 2. m. Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.

En ambas definiciones, un documento consiste en un testimonio registrado en cualquier medio (papel o medio electrónico) para probar algún hecho. En el caso de un documento de seguridad en el contexto de protección de datos personales, se trata de un instrumento que describe en forma detallada las medidas de seguridad implementadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales a cargo del responsable.

El Artículo 35 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO),[930] especifica para el documento de seguridad lo siguiente:

> Artículo 35. De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:
>
> I. el inventario de datos personales y de los sistemas de tratamiento;
>
> II. las funciones y obligaciones de las personas que traten datos personales;
>
> III. el análisis de riesgos;
>
> IV. el análisis de brecha;
>
> V. el plan de trabajo;

929 Real Academia Española.

930 DOF. (2017, enero). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados". Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

VI. los mecanismos de monitoreo y revisión de las medidas de seguridad y

VII. el programa general de capacitación.

En la parte del inventario de los datos personales y de los sistemas de tratamiento, el documento de seguridad debe contener un listado de todos los sistemas en donde se efectúe tratamiento de datos y una clasificación de todos los datos personales.

Los sistemas de tratamiento consisten generalmente en todos los sistemas informáticos en donde se almacenan o se procesan los datos personales como bases de datos, directorios, sistemas de recursos humanos, páginas web de registro, entre otros.

A lo largo del ciclo de vida de los datos personales es importante identificar los sistemas de tratamiento y determinar su función en la obtención, almacenamiento, uso, divulgación, bloqueo y destrucción de los mismos.

Adicionalmente al listado de sistemas de tratamiento, es imperativo crear una lista de los diferentes tipos de datos bajo tratamiento. Los datos se clasifican en función de su sensibilidad o riesgo inherente que está relacionado al valor significativo que tiene para el titular y responsable, así como para las personas que pudieran tener acceso a los datos sin autorización.

En la *Guía para Implementación del Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP)[931] se propone una clasificación de tres categorías de datos: nivel estándar, nivel sensible y nivel especial. Esta clasificación es adecuada para aplicarla en la mayoría de las organizaciones, sin embargo, se podrá generar una clasificación diferente dependiendo del contexto de la organización.

El nivel estándar abarca todos los datos de identificación, contacto, académicos y laborales como nombre, edad, sexo, nacionalidad, RFC, CURP, estado civil, número telefónico, dirección de correo electrónico, identificadores de redes sociales, nivel académico, profesión, cédula profesional, puesto de trabajo, lugar de trabajo, experiencia laboral, entre otros. Básicamente los datos personales clasificados como nivel estándar se consideran de bajo riesgo inherente, es decir, en caso de que exista un incidente de seguridad y se vea comprometido su confidencialidad, integridad o disponibilidad, el impacto para el titular, responsable y encargado es menor, por lo que el daño ocasionado podrá resarcirse en forma inmediata. Este tipo de datos requieren medidas de seguridad básicas.

En el nivel sensible están incluidos todos los datos personales de ubicación física, patrimoniales, de autenticación, jurídicos, de salud, creencias religiosas o filosóficas y de opinión pública como dirección física, geolocalización, información de cuentas bancarias, estados financieros, información fiscal, historial crediticio, ingresos, seguros, contraseñas, firma autógrafa, datos biométricos, antecedentes penales, contratos, demandas, información genética, estado de salud, historial médico, origen racial o étnico, afiliación filosófica o política, entre otros. A los datos de nivel sensible se les asocia un riesgo inherente medio, por lo tanto, en caso de presentarse algún incidente de seguridad, el impacto para el titular, responsable y encargado es considerable. Las medidas de seguridad necesarias para salvaguardar este tipo de dato son de complejidad media a alta.

Los datos personales clasificados en el nivel especial corresponden a datos de personas que, debido al contexto, una vulneración representa un alto riesgo, no solo a los titulares de los mismos, sino también pudiera ser una cuestión de seguridad nacional. Personas dentro del ámbito político, religioso, militar, líderes de opinión, grandes empresarios, entre otros, están clasificados en este grupo.

931 INAI. (2015, junio). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, pp. 14-15. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Otra parte importante del documento de seguridad es la identificación de todas las personas que intervienen en el tratamiento de datos personales a lo largo de su ciclo de vida. El proceso de identificación se logra mediante el análisis de los procesos de negocio y los tipos de datos personales tratados como parte del flujo de información. El tratamiento que se les dé a los datos debe estar en concordancia con los roles y responsabilidades de las personas en su papel de responsable o encargado. La asignación no adecuada de privilegios puede producir que —por error o intencionalmente— se afecte la confidencialidad, integridad o disponibilidad de los datos personales.

La sesión de análisis de riesgo en el documento de seguridad describe a detalle cómo se implementa el proceso en forma sistemática. Existen diversas metodologías o estándares en el mercado que pueden emplearse para su correcta implementación. Para el caso particular de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) propone la metodología de análisis de riesgo MARBAA[932] que para cada dato personal con un nivel de riesgo inherente asociado, se evalúan tres factores ligados a los propios datos: el volumen de los datos y su nivel de riesgo inherente (factor conocido como beneficio), el número de acceso a los datos (factor conocido como accesibilidad) y el entorno desde donde se acceden los datos (factor conocido como anonimidad).

Independiente de la metodología utilizada, el proceso de análisis de riesgo inicia con la identificación del activo a proteger, que en el caso de los datos personales, se identifican los tipos o categorías de los datos personales bajo estudio. La segunda fase en el proceso es identificar las amenazas que pudieran ocasionar algún daño a los datos. Las amenazas pueden ser internas o externas y pueden tener diferentes orígenes: fenómenos naturales, incidentes, infraestructura tecnológica o de origen humano. A continuación, se identifican las vulnerabilidades o debilidades que se presentan al momento de procesar la información o tratar los datos personales. Las vulnerabilidades se localizan en los procesos, en la tecnología o en la gente y su nivel de exposición depende de las medidas de seguridad existentes asociadas a cada vulnerabilidad.

Con la información recolectada se procede a construir escenarios de riesgo, los cuales describen situaciones que pueden pasar y que relacionan los componentes del riesgo: activo, amenazas y vulnerabilidades. Cada escenario de riesgo se evalúa estimando su probabilidad de ocurrencia y el impacto que pudiera tener en caso de que dicho escenario de riesgo se materialice.

El análisis de riesgo permite llevar a cabo el análisis de brecha, el cual consiste en determinar la diferencia entre las medidas de seguridad existentes y las que faltan para reducir el riesgo hasta un nivel por abajo del establecido por la organización como nivel aceptable. El análisis de brecha es otro componente importante que debe contener el documento de seguridad.

El análisis de riesgo y el análisis de brecha ayudan a seleccionar las medidas de seguridad aplicables a la protección de los datos personales. Cada uno de los mecanismos de seguridad consiste en un control que puede ser del tipo tecnológico, administrativo o de procedimiento y su implementación debe realizarse definiendo un plan de trabajo. El plan de trabajo es parte medular del documento de seguridad y es donde se detallan las acciones tomadas para implementar las medidas de seguridad, además, se especifican los recursos del tipo económico, humano o de cualquier otra naturaleza. El plan de trabajo se puede controlar y documentar con alguna metodología existente de gestión de proyectos.

932 INAI. (2015, junio). *Metodología de Análisis de Riesgo BAA.* Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf

Las medidas de seguridad implementadas para proteger los datos personales deben ser efectivas y eficientes, es decir, deben mitigar los riesgos por debajo del nivel de aceptación y lo deben de hacer optimizando recursos. En el documento de seguridad se deben especificar indicadores clave de desempeño (KPI por sus siglas en inglés) para medir la efectividad de cada medida de seguridad, además, debe establecerse un procedimiento de monitoreo y revisión de las métricas, de tal forma que puedan tomarse medidas de ajuste y lograr un proceso de mejora continua.

Como parte final del documento de seguridad, se propone una sección en donde se establezca un programa general de capacitación que describa detalladamente los planes de capacitación para cada persona que intervenga en el tratamiento de datos personales a lo largo de su ciclo de vida.

Los programas de capacitación deben ajustarse para los responsables y encargado del tratamiento de los datos según sus roles y responsabilidades asignadas.

El documento de seguridad debe ser un instrumento actualizado continuamente para mantener las medidas de seguridad a un nivel adecuado a las nuevas amenazas y forma de ataque sobre los datos personales como lo expresa la LGPDPPSO, en su artículo 36, en el cual establece:

> Artículo 36. El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:
>
> I. se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;
>
> II. como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;
>
> III. como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y
>
> IV. implementación de acciones correctivas y preventivas ante una vulneración de seguridad.

El documento de seguridad debe actualizarse cuando se presente un cambio en el tratamiento de los datos personales derivado de una modificación del tipo de dato tratado, cambios en los procesos de negocio o modificaciones en los roles y responsabilidades de las personas que tratan datos personales. Los cambios al documento de seguridad también pueden obedecer a la misma naturaleza de mejora continua de la gestión de las medidas de seguridad.

En caso de que exista una vulneración a alguna medida de seguridad, se deberán ejecutar los ajustes correspondientes a los mecanismos de control y por lo tanto se deberá actualizar el documento de seguridad según corresponda.

Documento electrónico (mensaje de datos)

Jonathan Gabriel Garzón Galván

El documento en general, en materia legal, no solo es el escrito o instrumento que contiene manifestaciones, declaraciones de voluntad, y/o constancias de hechos o verdades suficientemente funcionales para probarlas; sino que puede ser definido como todo objeto que puede ser llevado ante la presencia de un juzgador u autoridad para su valoración.[933] Un hecho u acto jurídico para poder ser corroborado en el futuro, debe dejar evidencia o fundamento de que existió en un momento determinado. Es por ello que el documento, en el más amplio sentido de la palabra, es la base de todo acto jurídico.

933 Nava, A. (2011). *La Prueba Electrónica en Materia Penal*. México. Porrúa, p. 44.

Partiendo de los puntos anteriores, se puede apreciar que no se requiere que el documento deba estar escrito en papel para cumplir su definición u objetivo, sin embargo, se tiende a identificar el concepto de documento, únicamente como aquel materializado en papel y con escritura en tinta.

La palabra documento tiene su origen del vocablo latino que significa enseñar, mostrar, hacer saber o poner algo en presencia de uno.[934] Al respecto el *Diccionario de la Real Academia de la Lengua Española* (DRAE)[935] señala:

> Documento.
>
> (Del lat. *documentum*).
>
> 1. m. Diploma, carta, relación u otro escrito que ilustra acerca de algún hecho, principalmente de los históricos.
>
> 2. m. Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.
>
> 3. m. desus. Instrucción que se da a alguien en cualquier materia, y particularmente aviso y consejo para apartarle de obrar mal.
>
> Escribir.
>
> (Del lat. *scribĕre*).
>
> 1. tr. Representar las palabras o las ideas con letras u otros signos trazados en papel u otra superficie.

En materia electrónica, la escritura o información puede trazarse en medios de almacenamiento físico (USB, disquetes, CD, tarjetas de memoria, etc.). Sin embargo, únicamente se puede acceder a la información a través de sistemas de cómputo que requieren equipos especiales para su visualización y comprensión.

Uno de los conceptos principales que fue establecido en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre Comercio Electrónico —y que posteriormente se incluyó en las reformas de mayo del 2000 al Código de Comercio— es el de mensaje de datos, el cual deberá ser sinónimo de documento electrónico, siendo la definición legal la ubicada en el artículo 89 del Código de Comercio: "La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología" complementada por su aceptación legal como prueba contenida en los artículos 89 bis: "No se negarán efectos jurídicos, validez o fuerza obligatoria a cualquier tipo de información por la sola razón de que esté contenida en un mensaje de datos" y 1061 Bis del mismo Código: "En todos los juicios mercantiles se reconoce como prueba la información generada o comunicada que conste en medios digitales, ópticos o en cualquier otra tecnología".[936]

La Ley Modelo de Comercio Electrónico antes mencionada, se basa en el reconocimiento de que los requisitos legales que prescriben el empleo de la documentación tradicional con soporte de papel constituyen el principal obstáculo para el desarrollo de la aplicación de los medios modernos de comunicación en los sectores económicos, por lo que busca establecer principios y bases mediante las cuales, cada país pueda apoyarse en la implementación de la aceptación y valoración probatoria de los acuerdos y contratos realizados a través de medios electrónicos, o en otras palabras, de documentos electrónicos.

934 Manning, G. (2012). "El correo electrónico como prueba en materia mercantil", en *Derecho Informático en México*. México. Editorial Popocatépetl, p. 49.

935 RAE. (2017). *Diccionario de la Real Academia Española.* Disponible en: http://dle.rae.es/ Fecha de consulta: agosto 2018.

936 Código de Comercio, última reforma DOF 28/03/2018, véase: http://www.diputados.gob.mx/LeyesBiblio/ pdf /3_280318.pdf

La finalidad de la Ley Modelo de Comercio Electrónico es la de ofrecer, a los legisladores de los países involucrados, reglas internacionalmente aceptadas que les permitan crear un marco jurídico confiable que brinde a los individuos certeza de las vías electrónicas de negociación designadas por el nombre de "comercio electrónico".[937]

Así mismo, las reformas de mayo de 2000 adicionaron diversas disposiciones del Código Federal de Procedimientos Civiles en donde, si bien no se plasma una definición del mensaje de datos o documento electrónico, sí se precisa su aceptación y valoración dentro del artículo 210 A.[938] En esta misma fecha se reformó la Ley Federal del Procedimiento Administrativo (LFPA)[939] para aceptar las promociones o solicitudes que los particulares presenten ante las entidades gubernamentales federales a través de medios de comunicación electrónica, así como permitirle a las entidades y dependencias de la administración pública federal realizar todo tipo de notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes o documentos y resoluciones administrativas, a través de estos mismos medios.

Si bien se puede observar que el Código de Comercio utiliza el mismo concepto y alcance del mensaje de datos que la normativa internacional, no toda la regulación mexicana está homologada o sigue los mismos criterios: el Código Fiscal de la Federación (CFF),[940] la

937 Sin embargo, en la *Guía de Incorporación de la Ley Modelo de Comercio Electrónico* en los comentarios al artículo primero (párrafo 26) se explica que existe la posibilidad de que el ámbito de aplicación abarque todo mensaje de datos, en cualquier ámbito de aplicación, sí así lo decide un país, proporcionando la redacción en caso de que esto suceda. La Ley Modelo de Comercio Electrónico no tiene como objetivo imponer la utilización de los medios electrónicos, sino, lo que es muy distinto, fomentar la igualdad jurídica entre estos y los tradicionales, por lo que contribuye con principios que deben aplicar a cualquier documento electrónico (mensaje de datos) sin importar la materia de regulación, quien lo haya generado o para quien este destinado.
Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

938 Código Federal de Procedimientos Civiles, última reforma DOF 09/04/2012, véase: http://www.diputados .gob.mx/LeyesBiblio/pdf/6.pdf
Artículo 210 A. Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. (…)

939 Ley Federal del Procedimiento Administrativo, última reforma DOF 18/05/2018, véase: http://www. diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf
Artículo 35. Las notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes o documentos y las resoluciones administrativas definitivas podrán realizarse: […]
II. […] También podrá realizarse mediante telefax, medios de comunicación electrónica o cualquier otro medio, cuando así lo haya aceptado expresamente el promovente, y siempre que pueda comprobarse fehacientemente la recepción de los mismos. […]
Tratándose de actos distintos a los señalados anteriormente, las notificaciones podrán realizarse […] a través de telefax, medios de comunicación electrónica u otro medio similar.
Artículo 69-C. En los procedimientos administrativos, las dependencias y los organismos descentralizados de la administración pública federal recibirán las promociones o solicitudes que, en términos de esta Ley, los particulares presenten por escrito, sin perjuicio de que dichos documentos puedan presentarse a través de medios de comunicación electrónica en las etapas que las propias dependencias y organismos así lo determinen […]. En estos últimos casos se emplearán, en sustitución de la firma autógrafa, medios de identificación electrónica.
El uso de dichos medios de comunicación electrónica será optativo para cualquier interesado. […] Los documentos presentados por medios de comunicación electrónica producirán los mismos efectos que las leyes otorgan a los documentos firmados autógrafamente y, en consecuencia, tendrán el mismo valor probatorio que las disposiciones aplicables les otorgan a éstos. […].

940 Código Fiscal de la Federación, última reforma DOF 25/06/2018, véase: http://www.diputados.gob.mx /LeyesBiblio/pdf/8_250618.pdf
Artículo 17-D. Cuando las disposiciones fiscales obliguen a presentar documentos, estos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente. Las autoridades fiscales, mediante reglas de carácter general, podrán autorizar el uso de otras firmas electrónicas. (…)
En los documentos digitales, una firma electrónica avanzada amparada por un certificado vigente sustituirá a la firma autógrafa del firmante, garantizará la integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.
Se entiende por documento digital todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología. […]

Ley Federal de Firma Electrónica,[941] la Ley Federal del Procedimiento Contencioso Administrativo (LFPCA)[942] y la Ley Federal del Trabajo (LT)[943] son normativas que modifican, de una forma no tan clara, los alcances de las definiciones del mensaje de datos o incluso lo diferencian erróneamente del documento electrónico o documento digital.

Lo anterior sucede principalmente porque la palabra "mensaje"[944] en su significado más clásico requiere de la comunicación de un originador a un destinatario, sin embargo, la *Guía de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional* (CNUDMI) sobre comercio electrónico clarifica el objetivo de la definición de mensaje de datos y señala que va más allá de las comunicaciones entre individuos o instituciones, ya que el objeto principal de dicha definición pretende abarcar toda información consignada en medios electrónicos o similares:

> 30. El concepto de "mensaje de datos" no se limita a la comunicación, sino que pretende también englobar cualquier información consignada sobre un soporte informático que no esté destinada a ser comunicada. Así pues, el concepto de "mensaje" incluye el de información meramente consignada. No obstante, nada impide que, en los ordenamientos jurídicos en que se estime necesario, se añada una definición de "información consignada" que recoja los elementos característicos del "escrito" en el artículo 6.
>
> […]
>
> 32. La definición de "mensaje de datos" pretende abarcar también el supuesto de la revocación o modificación de un mensaje de datos. Se supone que el contenido de un mensaje de datos es invariable, pero ese mensaje puede ser revocado o modificado por otro mensaje de datos. [945]

Por todo lo anterior, es posible señalar que los contratos, correos, notificaciones, actas, resoluciones, facturas, instrucciones, y cualquier información intercambiada, generada o almacenada a través de medios electrónicos u otras tecnologías deberán ser entendidas

941 Ley Federal de Firma Electrónica Avanzada, última reforma DOF 11/01/2012, véase: http://www. diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf
Artículo 2. Para los efectos de la presente Ley se entenderá por: [...]
Documento Electrónico: aquél que es generado, consultado, modificado o procesado por medios electrónicos; [...]
Mensaje de Datos: la información generada, enviada, recibida, archivada o comunicada a través de medios de comunicación electrónica, que puede contener documentos electrónicos; [...]

942 Ley Federal del Procedimiento Contencioso Administrativo, última reforma DOF 27/01/2017, véase: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf
Artículo 1-A.- Para los efectos de esta Ley se entenderá por: [...]
II. Archivo Electrónico: Información contenida en texto, imagen, audio o video generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología que forma parte del Expediente Electrónico
VIII. Documento Electrónico o Digital: Todo mensaje de datos que contiene texto o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología que forma parte del Expediente Electrónico. [...]
IX. Expediente Electrónico: Conjunto de información contenida en archivos electrónicos o documentos digitales que conforman un juicio contencioso administrativo federal, independientemente de que sea texto, imagen, audio o video, identificado por un número específico. [...]

943 Ley Federal del Trabajo última reforma DOF 22/06/2018, véase: http://www.diputados.gob.mx/Leyes Biblio/pdf/125_220618.pdf
Artículo 836-B. Para el desahogo o valoración de los medios de prueba referidos en esta sección, se entenderá por: [...]
h) documento digital: la información que solo puede ser generada, consultada, modificada y procesada por medios electrónicos, y enviada a través de un mensaje de datos; […]
ñ) mensaje de datos: al intercambio de información entre un emisor y un receptor a través de medios de comunicación electrónica; […]

944 RAE. (2017). *Diccionario de la Real Academia Española.* Disponible en: http://dle.rae.es/ Fecha de consulta: agosto 2018: Mensaje
1. m. Recado que envía alguien a otra persona.

945 Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, p. 27, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

como mensajes de datos o documento electrónico, y que por regla general deben ser aceptados como pruebas por las autoridades (jueces y tribunales) en cualquier materia procesal en México.

Sin embargo, no por el hecho de que deban ser aceptados quiere decir que el juzgador o la autoridad deban forzosamente otorgarle plenos efectos al mensaje de datos. Se requiere de un análisis de valoración probatoria, es decir, evaluar qué tanto le sirven estos elementos para cerciorase de que una persona realizó y/o estuvo en un momento determinado de acuerdo con el contenido de dicho mensaje de datos o documento digital, el cual no ha sido modificado y, por lo tanto, sus efectos pueden vinculársele.

En otras palabras, las autoridades y juzgadores tienen la obligatoriedad de recibir como elemento de prueba la información contenida en medios electrónicos o cualquier tecnología (mensaje de datos) y utilizar los siguientes elementos para valorar qué tanto le ayuda esta información al juzgador a conocer la verdad (fuerza probatoria): fiabilidad, integridad, accesibilidad y atribución.[946]

Cabe recalcar que los elementos antes descritos no son exclusivos para valorar la fuerza probatoria en el mundo digital, ya que los medios físicos aportados como pruebas también requieren análisis, pero la regulación no hace mención expresa de ello. El documento electrónico, por sí mismo, no tiene ningún impedimento diferente al que puede tener otro documento, como aquellos soportados en papel, ya que cualquier documento debe cumplir con las consideraciones y el proceso de validación del tradicionalmente aceptado y que opera en la actividad jurídica.[947]

Esta circunstancia especial es conocida como equivalencia funcional que significa que un mensaje de datos no es lo mismo que un documento soportado en papel, ya que es de naturaleza distinta, pero es equivalente para las funciones legales de demostrar un hecho u acto jurídico en cuanto logre demostrar su integridad, accesibilidad, atribución y fiabilidad. Por ello, para evitar interpretaciones erróneas, la regulación adopta un criterio flexible que toma en cuenta los requisitos aplicables a la documentación consignada sobre papel.

En conclusión, todo documento y/o contrato electrónico debe ser entendido como mensaje de datos, y éstos a su vez pueden ser definidos como cualquier información —comunicada o no— que se encuentre disponible en algún medio tecnológico, y por tanto están contemplados en la regulación para ser presentados como elemento de prueba en la mayoría de las materias jurídicas y valorados bajo los mismos requerimientos jurídicos que cualquier otra información soportada en medios físicos.

946 Estos elementos están contenidos en los artículos:
210-A del Código Federal de Procedimientos Civiles, última reforma DOF 09/04/2012, véase: http://www. diputados. gob.mx/LeyesBiblio/pdf/6.pdf
1834 bis del Código Civil Federal, última reforma DOF 09/03/2018, véase: http://www.diputados.gob.mx /LeyesBiblio / pdf/2_090318.pdf
93, 93bis y 1298 bis del Código de Comercio, última reforma DOF 28/03/2018, véase: http://www.diputados. gob.mx/ LeyesBiblio/pdf /3280318.pdf
6, 8 y 10 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

947 Davara, M. (2008). *Manual de Derecho Informático*. España. Thomson Aranzadi. Décima edición, p. 444.

NOTAS

NOTAS

NOTAS

Encargado

Isabel Davara Fernández de Marcos,[948]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La fracción XIX del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) define al encargado del tratamiento como "la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable".

En adición a lo anterior, el artículo 49 de la Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) señala que "el encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio".

El concepto de encargado, también se encuentra previsto en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), cuyo artículo 3, fracción XV lo definen como: "La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable".

Es decir, el concepto de encargado en la normatividad de datos personales en el sector público y en el privado es idéntico.

El artículo 108 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) robustece lo anterior pues señala que "el encargado es un prestador de servicios que realiza actividades de tratamiento de datos personales a nombre y por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita su ámbito de actuación para la prestación de un servicio".

948 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

En el ámbito regional, el concepto de encargado del tratamiento es definido por los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) como el "prestador de servicios, que con el carácter de persona física o jurídica o autoridad pública, ajena a la organización del responsable, trata datos personales a nombre y por cuenta de éste".

En el entorno internacional, cabe destacar que el Reglamento General de Protección de Datos Personales de la Unión Europea (RGPD o GDPR por sus siglas en inglés) establece en el apartado 8 de su artículo 4 que el encargado del tratamiento es "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

1. Elementos de la definición

Del contenido normativo de las definiciones anteriores, se advierte que cualquier encargado del tratamiento siempre cumplirá con las siguientes condiciones:

a) Tratar los datos por cuenta de un responsable. El encargado solo debe tratar los datos objeto del encargo para cumplir los fines del tratamiento que decida e instruya el responsable, no los suyos propios. Es decir, la condición de encargado se refiere y se mantiene únicamente en los tratamientos que se realicen por cuenta de uno o varios responsables siguiendo sus instrucciones.

b) No tiene poder de decisión acerca de los tratamientos. Las decisiones sobre el uso, destino y finalidad del tratamiento corresponden al responsable, siendo el encargado el que ejecuta sus instrucciones respecto al tratamiento.

c) Es ajeno a la organización del responsable. No debe confundirse al encargado del tratamiento con el empleado o empleados que realizan algún tratamiento dentro de la organización del responsable. El encargado pertenece a una entidad diferente, es decir, otra empresa, un profesional independiente o un prestador de servicios, por señalar algunos ejemplos.

Como decíamos, resulta esencial resaltar que el encargado se limita a actuar en virtud de las instrucciones conferidas por el responsable del tratamiento, y por eso la definición señala que éste ejecutará sus acciones "por cuenta del responsable". Por lo anterior, la condición de responsable o encargado del tratamiento viene determinada en virtud de la capacidad de decisión sobre los fines y medios del tratamiento, siendo el encargado un sujeto que no cuenta con dicha facultad exclusiva.

En relación con lo anterior, el Grupo de Trabajo del Artículo 29 (GTA29 o WP29 por sus siglas en inglés)[949] ha señalado que deben actualizarse dos condiciones básicas para que una persona física o moral pueda considerarse como encargado: a) el encargado debe ser una entidad legal separada respecto al responsable y b) el tratamiento de datos personales deberá darse por cuenta del responsable. Además, el GTA29 señala que la actividad de tratamiento por parte del encargado puede estar limitada a una tarea o contexto muy específico, o puede ser más general y extendida.

Con base en lo anterior, se puede afirmar que el elemento más importante de la figura del encargado es la prescripción de que este último actúe por cuenta del responsable.

949 Este grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

Así, es importante precisar que el tratamiento de datos personales se da bajo la figura de la remisión implicando lo siguiente:

- La comunicación o divulgación de datos personales entre un responsable y un encargado.[950] En virtud de la remisión el responsable comparte con el encargado determinados datos personales que serán sujetos a tratamiento.
- La remisión puede realizarse dentro o fuera del territorio nacional. Es decir, pueden existir remisiones nacionales e internacionales de datos personales.

En consecuencia, el encargado deberá realizar el tratamiento de los datos conforme a las instrucciones del responsable, que se concretarán en un contrato o instrumento jurídico vinculante, respetando los fines del tratamiento y los medios necesarios conforme a la legislación aplicable al tratamiento de datos personales.

2. Obligaciones del encargado del tratamiento

En relación con las obligaciones del encargado del tratamiento, podemos señalar que tanto el RLFPDPPP,[951] como la LGPDPPSO[952] coinciden en el establecimiento de las obligaciones para éste último.

De forma, específica, podemos precisar que la normatividad de datos personales señala como obligaciones del encargado del tratamiento las siguientes:

a) Dependencia: únicamente puede tratar los datos conforme a las instrucciones que le facilite el responsable.
b) Finalidad: debe abstenerse de tratar los datos para finalidades distintas a las instruidas por el responsable.
c) Seguridad: debe cumplir con las medidas de seguridad previstas en la normatividad de datos personales.
d) Confidencialidad: debe mantener la confidencialidad sobre los datos que trate y esta obligación subsistirá aún después de la finalización del contrato de prestación de servicios que le vincula al responsable.
e) Cancelación: una vez finalizada la relación, o siempre que el responsable se lo pida, debe suprimir los datos personales que trate, salvo una ley exija su conservación.
f) No transmisión: no podrá transferir ni remitir los datos a terceros, salvo que:
    1. El responsable le dé instrucciones para que lo haga.
    2. El responsable le permita específicamente subcontratar.
    3. Los requiera la autoridad competente en términos de Ley.

De forma concreta, los Lineamientos Generales señalan, en su artículo 109, que además de las cláusulas generales señaladas en el artículo 59 de la LGPDPPSO, el responsable deberá prever en el contrato o instrumento jurídico con el encargado las siguientes obligaciones:

a) Permitir al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de datos personales.

950 Para un estudio detallado de la figura del encargado del tratamiento recomendamos al lector consultar la definición de "encargado del tratamiento" de este diccionario.

951 Artículo 50 del RLFPDPPP.

952 Artículo 59 de la LGPDPPSO.

b) Colaborar con el INAI en las investigaciones previas que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y los Lineamientos Generales.

c) Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

En el ámbito regional, los Estándares Iberoamericanos indican, en su artículo 34.4 que el contrato o instrumento jurídico establecerá, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:

a) Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable.

b) Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable.

c) Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

d) Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones.

e) Guardar confidencialidad respecto de los datos personales tratados.

f) Suprimir, devolver o comunicar a un nuevo encargado designado por el responsable los datos personales objeto de tratamiento, una vez cumplida la relación jurídica con el responsable o por instrucciones de éste, excepto que una disposición legal exija la conservación de los datos personales, o bien, que el responsable autorice la comunicación de éstos a otro encargado.

g) Abstenerse de transferir los datos personales, salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad de control.

h) Permitir al responsable o autoridad de control inspecciones y verificaciones en sitio.

i) Generar, actualizar y conservar la documentación que sea necesaria y que le permita acreditar sus obligaciones.

j) Colaborar con el responsable en todo lo relativo al cumplimiento de la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

En el derecho internacional, específicamente en el apartado 3 del artículo 28 del RGPD encontramos las siguientes obligaciones para el encargado del tratamiento:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del derecho de la Unión Europea (UE) o de los estados miembros que se aplique al encargado.

b) Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.

c) Tomará todas las medidas necesarias para garantizar la seguridad de los datos personales.

d) Respetará las condiciones indicadas en los apartados 2 y 4 del artículo 28 para recurrir a otro encargado del tratamiento.

e) Asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que pue-

da cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.

f) Ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.

g) A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del derecho de la UE o de los estados miembros.

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones por parte del responsable o de otro auditor autorizado por dicho responsable.

i) Informará inmediatamente al responsable si, en su opinión, una instrucción infringe el RGPD u otras disposiciones en materia de protección de datos de la UE o de los estados miembros.

Respecto de la concreción de las anteriores obligaciones en la normatividad de datos personales, podemos presentar la siguiente comparativa entre la normatividad nacional y el RGPD:

Obligaciones del encargado del tratamiento	
RGPD	Normatividad nacional (RLFPDPPP y LGPDPPSO)
Tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional.	Tratar únicamente los datos personales conforme a las instrucciones del responsable. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.
Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.	Guardar confidencialidad respecto de los datos personales tratados.
Tomar todas las medidas necesarias de conformidad con el artículo 32 (seguridad del tratamiento).	Implementar las medidas de seguridad conforme a la normatividad aplicable.
Respetar las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento.	Guardar confidencialidad respecto de los datos personales tratados.
Asistir al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.	No aplica.

continúa...

Ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado.	No aplica.
A elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del derecho de la UE o de los Estados miembros.	Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.
Pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.	No aplica.
Informar inmediatamente al responsable si, en su opinión, una instrucción infringe el RGPD u otras disposiciones en materia de protección de datos de la UE o de los Estados miembros.	No aplica.

Subcontratación

En relación con esta figura, la normatividad de los sectores público y privado señala que toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último. Para una referencia detallada de esta figura, recomendamos al lector consultar la voz de "subcontratación" en la presente obra.

4. Responsabilidad del encargado del tratamiento.

En el supuesto de incumplimiento a las instrucciones del responsable, según disponen el artículo 53 del RLFPDPPP[953] y el artículo 60 de la LGPDPPSO,[954] el encargado será considerado como un responsable ilícito del tratamiento y en consecuencia, asumirá el carácter de responsable (ilícito, además) conforme a la legislación en la materia que le resulte aplicable, cuando destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o efectúe una transferencia, incumpliendo las instrucciones del responsable.

953 Remisiones de datos personales
Artículo 53. Las remisiones nacionales e internacionales de datos personales entre un responsable y un encargado no requerirán ser informadas al titular ni contar con su consentimiento.
El encargado será considerado responsable con las obligaciones propias de éste, cuando:
I. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable o
II. efectúe una transferencia, incumpliendo las instrucciones del responsable.
El encargado no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, remita los datos personales a otro encargado designado por este último, al que hubiera encomendado la prestación de un servicio o transfiera los datos personales a otro responsable conforme a lo previsto en el presente Reglamento.

954 Artículo 60. Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.

Equivalencia funcional

Jonathan Gabriel Garzón Galván

En el ámbito de las normas del uso de medios electrónicos en los actos jurídicos, resaltan varios principios en la interpretación, aplicación y regulación, como son los de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional. Estos principios se especifican, entre otros, en el artículo 89 del Código de Comercio.[955]

Este principio consistente en que el legislador, al regular el uso de los medios tecnológicos en los actos jurídicos, deberá expresar que se le atribuyen los mismos efectos legales a la documentación soportada en papel que aquella soportada en medios electrónicos, y lo mismo sucede con la firma electrónica y la autógrafa.

El concepto de equivalencia funcional se analiza en la *Guía de Incorporación* de la Ley Modelo de Comercio Electrónico de la Comisión de Naciones Unidad para el Derecho Mercantil Internacional (Ley Modelo), la cual precisa que, si bien los soportes en papel y las firmas autógrafas materialmente no son lo mismo que los documentos y firmas electrónicas, pueden tener las mismas funciones, y por tanto los mismo efectos legales, es decir, la función jurídica de los soportes en papel y firma autógrafa respecto de los actos jurídicos se cumplen instrumentalmente igual a través de medios electrónicos.[956]

Adicionalmente a lo ya comentado, este principio sirve para resolver la problemática de la originalidad del documento para la presentación de evidencias o pruebas de los actos jurídicos.[957] La originalidad del documento es una cuestión muy debatida en el entorno electrónico y tecnológico, donde las fronteras entre original y sus copias se vuelven confusas, dado que cualquier reproducción de un mensaje de datos es igual al original que permitió su reproducción, a diferencia de las copias en documentos soportados en papel, donde al reproducir copias de estos documentos, se pierden ciertas características con las cuales contaban los originales.

Así pues, la Ley Modelo sigue el criterio del equivalente funcional, basado en un análisis de los objetivos y funciones de la información con soporte en papel: la legibilidad, la posibilidad de validar su inalterabilidad a lo largo del tiempo, la autenticación de los datos consignados suscribiéndolos con una firma, entre otros, los cuales pueden ser logrados a través de medios tecnológicos, y por tanto los mensajes de datos o documentos electrónicos

955 Código de Comercio, última reforma DOF 28/03/2018, véase: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_280318.pdf
Artículo 89. (…)
Las actividades reguladas por este título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de datos en relación con la información documentada en medios no electrónicos y de la firma electrónica en relación con la firma autógrafa. (…)

956 Vargas, S. (2007). *Algunos comentarios sobre el comercio electrónico y la correduría* pública. México. Porrúa, p. 17.

957 Código Federal de Procedimientos Civiles, última reforma DOF 09/04/2012, véase: http://www.diputados .gob.mx/LeyesBiblio/pdf/6.pdf
Artículo 136. Los documentos privados se presentarán originales, y, cuando formen parte de un libro, expediente o legajo, se exhibirán para que se compulse la parte que señalen los interesados.
Ley Federal del Procedimiento Administrativo, última reforma DOF 18/05/2018, véase: http://www. diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf
Artículo 15-A. Salvo que en otra disposición legal o administrativa de carácter general se disponga otra cosa respecto de algún trámite:
I. Los trámites deberán presentarse solamente en original, y sus anexos, en copia simple, en un tanto. Si el interesado requiere que se le acuse recibo, deberá adjuntar una copia para ese efecto;(...)

y los documentos físicos, así como las firmas tradicionales y electrónicas, tienen la misma equivalencia en cuanto a sus funciones, a pesar de ser plasmadas y soportadas en medios distintos a los físicos.[958]

Incluso, la guía para su incorporación al derecho interno de la referida Ley Modelo señala que la información soportada en medios electrónicos ofrece un grado suficiente de cumplimiento con las funciones antes descritas, y en algunos casos, una mayor fiabilidad e inmediatez, especialmente respecto de la determinación del origen, destino y contenido del documento electrónico.[959]

A este respecto, el regulador deberá crear un entorno jurídico no discriminatorio al uso de medios electrónicos, ópticos o de cualquier otra tecnología, concediendo igualdad de trato jurídico a la documentación y a las firmas consignadas sobre papel, así como a la información y firmas consignadas en soporte informático.

En el mismo sentido, cuando las autoridades interpreten y apliquen las normas conforme a lo ya mencionado, deberán resolver sus actos sin otorgar un grado superior de valoración al acto realizado en medios físicos o tradicionales, que a los realizados a través de medios tecnológicos.

En los casos antes mencionados no debe entenderse que si algún acto está realizado por medios tecnológicos, la ley, por ese simple hecho, le reconozca plenos efectos jurídicos o mayor valor probatorio. La eficacia jurídica de dicho medio será equivalente, es decir, deberá comprobarse los mismos elementos probatorios que se requieren en los medios tradicionales: accesibilidad, integridad —y en su caso— autenticación y atribución.

La adopción del criterio del equivalente funcional busca que no se impongan normas legales o valoraciones probatorias más estrictas a los usuarios de los medios electrónicos, que las aplicables a usuarios que generen, almacenen o intercambien los documentos y evidencias en medios físicos o tradicionales.

Actualmente, varios cuerpos normativos ya contemplan que los documentos electrónicos producen los mismos efectos y tienen el mismo valor probatorio que los documentos físicos,[960] o bien, cuando la ley requiera que algún acto sea realizado por escrito, podrá realizarse a través de medios tecnológicos siempre y cuando se logre evidenciar las mismas funciones: accesibilidad, integridad, atribución y fiabilidad.[961]

958 Párrafo 16 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

959 Párrafo 16 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf.

960 69-C de la Ley Federal del Procedimiento Administrativo, última reforma DOF 18/05/2018, véase: http://www. diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf
17-D y 38, Código Fiscal de la Federación, última reforma DOF 25/06/2018, véase: http://www.diputados .gob.mx / LeyesBiblio/pdf/8_250618.pdf
58-F de la Ley Federal del Procedimiento Contencioso Administrativo, última reforma DOF 27/01/2017, véase: http:// www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf .

961 Artículo 6.1 de Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf
93 y 93 bis del Código de Comercio, última reforma DOF 28/03/2018, véase: http://www.diputados.gob.mx/ LeyesBiblio/pdf /3_280318.pdf;
1834 bis del Código Civil Federal, última reforma DOF 09/03/2018, véase: http://www.diputados .gob.mx/LeyesBiblio / pdf/2_090318.pdf.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos)

Jacobo Esquenazi Franco

1. Introducción

La Red Iberoamericana de Protección de Datos (RIPD), creada en 2003 con la participación de 14 países Iberoamericanos, se constituye en un foro permanente de intercambio de información abierto a todos los países miembros de la comunidad iberoamericana y permite el involucramiento de los sectores público, privado y social, con la finalidad de promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático y global.[962]

Durante el XV encuentro de la RIPD, en Santiago de Chile en 2017, se aprobaron los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos). Durante el encuentro se llegó a una serie de compromisos entorno al documento entre los que se incluyen:[963]

- difundir los Estándares Iberoamericanos en los foros nacionales e internacionales vinculados a la materia y
- promover la inclusión de las directrices establecidas en los mencionados estándares en la discusión de futuras reformas de las legislaciones nacionales o en la génesis de nuevas legislaciones tuitivas del derecho a la protección de datos personales.

Así, los Estados que forman parte de la RIPD convinieron adoptar los aludidos Estándares Iberoamericanos como máxima prioridad en la comunidad iberoamericana como directrices orientadoras para contribuir a la emisión de iniciativas regulatorias de protección de datos personales y la modernización y actualización de las legislaciones existentes.[964]

2. Contenido

Según su artículo primero, los Estándares Iberoamericanos tienen por objeto, entre otros, establecer un conjunto de principios y derechos de protección de datos personales que los Estados iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región.[965]

Los Estándares Iberoamericanos son de aplicación para las personas físicas o jurídicas de carácter privado, autoridades y organismos públicos que traten datos personales en el ejercicio de sus actividades y funciones.[966]

En lo que concierne a su ámbito de actuación objetivo, los Estándares Iberoamericanos se aplican al tratamiento de datos personales que obren en soportes físicos, automatizados —total o parcialmente— o en ambos soportes, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.[967]

962 *Vid*. Considerando 6 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

963 Red Iberoamericana de Protección de Datos Personales. (2017). Declaración del XV Encuentro de la Red Iberoamericana de Protección de Datos. Disponible en: http://www.redipd.es/documentacion/common/Declaracion_RIPD_XV_encuentro.pdf Fecha de consulta: 14 de noviembre 2018.

964 *Vid*. Considerando 26 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

965 *Vid*. Artículo 1, inciso a) de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

966 Artículo 3.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

967 Artículo 4.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

Respecto de su ámbito de aplicación territorial, [968] los Estándares referidos se aplican al tratamiento de datos personales efectuado:

1. Por un responsable o encargado establecido en territorio de los Estados iberoamericanos.
2. Por un responsable o encargado no establecido en territorio de los estados iberoamericanos, cuando las actividades del tratamiento estén relacionadas con la oferta de bienes o servicios dirigidos a los residentes de los Estados iberoamericanos, o bien, estén relacionadas con el control de su comportamiento, en la medida en que éste tenga lugar en los estados iberoamericanos.
3. Por un responsable o encargado que no esté establecido en un Estado iberoamericano, pero le resulte aplicable la legislación nacional de dicho Estado, derivado de la celebración de un contrato o en virtud del derecho internacional público.
4. Por un responsable o encargado no establecido en territorio de los estados iberoamericanos y que utilice o recurra a medios, automatizados o no, situados en ese territorio para tratar datos personales, salvo que dichos medios se utilicen solamente con fines de tránsito.

Otro aspecto relevante es el establecimiento de supuesto de excepción de aplicación de la normatividad de modo que los Estándares Iberoamericanos consignan que el derecho de protección de datos personales podrá para salvaguardar la seguridad nacional, la seguridad pública, la protección de la salud pública, la protección de los derechos y las libertades de terceros, así como por cuestiones de interés público.[969]

En su capítulo II, los referidos Estándares reconocen y regulan los principios del tratamiento de los datos personales:

- Principio de legitimación. En el artículo 11 establece las bases jurídicas para la legitimación del tratamiento de los datos personales.
- Principio de consentimiento. En los artículos 12 y 13 se prevén las reglas bajo las cuales resulta admisible el tratamiento de los datos mediante el consentimiento del titular, incluyendo condiciones para el tratamiento de datos de niños, niñas y adolescentes.
- Principio de licitud. Se regula en el artículo 14 y conmina al responsable a dar tratamiento a los datos con base en lo dispuesto por los Estándares y demás normatividad aplicable.
- Principio de lealtad. Este principio se reconoce en el artículo 15 y obliga al responsable a tratar los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratar éstos a través de medios engañosos o fraudulentos.
- Principio de transparencia. Se regula en el artículo 16 y obliga al responsable a informar al titular sobre la existencia misma y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.
- Principio de finalidad. Se regula en el artículo 17 y conmina al responsable a limitar el tratamiento de datos personales al cumplimiento de finalidades determinadas, explícitas y legítimas.
- Principio de proporcionalidad. Reconocido en el artículo 18, obliga al responsable a tratar los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario en relación con las finalidades que justifican su tratamiento.

968 Artículo 5.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

969 Artículo 6.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

- Principio de calidad. Se regula en el artículo 19 y obliga al responsable a adoptar las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.
- Principio de responsabilidad. Previsto en el artículo 20, establece la obligación de implementar los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los Estándares y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control.
- Principio de seguridad. Este principio, regulado en el artículo 21, obliga al responsable a mantener, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales.
- Principio de confidencialidad. Previsto en el artículo 23, señala la obligación del responsable de establecer controles o mecanismos para garantizar confidencialidad los datos personales.

El Capítulo III está destinado a los derechos de los titulares. Es en este capítulo se regulan los derechos de acceso, rectificación, cancelación y oposición (ARCO) y se añaden los derechos a no ser objeto de decisiones individuales automatizadas, a la portabilidad de los datos y a la limitación del tratamiento de los datos personales, mismos que reseñamos a continuación:

- Derecho a no ser objeto de decisiones individuales automatizadas. De acuerdo con el artículo 29, el titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o que le afecten de manera significativa, que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.
- Derecho a la portabilidad. De acuerdo con el artículo 30, cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable (o que sean objeto de tratamiento) en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.
- Derecho a la limitación del tratamiento de los datos personales. De acuerdo con el artículo 31 el titular tendrá derecho a que el tratamiento de datos personales se limite a su almacenamiento durante el periodo que medie entre una solicitud de rectificación u oposición hasta su resolución por el responsable.

En cuanto a la relación entre responsable y encargado, el capítulo IV de los Estándares regula dichos aspectos sobre una base bastante similar a la de la normatividad mexicana, y establece obligaciones para el encargado respecto del tratamiento de los datos y la obligación de que las partes formalicen el acuerdo respectivo.

Uno de los aspectos que llaman la atención es el de las transferencias internacionales que está regulado en el capítulo V y cuyo artículo 36.1 indica que el responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:

- El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de éste que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.
- El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado iberoamericano aplicable en la materia.
- El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados iberoamericanos aplicable en la materia.
- El exportador y destinatario adopten un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando sea acorde con las disposiciones previstas en la legislación nacional del Estado iberoamericano aplicable en la materia que está obligado a observar el exportador.
- La autoridad de control del Estado iberoamericano del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.

Un capítulo muy interesante es el VI, el cual está dedicado a las medidas proactivas en el tratamiento de datos personales y sugiere la adopción de las siguientes figuras:

- Privacidad por diseño: establece aplicar —desde el diseño— medidas preventivas de diversa naturaleza que permitan aplicar, de forma efectiva, los principios, derechos y demás obligaciones previstas en la legislación nacional aplicable en la determinación de los medios del tratamiento de los datos personales durante el mismo y antes de recabar los datos personales.[970]
- Privacidad por defecto: establece que el responsable debe garantizar que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional aplicable. [971]
- Oficial de protección de datos personales: se establece la obligación del responsable de designar un oficial de protección de datos personales o figura equivalente en los casos que establezca la legislación nacional aplicable.[972]
- Autorregulación: se establece la posibilidad de que el responsable pueda adherirse a esquemas de autorregulación vinculante que contribuyan a la correcta aplicación de la legislación nacional aplicable.[973]

970 Artículo 38.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

971 Artículo 38.2 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

972 Artículo 39 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

973 Artículo 40 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

- Evaluación de impacto a la privacidad (PIA): se establece la obligación del responsable de realizar un PIA de manera previa a la implementación de un tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares.[974]

El tema de las autoridades de control se regula en el capítulo VII y establece, entre otras cosas, la obligación de cada Estado iberoamericano de contar con una o más autoridades de control en materia de protección de datos personales con plena autonomía y de conformidad con su legislación nacional aplicable en la materia (artículo 42.1).

El capítulo VIII está destinado al régimen de reclamaciones y de imposición de sanciones, y de manera general indica que, todo titular tendrá derecho a presentar su reclamación ante la autoridad de control, así como recurrir a la tutela judicial para hacer efectivos sus derechos conforme a la legislación nacional aplicable (artículo 43.1).

Una novedad interesante es el derecho a la indemnización que aparece regulado en el capítulo IX, y cuyo artículo 44.1 recomienda que la legislación nacional reconozca el derecho que tiene el titular a ser indemnizado cuando hubiere sufrido daños y perjuicios como consecuencia de una violación de su derecho a la protección de datos personales.

Finalmente, el capítulo X y último de los Estándares se dedica al establecimiento de mecanismos de cooperación internacional y señala, en el artículo 45.1, que los Estados podrán adoptar mecanismos de cooperación internacional que faciliten la aplicación de las legislaciones nacionales aplicables en la materia.

Esquemas de mejores prácticas en materia de protección de datos personales

María Solange Maqueo Ramírez

Los esquemas de mejores prácticas son mecanismos complementarios al cumplimiento de la normatividad en materia de protección de datos personales que adoptan voluntariamente, los responsables del tratamiento de datos personales, sea de manera individual o colectiva, para acreditar el cumplimiento del principio de responsabilidad y rendir cuentas sobre el tratamiento de los datos personales tanto a los titulares de datos personales como a los órganos garantes o autoridades de control. Usualmente adoptan la forma de códigos de buenas prácticas, guías o políticas internas que rigen al interior de una organización, tanto pública como privada, a fin de establecer un estándar de protección de datos personales mayor al establecido por la ley y demás disposiciones jurídicas aplicables en la materia.[975]

En ese sentido, los esquemas de mejores prácticas presentan las siguientes características:

a) Su adopción es estrictamente voluntaria por parte del responsable del tratamiento de datos personales. No obstante, si dichos esquemas de mejores prácticas han sido validados o reconocidos por los órganos garantes del derecho a la protección de datos personales, su cumplimiento adquiere un carácter vinculante.
b) Tienen un carácter complementario al cumplimiento de los principios, deberes y obligaciones establecidos por la normatividad de protección de datos personales. Ello significa que las disposiciones jurídicas aplicables en la materia constituyen

974 Artículo 41 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

975 Cfr. INAI. (2017). *Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Manual del Participante*. México INAI, p. 36.

pisos mínimos que pueden ser superados por la adopción de esquemas de mejores prácticas, pero nunca contravenidos.

c) Permiten reforzar el cumplimiento del principio de responsabilidad demostrada o *accountability* de manera que sea factible que el responsable del tratamiento de datos personales acredite —ante las autoridades competentes, o bien, ante el titular de datos personales— el cumplimiento de los principios, deberes y obligaciones en materia de protección de datos personales. Si bien existen ciertas medidas obligatorias para comprobar el cumplimiento del principio de responsabilidad establecido por la ley,[976] lo cierto es que la adopción de esquemas de mejores prácticas puede coadyuvar, de manera efectiva, a su cumplimiento.[977]

La implementación de esquemas de mejores prácticas redunda en beneficios para el responsable del tratamiento de datos personales. Por ejemplo, por lo que hace a los responsables, estas prácticas incrementan la confianza de los consumidores o usuarios y son tomadas en consideración al momento de evaluar una posible imposición de sanciones por incumplimiento de la ley; en cuanto a la sociedad en general, cabe decir que coadyuvan a la tutela y efectividad del derecho humano a la protección de datos personales.

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos), adoptados en el marco del XV encuentro de la Red Iberoamericana de Protección de Datos (RIPD), ponen especial énfasis en el establecimiento de esquemas de mejores prácticas u otras medidas afines en dos situaciones: cuando los datos personales son tratados por parte de un encargado a nombre y cuenta del responsable y cuando se realizan transferencias —nacionales o internacionales— de datos personales.[978]

a) Tiene un carácter preventivo dado que coadyuva "a robustecer los controles de protección de datos personales implementados" y puede utilizarse, conjuntamente con la evaluación de impacto en la protección de datos personales "para prevenir o mitigar riesgos en los tratamientos de datos personales".[979]

b) Los esquemas de mejores prácticas, a fin de que sean efectivos, deben tomar en consideración, como mínimo, la naturaleza de los datos personales, las finalidades de su tratamiento, la capacidad económica y técnica de los responsables del tratamiento de los datos personales, así como el desarrollo tecnológico y las técnicas existentes.[980]

976 Cfr. Artículo 30 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

977 Cfr. Artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y artículo 47 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *Diario Oficial de la Federación* el 21 de diciembre de 2011.

978 Numeral 20.2 de los Estándares de Protección de Datos Personales de los Estados Iberoamericanos, aprobados en junio de 2017. Una disposición análoga se puede encontrar en el artículo 46 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

979 INAI. (2017). *Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Manual del Participante*. México. INAI, p. 35. Al respecto, también véase Mendoza, O. (2018, enero-junio, 2018). "Marco jurídico en la protección de datos personales en las empresas establecidas en México", en *Revista del Instituto de Ciencias Jurídicas de Puebla,* vol. 12, núm. 41, p. 285.

980 Cfr. Artículo 39 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados no establece estas consideraciones de manera específica para los esquemas de mejores prácticas, no obstante, las contempla respecto de otras medidas obligatorias que deberá adoptar el responsable del tratamiento de datos personales para el cumplimiento del principio de responsabilidad, por lo que puede hacerse extensiva su interpretación en este sentido.

Además, el responsable debe revisarlos y evaluarlos permanentemente "con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable".[981]

1. Objeto

El artículo 72 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) aplicable para el sector público establece que los esquemas de mejores prácticas, entre otros mecanismos, tendrán por objeto:

a) elevar el nivel de protección de los datos personales;
b) armonizar el tratamiento de datos personales en un sector específico;
c) facilitar el ejercicio de los derechos ARCO por parte de los titulares;
d) facilitar las transferencias de datos personales;
e) complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales y
f) demostrar ante el Instituto o ante los organismos garantes el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

Por lo que hace al régimen jurídico aplicable para el sector privado, el artículo 80 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) establece que los esquemas de autorregulación, entre los que se encuentran los esquemas de mejores prácticas, tendrán los siguientes objetivos primordiales:

a) coadyuvar al cumplimiento del principio de responsabilidad al que refiere la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el presente RLFPDPPP;
b) establecer procesos y prácticas cualitativos en el ámbito de la protección de datos personales que complementen lo dispuesto en la LFPDPPP;
c) fomentar que los responsables establezcan políticas, procesos y buenas prácticas para el cumplimiento de los principios de protección de datos personales, garantizando la privacidad y confidencialidad de la información personal que esté en su posesión;
d) promover que los responsables de manera voluntaria cuenten con constancias o certificaciones sobre el cumplimiento de lo establecido en la LFPDPPP y mostrar a los titulares su compromiso con la protección de datos personales;
e) identificar a los responsables que cuenten con políticas de privacidad alineadas al cumplimiento de los principios y derechos previstos en la LFPDPPP, así como de competencia laboral para el debido cumplimiento de sus obligaciones en la materia;
f) facilitar la coordinación entre los distintos esquemas de autorregulación reconocidos internacionalmente;
g) facilitar las transferencias con responsables que cuenten con esquemas de autorregulación como puerto seguro;
h) promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de privacidad, incluyendo herramientas de transparencia, supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación y

981 Red Iberoamericana de Protección de Datos Personales. (2017). *Estándares de Protección de Datos Personales*, numeral 20.4, aprobados en junio de 2017.

i) encauzar mecanismos de solución alternativa de controversias entre responsables, tituilares y terceras personas, como son los de conciliación y mediación.

En términos generales, todos estos objetivos, sea en el ámbito público o privado, tienen por objeto demostrar el compromiso de los responsables del tratamiento de datos personales con el derecho a la protección de datos personales.

2. Clasificación

Los esquemas de mejores prácticas pueden ser nacionales o internacionales; ser adoptados en lo individual por parte de un responsable del tratamiento de datos personales o de acuerdo con otros responsables, encargados u organizaciones civiles o gubernamentales y, finalmente, pueden estar o no reconocidos y validados por las autoridades de control u órganos garantes competentes para tales efectos.

Por lo que se refiere a la primera clasificación, cabe decir que, en términos del artículo 43 de la LFPDPPP, es facultad de la Secretaría de Economía emitir los parámetros que correspondan para el correcto desarrollo e implementación de los esquemas de mejores prácticas.[982] Tratándose de datos personales en posesión del sector público, esta facultad está encomendada al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y a los órganos garantes de cada entidad federativa en el ámbito de su competencia, de conformidad con el artículo 73 de la LGPDPPSO. Cabe advertir que el seguimiento de estos parámetros cobra especial relevancia si se desea que exista una validación o reconocimiento de los esquemas de mejores prácticas implementados.

En cualquiera de ambos casos, las mejores prácticas que llegaren a implementarse por parte de los responsables del tratamiento de datos personales pueden tener un origen nacional o internacional (v. gr. el Código de Buenas Prácticas para Proyectos Big Data de la Agencia Española de Protección de Datos Personales o *The Employment Practices Code* en el Reino Unido o la Guía para el uso de drones, emitida por la *National Communications and Information Administration* en Estados Unidos y consensuada con diversas empresas multinacionales).[983]

La segunda clasificación atiende al carácter de quien adopta las mejores prácticas. Pueden ser implementadas por un solo responsable del tratamiento de datos personales, o bien, por un conjunto de responsables del tratamiento, por ejemplo, dentro de un sector específico e, incluso, responsables del tratamiento en connivencia con organizaciones de la sociedad civil o las autoridades gubernamentales.

Finalmente, la tercera clasificación atiende al carácter vinculante o no de los esquemas de mejores prácticas. Para esos efectos, en el ámbito del sector público, la LGPDPPSO, en su artículo 73, faculta a los diversos órganos garantes del derecho a la protección de datos personales para validar o reconocer esquemas de mejores prácticas, siempre que cumplan con los parámetros y los procedimientos para su evaluación que para tal efecto emitan dichas autoridades de control. Los esquemas de mejores prácticas que hayan sido validados

982 Cfr. Secretaría de Economía. (2014). "Parámetros de Autorregulación en materia de Protección de Datos Personales", publicados en el *Diario Oficial de la Federación* el 29 de mayo de 2014. De igual forma cabe mencionar el Acuerdo del Pleno del Instituto Federal de Acceso a la Información y Protección de Datos Personales, por el que se aprueba el Proyecto de Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante y se instruye su publicación oficial, publicadas en el *Diario Oficial de la Federación* el 18 de febrero de 2015, aplicables para el sector privado.

983 La sección 5 del capítulo IV del Reglamento (UE)2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), hace referencia a los códigos de conducta y la certificación con la finalidad de contribuir a la correcta aplicación de este ordenamiento y que los responsables del tratamiento puedan efectivamente demostrar dicho cumplimiento, respectivamente.

o reconocidos por los órganos garantes deberán estar inscritos en un registro administrado por los mismos. Además, en los términos de este precepto, los órganos garantes de las entidades federativas podrán solicitar su inscripción en el registro administrado por el INAI, de conformidad con las disposiciones que establezca este último.

Por su parte, en el ámbito del sector privado, tanto la LFPDPPP como el RLFPDPPP contemplan diversos mecanismos de autorregulación vinculante, mismos que deberán cumplir con los parámetros que para tales efectos fije la Secretaría de Economía, además de ser notificados al INAI. En el supuesto de que los esquemas de autorregulación vinculante hayan sido efectivamente validados por el Instituto, deberán de estar inscritos en el Registro de Esquemas de Autorregulación Vinculante (REA) y los responsables del tratamiento de los datos personales que los hayan desarrollado o que se hayan adherido a los mismos podrán, mediante previa autorización, utilizar el logotipo "REA INAI".[984]

Estándares de seguridad

Uciel Fragoso Rodríguez

Los estandares, tal como lo define ISO,[985]son "acuerdos documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías o definiciones de características para asegurar que los materiales, productos, y servicios cumplan con su propósito".

En este sentido, los estándares de seguridad garantizan el correcto diseño, implementación, mantenimiento, supervisión y ajuste de las políticas, procedimientos y controles que tienen como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información y en particular de los datos personales.

Los estándares pueden ser clasificados en dos categorías según su origen de creación:

a) estándar de *facto*
b) estándar de *iure*

Los estándares de *facto* son creados por individuos u organizaciones que tienen un interés en común y constituyen especificaciones o normas seguidas en forma voluntaria por las organizaciones debido a su efectividad y amplia aceptación. Un ejemplo de este tipo son los estándares OWASP[986] desarrollados para garantizar la seguridad de la información en aplicaciones *web*.

Por otro lado, los estándares de *iure* son generados por organizaciones oficiales a nivel nacional o internacional con una estructura y metodología de generación de estándares formal. Como ejemplos de organizaciones de estandarización nacional e internacional tenemos a ISO, BSI,[987] ITU,[988] NIST,[989] entre otros. En el caso de estándares de seguridad

984 INAI. (2017). "Acuerdo mediante el cual se aprueban las reglas del uso del logotipo del Registro de Esquemas de Autorregulación Vinculante REA INAI y condiciones para su autorización", publicado en el *Diario Oficial de la Federación* el 7 de abril de 2017. De igual forma véase el acuerdo del Pleno del Instituto Federal de Acceso a la Información y Protección de Datos Personales por el que se aprueba el Proyecto de Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante y se instruye su publicación oficial, publicado en el *Diario Oficial de la Federación* el 18 de febrero de 2015.

985 International Organization for Standardization.

986 Open Web Application Security Project.

987 British Standards Institution.

988 International Telecommunication Union.

989 National Institute of Standards and Technology.

tenemos como ejemplo al ISO/IEC 27000[990] que consiste en una familia de estándares para la seguridad de la información.

Cuando las organizaciones operan bajo estándares garantizan la sistematización de la planeación, el diseño, la implementación y el mantenimiento de los procesos de negocio de la organización.

Se puede trabajar con estándares de *facto* o de *iure*, pero también es común que las organizaciones tomen lo más adecuado de diferentes estándares y generen su estándar propio que se adapta mejor a sus requerimientos.

Los beneficios de operar bajo estándares son múltiples: se optimiza el uso de recursos, se da certeza en la operación, representa una ventaja competitiva y eventualmente permite garantizar el cumplimiento de requerimientos legales.

Los estándares de seguridad ayudan al establecimiento y mantenimiento de acciones estratégicas (gobierno de la seguridad de la información) y de las acciones tácticas (gestión de la seguridad de la información).

En el caso del gobierno de seguridad de la información, existen estándares de seguridad para:

a) establecer una estrategia de seguridad de la información,
b) conformar un gobierno de seguridad de la información,
c) crear políticas de seguridad y
d) llevar a cabo un análisis de impacto al negocio (BIA por sus siglas en inglés)

Para la gestión de seguridad de la información, existen estándares que apoyan en el diseño e implementación de las fases de un sistema de gestión de seguridad de la información, las cuales son: planificar, hacer, verificar y actuar.

Los estándares para la gestión de la seguridad de la información permiten —entre otras actividades:

a) clasificar la información,
b) realizar un análisis de riesgo,
c) seleccionar los controles o medidas de seguridad,
d) monitorear el desempeño de los controles y
e) auditar los sistemas de gestión

Para el caso de la protección de datos personales, la LFPDPPP[991] en su artículo 39, establece lo siguiente con relación a los estándares de seguridad:

> Artículo 39. El Instituto tiene las siguientes atribuciones:
>
> V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable…

El responsable del tratamiento de los datos personales podrá apoyarse en estándares y mejores prácticas de seguridad de la información para proteger los datos según su naturaleza y por lo tanto su riesgo inherente.

990 ISO/IEC 27000 family – Information security management systems.

991 DOF. (2010, julio). "Ley Federal de Protección de Datos Personales en Posesión de los Particulares", en *Diario Oficial de la Federación.* Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) en su *Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales (*GISGSDP)[992] describe un estándar de seguridad para la implementación de un sistema de gestión de seguridad para los datos personales.

Las fases para implementar el sistema de gestión son:

1) Planear. Consiste en establecer el alcance y los objetivos del sistema de gestión, elaborar una política de gestión de datos personales, asignar funciones y obligaciones, realizar un inventario de datos personales, llevar a cabo un análisis de riesgo e identificar las medidas de seguridad.
2) Implementar. Fase en donde se ponen en marcha las políticas, procesos, procedimientos y medidas de seguridad que hayan resultado según el análisis de riesgo.
3) Monitorear. Se realiza una medición y evaluación de las medidas implementadas para verificar que se logró la mejora esperada.
4) Mejorar. Fase que permite adoptar medidas correctivas y preventivas en función de los resultados obtenidos en la fase anterior.

La Guía es creada tomando como base los siguientes estándares internacionales:

a) *BS 10012:2009 Data protection-Specification for a personal information management system*
b) *ISO/IEC 27001:2013, Information technology-Security techniques-Information security management systems-Requirements*
c) *ISO/IEC 27002:2013, Information technology-Security techniques-Code of practice for information security controls*
d) *ISO/IEC 27005:2008, Information Technology-Security techniques-Information security risk management*
e) *ISO/IEC 29100:2011 Information technology-Security techniques-Privacy framework*
f) *ISO 31000:2009, Risk management-Principles and guidelines*
g) *ISO GUIDE 72, Guidelines for the justification and development of management systems standards*
h) *ISO GUIDE 73, Risk management-Vocabulary*
i) *ISO 9000:2005, Quality management systems-Fundamentals and vocabulary*
j) *NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems*
k) *OECD Guidelines for the Security of Information Systems and Networks-Towards a Culture of Security*

Los estándares internacionales en los que se basaron para la elaboración de la GSGSDP son los siguientes:

Para la especificación general del sistema de gestión de seguridad de datos personales:

1) BS 10012:2009 es un estándar británico emitido por el gobierno del Reino Unido para garantizar la privacidad de la información personal sensible tratada por las corporaciones británicas.
2) ISO/IEC 27001:2013 es un marco de trabajo para la especificación de un sistema de gestión de seguridad de la información (ISMS por sus siglas en inglés). Estándar desarrollado por el ISO como parte de la serie de estándares de seguridad ISO/IEC 27000.

992 INAI. (2015, junio). Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. INAI, pp. 14-15. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

3) ISO/IEC 29100:2011 estándar desarrollado por ISO enfocado al establecimiento de un marco de trabajo para la protección de la privacidad de la información de identificación personal (PII).
4) ISO GUIDE 72 es una guía publicada por ISO para la correcta creación de estándares enfocados a la gestión de sistemas o documentos comparables.
5) NIST SP 800-14 es una publicación especial generada por NIST que provee los fundamentos para que las organizaciones puedan establecer y revisar programas de seguridad de tecnologías de la información.

Para la especificación e implementación de cada una de las cuatro fases de la guía fueron utilizados los siguientes estándares:

1) OECD Guidelines for the Security of Information Systems and Networks es una guía elaborada por la OECD[993] para establecer un marco de trabajo de principios aplicables a toda persona involucrada en la seguridad de los sistemas de información y redes de comunicaciones.
2) ISO 9000:2005 es un conjunto de normas sobre calidad y gestión de la calidad, establecidas por ISO. Pueden ser aplicadas a cualquier tipo de organización y actividades orientadas a la producción de bienes y servicios.
3) ISO GUIDE 73 guía creada por ISO y que provee la definición de términos genéricos relacionados con la descripción consistente y coherente de actividades para la gestión del riesgo.
4) ISO/IEC 27005:2008 estándar que provee información para desarrollar e implementar un proceso de gestión de riesgo para las tecnologías de la información y alineado a la gestión de riesgos empresariales. Estándar desarrollado por ISO.
5) ISO 31000:2009 es una familia de normas creadas por ISO con el objeto de proporcionar directrices para la gestión de riesgos y el proceso de implementación a nivel estratégico y operativo. El estándar puede aplicarse para gestionar riesgos en cualquier área.

ISO/IEC 27002:2013 es un código de práctica perteneciente a la serie de estándares de seguridad ISO/IEC 27000 desarrollado por ISO y que tiene como objetivo la selección correcta de las medidas de seguridad que fueron identificadas como resultados del análisis de riesgo.

El INAI generó el documento TEFES[994] que consiste en un material de referencia para los responsables y encargados del tratamiento de datos personales, que permite evaluar si la implementación de estándares de seguridad de amplia aceptación a nivel internacional facilita el cumplimiento de los requisitos y obligaciones especificados en la legislación vigente en materia de protección de datos personales.

993 The Organization for Economic Cooperation and Development.

994 INAI. (2015, junio). *Tabla de equivalencia funcional entre estándares de seguridad y la LFPDPPP, su reglamento y las recomendaciones en materia de seguridad de datos personales.* INAI. Disponible en: http://inicio.inai.org.mx/DocumentosdeInteres/Tabla_de_Equivalencia_Funcional(Junio2015).pdf

Ética en la protección de datos personales

Erik Huesca Morales

La ética en la protección de datos personales significa la responsabilidad que adquieren las empresas, dependencias, gobiernos y/o cualquiera otro ente que trate datos personales a grandes escalas de comprender y evaluar los tratamientos de datos personales que llevan a cabo con el propósito de identificar los impactos positivos y negativos tanto en el ámbito operacional, como en el de la protección de los derechos humanos de la persona cuyos datos personales están siendo sujetos a tratamiento.

El gran volumen de datos sujeto a tratamiento derivado del uso de la *data* mediante algoritmos avanzados puede llegar a tener un impacto positivo en la vida de las personas (salud, negocios, consumo, seguridad, etc.), así como en la sociedad (prevención de enfermedades, disminución de contaminación, etc.). Sin embargo, estos mismos datos y tecnologías pueden generar una repercusión no deseable para el individuo e incluso causarle un daño. Como consecuencia de lo anterior, diversos expertos en materia de protección de datos personales enfatizan la necesidad de contar con una forma evolucionada de responsabilidad, mediante el uso de la ética, para ser aplicada al uso de tecnología avanzada que se sustenta en datos, y así poder impulsar el uso de estos datos sin causar un daño a los titulares.

En este sentido, podemos afirmar que la necesidad de la ética en la protección de datos personales nace como consecuencia de los tratamientos masivos de datos personales que se están llevando a cabo derivado del auge de las tecnologías basadas en datos (*big data*, inteligencia artificial, aprendizaje de máquinas, cómputo en la nube, etc.) Derivado de la naturaleza del tratamiento de datos personales que se materializa con el uso de tecnologías como las antes señaladas, se ha creado un vacío entre los requerimientos legales aplicables al derecho de protección de datos personales y el uso que requieren dar las empresas y/o cualquier otro ente a los datos personales como parte del uso de las mencionadas tecnologías. Esto es, la complejidad de las tecnologías basadas en datos personales está provocando que los marcos legales actuales de protección de datos personales se vean rebasados. Para cubrir este vacío, diversos expertos en la materia de protección de datos personales han sugerido la necesidad de implementar la ética en los tratamientos de datos personales que se llevan a cabo derivado del uso de las tecnologías ya referidas.

La ética en la protección de datos conlleva que las empresas, dependencias, gobiernos y/o cualquiera otro ente que trate datos personales a grandes escalas designe al interior de su organización a los llamados *data stewards*, que son personas que, al interior de la organización, tiene la responsabilidad de velar por los intereses de todas las partes involucradas en el sentido de buscar maximizar los beneficios para todos, sin que lo anterior implique un riesgo para los titulares de los datos personales o cualquier otro tercero involucrado. En otras palabras, los *data stewards* deben cerciorarse de que los tratamientos de datos personales a grandes escalas sean lícitos y justos.

Puede decirse que la ética en la protección de datos personales es el establecimiento abierto y preciso de las normas éticas en la recolección, gestión y uso de los datos que hacen programas específicos para su manipulación y que son dependientes directamente de la ética del programador o de la organización que lo desarrolla. La ética en el manejo de los datos no solo debe estar ligada a los datos personales, sino a todo manejo de datos. La ética debe ser explicita para todo tratamiento de datos desde su recolección, procesamiento, almacenamiento y hasta su destrucción.

El establecimiento de estas normas puede ser de carácter universal como es el caso de las Pautas Éticas Internacionales para la Investigación Biomédica en Seres Humanos establecidas por la OMS[995] desde 2002 y que han estado en constante revisión o de carácter selectivo, como es el caso de la recolección de datos por objetos[996] sobre nuestro quehacer cotidiano. La recolección selectiva puede ser desde patrones de consumo, hasta preferencias políticas. Lo que permite a quien manipula los datos inducir tendencias en el consumo e incluso en las decisiones políticas de una localidad o región.

Por ello, es conveniente explicitar para cada conjunto de datos recabados al menos las siguientes tres descripciones: fuente de datos, propósito del uso de los datos y gestión de riesgos. En todos los casos es importante indicar el impacto que el manejo de un objeto o programa tendrá sobre los datos y sus implicaciones sobre las personas a las que les corresponden los datos. Por ello, es importante definir la escala de valores desde una ética que considere los derechos humanos.

Evaluación de Impacto en la Protección de Datos Personales (EIPD)

Isabel Davara Fernández de Marcos,[997]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La Evaluación de Impacto en la Protección de Datos Personales, también conocida como *Privacy Impact Assesment* en inglés (EIPD o PIA respectivamente) es un proceso concebido para describir el tratamiento de los datos personales, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinando las medidas para abordarlos.[998]

En el ámbito normativo mexicano,[999] la EIPD se define en la fracción XVI del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) como "el documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales,[1000] valoran los impactos reales respecto

995 Recuperado de: https://cioms.ch/wp-content/uploads/2017/12/CIOMS-EthicalGuideline_SP_INTERIOR-FINAL.pdf Fecha de consulta: agosto 2018.

996 Como es el caso de la interacción de las personas con la Internet de los Objetos o con programas de Inteligencia Artificial

997 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

998 Grupo de Trabajo del Artículo 29. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/679, adoptadas el 4 de abril de 2017.

999 En relación con el contenido de esta voz es pertinente destacar que la concepción normativa de la EIPD se realiza partiendo de la normatividad aplicable al sector público en virtud de que a la fecha de elaboración de este documento, en el sector privado no existe una previsión normativa específica que regule las EIPD como si existe en el sector público.

1000 En relación con la definición del tratamiento intensivo de datos personales, el artículo 120 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público indica en lo siguiente:
[…]
Para efectos de los presentes Lineamientos Generales y en términos de lo dispuesto por el artículo 75 de la Ley General, el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales cuando concurra cada una de las siguientes condiciones:
I. Existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales, las categorías de titulares involucrados; el volumen total de los datos personales tratados; la

de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable".[1001]

La elaboración de una EIPD se ha convertido en un requisito previo imprescindible en la práctica y exigido por la normatividad aplicable al sector público, y así, el artículo sexto de las Disposiciones Administrativas de Carácter General para la Elaboración, Presentación y Valoración de Evaluaciones de Impacto en la Protección de Datos Personales (en adelante Disposiciones sobre EIPD), en términos bastante similares a la definición normativa antes referida, indican que la EIPD es "un documento mediante el cual el responsable valora los impactos reales respecto de un tratamiento intensivo o relevante de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes, derechos y demás obligaciones en la materia, de acuerdo con lo dispuesto en el artículo 3, fracción XVI de la LGPDPPSO".

No obstante la definición anterior, la EIPD —aunque se concreta formalmente en un documento en el que se plasman los resultados observados y obtenidos de los tratamientos que podrían entrañar riesgos en los derechos de los titulares— tiene un efecto más profundo y se puede definir también como "una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas".[1002]

En este contexto, respecto del potencial de la EIPD para apoyar a los responsables (y encargados) en el cumplimiento de las obligaciones establecidas en la normatividad de datos personales, el Grupo de Trabajo del Artículo 29 (GTA29 o WP29 por sus siglas en inglés) ha señalado que éstas "son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos de la normatividad, sino también a demostrar que se han tomado medidas adecuadas para garantizar su cumplimiento".[1003]

---

cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas;
II. Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General, entendidos como que se refieren a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual, y
III. Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General, según corresponda, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa más no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares involucrados; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los datos destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

1001 Artículo 3. Para los efectos de la presente Ley se entenderá por:
[…]
XVI. Evaluación de impacto en la protección de datos personales: documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;
[…]

1002 Agencia Española de Protección de Datos. (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD*. Disponible en: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf Fecha de consulta: 25 de septiembre de 2018.

1003 Grupo de Trabajo del Artículo 29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/679, adoptadas el 4 de abril de 2017.

En definitiva, la EIPD es una herramienta imprescindible —obligada por la normatividad aplicable a la Administración Pública Federal en México— que permite evaluar con anticipación cuáles son los potenciales riesgos[1004] a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. [1005]

1. Objeto de la EIPD

La EIPD tiene una crucial importancia en el cumplimiento al principio de responsabilidad, pues permite al responsable determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable. [1006]

Por lo tanto, el artículo 7 de las disposiciones sobre EIPD[1007] indica que la EIPD tiene por objeto:

a) Identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales.

b) Describir las acciones concretas para la gestión de los riesgos señalados en el numeral 1.

c) Analizar y facilitar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la LGPDPPSO o las legislaciones estatales en la materia y demás disposiciones aplicables, respecto a tratamientos intensivos o relevantes de datos personales.

d) Fomentar una cultura de protección de datos personales al interior de la organización del responsable.

En la práctica, la EIPD destaca por ser una herramienta que permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.[1008]

1004 En este contexto el Reglamento General de Protección de Datos dispone en su Considerando 84 lo siguiente:
(84) A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

1005 Agencia Española de Protección de Datos. (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD*.

1006 Agencia Española de Protección de Datos. (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD*.

1007 Objeto de la evaluación de impacto en la protección de datos personales
Artículo 7. La evaluación de impacto en la protección de datos personales tiene por objeto:
I. Identificar y describir los altos riesgos potenciales y probables que entrañen los tratamientos intensivos o relevantes de datos personales;
II. describir las acciones concretas para la gestión de los riesgos a que se refiere la fracción anterior del presente artículo;
III. analizar y facilitar el cumplimiento de los principios, deberes, derechos y demás obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables, respecto a tratamientos intensivos o relevantes de datos personales y
IV. fomentar una cultura de protección de datos personales al interior de la organización del responsable.

1008 Agencia Española de Protección de Datos. (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD*.

2. Obligación de elaborar la EIPD

En las normatividades de datos personales, la elaboración de la EIPD se constituye como una obligación del responsable del tratamiento para prevenir, mitigar y detectar potenciales riesgos que pudieran afectar los derechos y libertades fundamentales del titular de los datos personales.

En el ámbito internacional, el Reglamento General de Protección de Datos Personales (RGPD o GDPR por sus siglas en inglés) indica en su artículo 35, que el responsable del tratamiento debe realizar la EIPD antes del tratamiento en aquellos casos en los que sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.[1009]

Por otro lado, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) señalan, en su artículo 41.1, que la EIPD será requerida cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que por su naturaleza, alcance, contexto o finalidades sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares y se realizará, de manera previa a la implementación del mismo, una evaluación del impacto a la protección de los datos personales.[1010]

1009 El Reglamento General de Protección de Datos Personales en su artículo 35 indica lo siguiente:
Artículo 35
Evaluación de impacto relativa a la protección de datos
1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

1010 41. Evaluación de impacto a la protección de datos personales.
41.1. Cuando el responsable pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares, realizará, de manera previa, a la implementación del mismo una evaluación del impacto a la protección de los datos personales.

En el ámbito nacional, la LGPDPPSO[1011] indica que será necesario elaborar la EIPD cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con la normatividad de datos personales impliquen el tratamiento intensivo o relevante de datos personales de manera general[1012]o particular.[1013]

1011 Artículo 74. Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.
El contenido de la evaluación de impacto a la protección de datos personales deberá determinarse por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

1012 En este contexto el artículo 8 de las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales señalan que el tratamiento intensivo de datos personales de carácter generales: Artículo 8. Para efectos de las presentes Disposiciones Administrativas y en términos de lo dispuesto en el artículo 75 de la Ley General, el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales cuando concurra alguna las siguientes condiciones:
I. Existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas.
II. Se traten datos personales sensibles a los que se refiere el artículo 3, fracción X de la Ley General o los que correspondan en las legislaciones estatales en la materia, entendidos como aquellos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa mas no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual, y
III. Se efectúen o pretendan efectuar transferencias de datos personales a las que se refiere el artículo 3, fracción XXXII de la Ley General o los que correspondan en las legislaciones estatales en la materia, entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa mas no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

1013 En este contexto el artículo 8 de las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales señalan que el tratamiento intensivo de datos personales particular es:
Tratamientos intensivos o relevantes de datos personales de manera particular:
Artículo 9. Considerando lo dispuesto en el artículo 76 de la Ley General, se entenderá, de manera enunciativa mas no limitativa, que el responsable está en presencia de un tratamiento intensivo o relevante de datos personales, de manera particular, cuando pretenda:
I. Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.
II. Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicos que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan, o pudieran establecerse, diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares.
III. Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa mas no limitativa, a su edad, género, origen étnico o racial, estado de salud, preferencia sexual, nivel de instrucción y condición socioeconómica.
IV. Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.
V. Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración de seguridad por la cantidad de información contenida en ellas, pudiera derivarse una afectación a la esfera personal de los titulares, sus derechos o libertades.
VI. Realizar un tratamiento frecuente y continuo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.
VII. Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.

En relación con lo anterior, las disposiciones sobre EIPD señalan que será obligado elaborar la EIPD en el supuesto de que se pretenda poner en operación o modificar una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que, a su juicio y de conformidad con lo dispuesto en la LGPDPPSO o las legislaciones estatales en la materia, las citadas disposiciones y demás normatividad aplicable, implique un tratamiento intensivo o relevante de datos personales.[1014]

De esta manera se puede sostener que la elaboración de una EIPD es requerida en aquellos supuestos en los que los tratamientos de datos personales presentes en la organización pudieren representar un riesgo para los derechos y libertades fundamentales de los titulares de datos personales y/o se esté en presencia de un tratamiento intensivo o relevante de datos personales en términos de la normatividad aplicable a la protección de datos personales.

3. Contenido de la EIPD

De acuerdo con lo dispuesto por el artículo 74 de la LGPDPPSO, el contenido de la EIPD será determinado por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT). Con base en ello, se emitieron las Disposiciones sobre EIPD el 23 de enero de 2018, en ellas se señalan los requisitos que deberá cubrir la EIPD.

Así, las Disposiciones sobre EIPD para el sector público previenen que la EIPD deberá de prever al menos los siguientes elementos:

a) La descripción de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales que pretenda poner en operación o modificar.

b) La justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.[1015]

VIII. Permitir el acceso de terceros a una gran cantidad de datos personales que anteriormente no tenían acceso, ya sea, entregándolos, recibiéndolos y/o poniéndolos a su disposición en cualquier forma.
IX. Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.
X. Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular.
XI. Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos.
XII. Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar.
XIII. Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales.
XIV. La observación sistemática a gran escala de una zona de acceso público.

1014 Artículo 10. El responsable que pretenda poner en operación o modificar una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que, a su juicio y de conformidad con lo dispuesto en la Ley General o las legislaciones estatales en la materia, las presentes Disposiciones administrativas y demás normatividad aplicable, implique un tratamiento intensivo o relevante de datos personales deberá elaborar y presentar ante el Instituto o los organismos garantes una evaluación de impacto en la protección de datos personales de conformidad con los citados ordenamientos.

1015 El artículo 17 de las Disposiciones sobre EIPD indica al respecto:
Justificación de la necesidad de implementar o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología.
Artículo 17. En la evaluación de impacto en la protección de datos personales, el responsable deberá señalar las razones o motivos que justifican la necesidad de poner en operación o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, en función de las atribuciones que la normatividad aplicable le confiera precisando para tal efecto:
I. Si la o las medidas propuestas son susceptibles o idóneas para garantizar el derecho a la protección de datos persona-

c) La representación del ciclo de vida de los datos personales a tratar.[1016]

d) La identificación, análisis y descripción de la gestión de los riesgos inherentes para la protección de los datos personales.[1017]

e) El análisis de cumplimiento normativo en materia de protección de datos personales de conformidad con la LGPDPPSO o las legislaciones estatales en la materia y demás disposiciones aplicables.[1018]

f) Los resultados de la o las consultas externas que, en su caso, se efectúen.[1019]

---

les de los titulares.
II. Si la o las medidas propuestas son las estrictamente necesarias, en el sentido de ser las más moderadas para garantizar el derecho a la protección de datos personales de los titulares.
III. Si la o las medidas son equilibradas en función del mayor número de beneficios o ventajas que perjuicios para el garantizar el derecho a la protección de datos personales de los titulares.
Lo anterior, con la finalidad de que el responsable adopte las medidas menos intrusivas en lo que respecta a la protección de datos personales de los titulares.

1016 Sobre este elemento de la EIPD, el artículo 18 de las Disposiciones sobre EIPD indica lo siguiente:
Ciclo de vida de los datos personales
Artículo 18. En la evaluación de impacto en la protección de datos personales, el responsable deberá describir y representar cada una de las fases de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, especificando el ciclo de vida de éstos a partir de su obtención, aprovechamiento, explotación, almacenamiento, conservación o cualquier otra operación realizada, hasta la supresión de los mismos.
Además de lo previsto en el párrafo anterior del presente artículo, el responsable deberá señalar:
I. Las fuentes internas y/o externas, así como los medios y procedimientos a través de los cuales se recabarán los datos personales, o bien, son recabados.
II. Las áreas, grupos o personas que llevarán a cabo operaciones específicas de tratamiento con los datos personales.
III. Los plazos de conservación o almacenamiento de los datos personales.
IV. Las técnicas a utilizar para garantizar el borrado seguro de los datos personales.

1017 Sobre este elemento en particular, el artículo 19 de las Disposiciones sobre EIPD indica lo siguiente:
Identificación, análisis y gestión de los riesgos para la protección de los datos personales
Artículo 19. En la evaluación de impacto en la protección de datos personales, el responsable deberá incluir la gestión de riesgos que tenga por objeto identificar y analizar los posibles riesgos y amenazas, así como los daños o consecuencias que pudieran producirse o presentarse si llegasen a materializarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
El responsable deberá presentar un plan general para gestionar los riesgos identificados, en el que se mencione, al menos, lo siguiente:
I. La identificación y descripción específica de los riesgos administrativos, físicos o tecnológicos que podrían presentarse con la puesta en operación o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.
II. La ponderación cuantitativa y/o cualitativa de la probabilidad de que los riesgos identificados sucedan, así como su nivel de impacto en los titulares en lo que respecta al tratamiento de sus datos personales, y
III. Las medidas y controles concretos que el responsable adoptará para eliminar, mitigar, transferir o retener los riesgos detectados, de tal manera que no tengan un impacto en la esfera de los titulares, en lo que respecta al tratamiento de sus datos personales.

1018 Para la realización del análisis de cumplimiento normativo, el artículo 20 de las Disposiciones sobre EIPD previene lo siguiente:
Análisis de cumplimiento normativo
Artículo 20. En la evaluación de impacto en la protección de datos personales, el responsable deberá señalar los mecanismos o procedimientos que adoptará para que la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que pretende implementar o modificar y que implique un tratamiento intensivo o relevante de datos personales cumpla, por defecto y diseño, con los principios, deberes, derechos y demás obligaciones previstas en la Ley General o las legislaciones estatales en la materia y demás disposiciones aplicables.

1019 Sobre los informes de consulta externa el artículo 21 de las Disposiciones sobre EIPD precisa:
Informe de la consulta externa
Artículo 21. En caso de que el responsable hubiere realizado consultas públicas a que se refiere el artículo 13 de las presentes Disposiciones administrativas, en la evaluación de impacto en la protección de datos personales deberá informar sobre los resultados de la o las consultas externas, distinguiendo las opiniones, puntos de vista y perspectivas del público que, a su juicio, consideró pertinente incorporar en el diseño o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, de aquéllas que no consideró.

g) La opinión técnica del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implique la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso.[1020]

h) Cualquier otra información o documentos que considere conveniente hacer del conocimiento del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) o los organismos garantes en función de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y que pretenda poner en operación o modificar.

Además de los elementos anteriores, el artículo 16 de las Disposiciones sobre EIPD previene que tratándose de las EIPD interinstitucionales se deberán de considerar elementos adicionales como la denominación de los responsables conjuntos que presentan la evaluación de impacto en la protección de datos personales; la denominación del responsable líder del proyecto, entendido para efecto de las presentes disposiciones administrativas como el responsable que tiene a su cargo coordinar las acciones necesarias entre los distintos responsables para la elaboración de la evaluación de impacto en la protección de datos personales y las obligaciones, deberes, responsabilidades, límites y demás cuestiones relacionadas con la participación de todos los responsables.[1021]

Por su parte, en el ámbito internacional, el RGPD señala que la EIPD deberá incluir los siguientes elementos:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda el interés legítimo perseguido por el responsable del tratamiento.

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.

c) Una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1 del artículo 35.[1022]

Con relación a las opiniones, puntos de vista y perspectivas no consideradas, el responsable deberá señalar las razones o motivos que lo llevaron a tal decisión.
El Instituto y los organismos garantes podrán tener acceso a los documentos recabados durante las consultas externas.

1020 Sobre la opinión técnica del oficial de protección de datos las disposiciones sobre EIPD indican lo siguiente:
Opinión técnica del oficial de protección de datos personales
Artículo 22. En la evaluación de impacto en la protección de datos personales, el responsable deberá señalar la opinión y consideraciones técnicas del oficial de protección de datos personales respecto del tratamiento intensivo o relevante de datos personales que implica la puesta a disposición o modificación de la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología, en su caso.

1021 Contenido adicional para las evaluaciones de impacto en la protección de datos personales interinstitucionales
Artículo 16. Tratándose de una evaluación de impacto en la protección de datos personales interinstitucional, de manera adicional a lo previsto en el artículo anterior, el responsable deberá señalar lo siguiente:
I. La denominación de los responsables conjuntos que presentan la evaluación de impacto en la protección de datos personales.
II. La denominación del responsable líder del proyecto, entendido para efecto de las presentes Disposiciones administrativas como el responsable que tiene a su cargo coordinar las acciones necesarias entre los distintos responsables para la elaboración de la evaluación de impacto en la protección de datos personales.
III. Las obligaciones, deberes, responsabilidades, límites y demás cuestiones relacionadas con la participación de todos los responsables.

1022 Artículo 35
Evaluación de impacto relativa a la protección de datos
1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el RGPD, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

En relación con la elaboración de las EIPD en el ámbito internacional, distintas autoridades de protección de datos han emitido guías orientadoras que consideran el cumplimiento al principio de responsabilidad previsto en RGPD como punto neurálgico. [1023]

4. Valoración de la EIPD por parte del INAI y/o los organismos garantes

En términos de lo dispuesto por el artículo 74 de la LGPDPPSO y los artículos 10, 12 y 23 de las Disposiciones sobre EIPD, las EIPD deben presentarse ante el INAI y/o los organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

Derivado de lo anterior, el artículo 23 de las Disposiciones sobre EIPD indica que, las EIPD deben ser presentadas en el domicilio del Instituto y/o de los organismos garantes, o bien, a través de cualquier otro medio que éstos habiliten para tal efecto, al menos, 30 días anteriores a la fecha en que pretende poner en operación o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales.[1024]

En conjunción con este procedimiento, los artículos 24, 25, 26, 27, 28, 29, 30, 31 y 32 de las Disposiciones sobre EIPD regulan concretamente el procedimiento y formalidades a seguirse para la valoración de las evaluaciones de impacto en la protección de datos personales ante el INAI y los órganos garantes locales, según corresponda.

5. Exención de presentación de la EIPD

La normatividad de datos personales aplicable al sector público establece que no será necesario realizar la EIPD en aquellos casos en los que, a criterio del sujeto regulado se pudieran comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o

---

del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.
[...]

1023 En relación con las recomendaciones para la elaboración de EIPD en el ámbito internacional se pueden mencionar los siguientes recursos:
Agencia Española de Protección de Datos. (2018). *Guía práctica para las evaluaciones de impacto en la protección de datos personale*s. Disponible en: https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
CNIL. (2017). *Guidelines on DPIA*. Disponible en: https://www.cnil.fr/en/guidelines-dpia
CNIL. (2019). *Privacy impact assesment software.* Disponible en*:* https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
ICO. (s.f.). *Conducting privacy impact assessments code of practice*. Disponible en: https://www.pdpjournals.com/docs/88317.pdf

1024 Artículo 23. El responsable deberá presentar la evaluación de impacto en la protección de datos personales en el domicilio del Instituto o de los organismos garantes, o bien, a través de cualquier otro medio que éstos habiliten para tal efecto, al menos, treinta días anteriores a la fecha en que pretende poner en operación o modificar la política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, de acuerdo con lo dispuesto en el artículo 77 de la Ley General o los que correspondan en las legislaciones estatales en la materia.

relevante de datos personales o se trate de situaciones de emergencia o urgencia[1025] (ver definición de "situación de emergencia" en el presente diccionario).

Finalmente, el artículo 34 de las Disposiciones sobre EIPD fija los requisitos de presentación y contenido del informe de exención para la presentación de la EIPD y los artículos 35, 36 y 37 del mismo dispositivo normativo regulan el procedimiento de notificación, requerimiento de información y respuesta por parte del INAI y los órganos garantes locales.

Evaluación del Sistema de Autorregulación Vinculante

Rosa María Franco Velázquez

Es el proceso establecido para determinar la procedencia de la validación o modificación de un determinado esquema de autorregulación, conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),[1026] el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP),[1027] los Parámetros de Autorregulación Vinculante y demás normativa aplicable. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) evaluará los elementos presentados por el solicitante para llevar a cabo el trámite en cuestión y emitirá una resolución sobre el particular, salvo en los casos en los que los Parámetros de Autorregulación Vinculante[1028] establezcan que no es necesaria una evaluación.

El INAI resolverá sobre la procedencia de la validación o modificación de un esquema de autorregulación, así como sobre su inscripción en el Registro de Esquemas de Autorregulación Vinculante (REA), después de realizar la evaluación correspondiente, en un plazo de tres meses contados a partir del día siguiente a la recepción de la notificación. Este plazo podrá ampliarse hasta por un periodo igual cuando existan razones que lo justifiquen, siempre y cuando éstas le sean notificadas al solicitante.[1029]

El reconocimiento de un esquema de autorregulación vinculante distinto de la certificación, por parte del INAI, estará vigente hasta en tanto no se actualice alguna condición prevista para su baja.[1030]

1025 La LGPDPPSO en su artículo 79 señala:
Artículo 79. Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la evaluación de impacto en la protección de datos personales.
Las disposiciones administrativas sobre EIPD en sintonía con el artículo 79 previenen lo siguiente:
Artículo 33. De conformidad con el artículo 79 de la Ley General o los que correspondan en las legislaciones estatales en la materia, el responsable no deberá realizar y presentar una evaluación de impacto en la protección de datos personales cuando pretenda poner en operación o modificar una política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales y a su juicio:
I. Se comprometan los efectos que se pretenden lograr con la posible puesta en operación o modificación de política pública, programa, sistema o plataforma informática, aplicación electrónica o cualquier otra tecnología que implique un tratamiento intensivo o relevante de datos personales, o
II. Se trate de situaciones de emergencia o urgencia.

1026 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010. (La Ley).

1027 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *Diario Oficial de la Federación* el 21 de diciembre de 2011. (El Reglamento).

1028 Parámetros de Autorregulación en materia de Protección de Datos Personales, publicados en el *Diario Oficial de la Federación* el 29 de mayo de 2014. (Los Parámetros).

1029 Numeral 51 de los Parámetros.

1030 Numeral 52 de los Parámetros.

Para que un esquema sea validado por el INAI o cuente con una certificación reconocida por el INAI deberá, al menos:

a) señalar su denominación;
b) señalar el nombre completo, denominación o razón social de los responsables o encargados adheridos al esquema;
c) especificar el sector o la actividad a la que aplica;
d) describir el alcance del esquema en cuestión, de acuerdo con el numeral anterior;
e) describir el ámbito personal de aplicación, es decir, el tipo o grupo de titulares cuyos datos personales están vinculados con el tratamiento al que aplica el esquema de autorregulación;
f) desarrollar e implementar un sistema de gestión de datos personales (SGDP);[1031]
g) documentarse y desarrollarse en idioma español y
h) proporcionar datos de contacto o un medio habilitado para que los interesados conozcan más acerca del esquema.[1032]

Es importante tomar en cuenta que el responsable o encargado deberá prever, implementar y mantener revisiones administrativas regulares y programadas, para asegurar un adecuado desarrollo continuo y la efectividad del SGDP. Estas revisiones administrativas deberán hacerse cuando se presenten cambios que afecten aspectos significativos del SGDP, tales como cambios en la normativa aplicable, en la tecnología o en los valores y procedimientos del responsable o encargado. Las revisiones administrativas deberán ser documentadas y basarse en:[1033]

a) la retroalimentación por parte de los usuarios del SGDP;
b) los riesgos identificados en el análisis de riesgos;
c) los resultados de auditorías;
d) los resultados de las revisiones;
e) las actualizaciones o cambios en la tecnología utilizada por el responsable o encargado;
f) los requerimientos por parte de autoridades;
g) el manejo de quejas y
h) las vulneraciones de seguridad.

1031 Sistema de gestión general para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios, deberes y obligaciones previstos en la Ley, demás normativa aplicable y buenas prácticas en materia de protección de datos personales. Numeral 4, fracción XIV, de los Parámetros.

1032 Numeral 14 de los Parámetros.

1033 Numeral 32 de los Parámetros.

Exportador[1034]

Isabel Davara Fernández de Marcos,[1035]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El término "exportador" es empleado en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) y se refiere a la persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en dichos Estándares.[1036]

De la definición anterior se desprenden los siguientes elementos sobre la figura del exportador:

a) El exportador puede ser una persona física o jurídica.

b) El exportador puede ser un sujeto de derecho público o privado. En este contexto, se pueden encontrar organizaciones privadas de todo tipo, autoridades públicas, servicios, organismos o prestador de servicios.

c) El exportador debe estar establecido en el territorio de uno de los Estados iberoamericanos que forman parte de la Red Iberoamericana de Protección de Datos (RIPD)[1037] y que son: Andorra, Argentina, Chile, Colombia, Costa Rica, España, México, Perú, Portugal y Uruguay.

d) El exportador es quien realiza la transferencia internacional de datos personales a un tercer Estado conforme a las condiciones previstas en el artículo 36.1 de los Estándares Iberoamericanos.

e) El exportador puede revestir tanto el carácter de encargado como el de responsable del tratamiento (según el artículo 36.1 de los Estándares Iberoamericanos).

De acuerdo con las previsiones de los Estándares Iberoamericanos,[1038] el exportador —previo a comunicar los datos personales a otro responsable y/o encargado establecido en el territorio de un tercer Estado— deberá asegurarse de que dicha comunicación cumple con alguna de realizarse en cumplimiento de cualquiera de las siguientes reglas específicas:

- El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de éste que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.

1034 En este *Diccionario de Protección de Datos Personales* también pueden consultarse las definiciones de "transferencia", "responsable" y "encargado" que son afines con el contenido de la definición de exportador que aquí se explica.

1035 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

1036 2. Definiciones
2.1. Para los efectos de los presentes Estándares se entenderá por:
f) exportador: persona física o jurídica de carácter privado, autoridad pública, servicios, organismo o prestador de servicios situado en territorio de un Estado que efectúe transferencias internacionales de datos personales, conforme a lo dispuesto en los presentes Estándares.

1037 Red Iberoamericana de Protección de Datos. Consultado el 28 de septiembre de 2018. Disponible en: http://www.redipd.es/la_red/Miembros/index-ides-idphp.php

1038 Artículo 36 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

- El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y éste, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado iberoamericano aplicable en la materia.
- El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los estados iberoamericanos aplicable en la materia.
- El exportador y destinatario adopten un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando éste sea acorde con las disposiciones previstas en la legislación nacional del Estado iberoamericano aplicable en la materia que está obligado a observar el exportador.
- La autoridad de control del Estado iberoamericano del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.

Finalmente, dado que los Estándares Iberoamericanos pretenden ser unas directrices de referencia para futuras regulaciones o para la revisión de las existentes, no pueden ser un desarrollo a detalle de las cuestiones, sino más bien exponer los mínimos necesarios, y así solo señalan que con carácter previo a realizar la comunicación de datos personales, el exportador deberá tener conocimiento de los límites existentes en cada Estado iberoamericano para la realización de las transferencias internacionales de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.[1039]

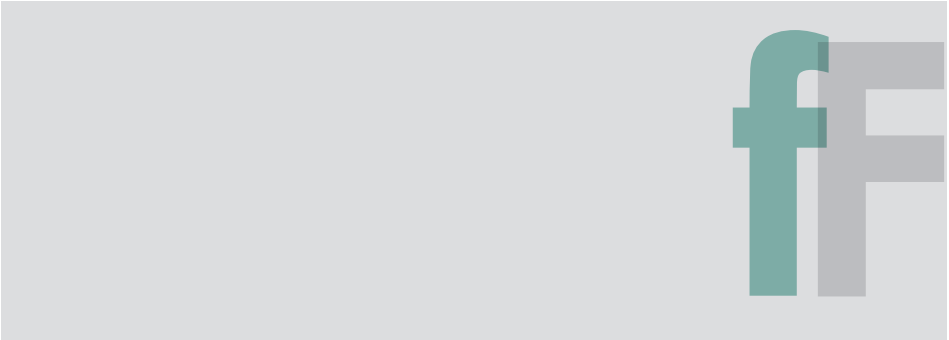
1039 36.2. La legislación nacional de los Estados iberoamericanos aplicable en la materia podrá establecer expresamente límites a las transferencias internacionales de categorías de datos personales por razones de seguridad nacional, seguridad pública, protección de la salud pública, protección de los derechos y libertades de terceros, así como por cuestiones de interés público.

NOTAS

NOTAS

NOTAS

NOTAS



Factores para determinar las medidas de seguridad

Christian Paredes González

De lo general a lo particular, las medidas de seguridad tienen como principales objetivos garantizar la integridad de la información, facultar su recuperación en caso de incidentes y eludir los accesos no autorizados. La determinación de las medidas de seguridad exigidas por la normatividad para cumplir con el deber de seguridad respecto de los datos personales debe de realizarse siguiendo las directrices que la normatividad aplicable establece para tal efecto.

En primer lugar, como factores o elementos para el establecimiento de las medidas de seguridad físicas, técnicas y administrativas para la adecuada protección de datos personales, según dispone el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) deberá considerarse el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.[1040]

Por su parte, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), en su artículo 60, indica que el responsable deberá determinar las medidas de seguridad considerando los siguientes elementos:

- el riesgo inherente por tipo de dato personal;
- la sensibilidad de los datos personales tratados;
- el desarrollo tecnológico y
- las posibles consecuencias de una vulneración para los titulares.

Adicionalmente, el citado artículo 60 precisa que el responsable deberá considerar los siguientes elementos:

- el número de titulares;
- las vulnerabilidades previas ocurridas en los sistemas de tratamiento;

1040 Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

- el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión y
- demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

En el ámbito de la protección de datos personales en el sector público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) indica, en su artículo 32, que las medidas de seguridad adoptadas deberán considerar factores como:

- el riesgo inherente a los datos personales tratados;
- la sensibilidad de los datos personales tratados;
- el desarrollo tecnológico;
- las posibles consecuencias de una vulneración para los titulares;
- las transferencias de datos personales que se realicen;
- el número de titulares;
- las vulneraciones previas ocurridas en los sistemas de tratamiento y
- el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

La normatividad de datos personales aplicable a los sectores público y privado es consistente en considerar similares elementos de cumplimiento legal para la concreción de las medidas de seguridad.

El Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) señala en su artículo 32,[1041] apartado 1, que las medidas de seguridad deberán determinarse por parte del responsable teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas. En relación con lo anterior, el considerando 76 previene que la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. Además, se señala que el riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.[1042]

1041 Artículo 32
Seguridad del tratamiento
1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:
[...]

1042 (76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

Firma autógrafa

Jonathan Gabriel Garzón Galván

La firma es un medio a través del cual es posible identificar a una persona y dejar evidencia de que expresó su consentimiento o voluntad para aceptar y quedar vinculado a ciertas condiciones, obligaciones y/o información. La forma en que la firma puede manifestarse varía, y en el caso de la firma autógrafa, se entiende que es de propia mano del autor. Aunque no hay una definición legal en la regulación mexicana, el *Diccionario de la Real Academia Española* (DRAE)[1043] aporta con los siguientes conceptos:

> Firma
>
> 1. f. Nombre y apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido.
>
> 2. f. Rasgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a un documento.
>
> (…)
>
> Autógrafo, fa.
>
> 1. adj. Que está escrito de mano de su mismo autor.

En el mismo diccionario encontramos que el vocablo "firma" deriva del verbo "firmar" y éste del latín *firmare*, cuyo significado es afirmar o dar fuerza. A su vez, la palabra "firmar" se define como "afirmar, dar firmeza y seguridad a una cosa".[1044]

Trasladando los mencionados conceptos al campo del derecho, debe decirse que la firma autógrafa consiste en asentar en algún documento, rasgos característicos (no necesariamente el nombre y apellido de la persona que los expide), en forma legible o no, con el propósito de dar autenticidad y firmeza a dicho documento, así como aceptar la responsabilidad o condiciones del mismo.[1045]

Como se mencionó previamente, no hay regulación específica de la validez y valoración en juicio para la firma autógrafa, como la que existe para la firma electrónica. Sin embargo, en la regulación se puede encontrar que ambas firmas son equivalentes funcionalmente. Por ejemplo, el Reglamento de la Ley Federal de Protección de Datos en Posesión de los Particulares (LFPDPPP), en su artículo 20,[1046] referente al consentimiento expreso y por escrito menciona:

> Artículo 19. Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento.

En el entorno físico no fue necesario un marco regulatorio que explicara su funcionamiento y/o efectos,[1047] sin embargo, existen criterios de los tribunales en los cuales se puede apoyar para ese efecto:

1043 RAE. (2017). *Diccionario de la Real Academia Española*. Disponible en: http://dle.rae.es/ Fecha de consulta: agosto 2018.

1044 RAE. (2017). *Diccionario de la Real Academia Española*. Disponible en: http://dle.rae.es/ Fecha de consulta: agosto 2018.

1045 Firma autógrafa, resolución carente de. Es inconstitucional. Tribunales Colegiados de Circuito. Séptima época. Apéndice 2000. Tomo VI, Común, Jurisprudencia TCC, p. 448, véase: http://sjf.scjn.gob.mx/ SJFSist/Documentos/Tesis/918/918045.pdf

1046 DOF, (2011). "Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares", en *Diario Oficial de la Federación*. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

1047 Davara, I. (2007, noviembre) "Firma electrónica en México su problemática jurídica", en *Revista Política Digital*, no. 39.

> [...] la firma es el conjunto de signos manuscritos a través de los cuales las personas expresan su voluntad de realizar determinado acto en forma escrita y con ella se acredita la autoría del documento, siendo indispensable para dar validez a cualquier actuación escrita. [1048]
>
> La firma tiene como función esencial identificar a su autor, así como imputarle la autoría del texto que le precede...la firma, para ser tal debe consistir en uno o varios signos manuscritos con características tales que permitan identificarlos con su autor, aunque no representen su nombre y apellido, ni estén acompañados de estos datos escritos [...][1049]
>
> [...] la firma es lo que da autenticidad a toda promoción o acto y es lo que constituye la base para tener por cierto que existe una manifestación de voluntad de parte del promovente[...][1050]

Como se puede observar, las funciones principales de cualquier tipo de firma (autógrafa y electrónica) es identificar a los autores y vincularlos con el contenido de un documento, y para el caso de la firma autógrafa, se requiere escribir en un documento a puño y letra cualquier tipo de gráfico o caracteres que permita cumplir dichas funciones.

Estos grafos o caracteres, si bien se esperan que sean usados de forma constante por la persona en todos los actos en los que quiera plasmar su consentimiento a través de este medio, no necesariamente debe ser así. Es decir, una persona podría plasmar de puño y letra diferentes caracteres o grafos, en cada documento que pretenda firmar autógrafamente y todos ellos serían válidos y auténticos.

Alfredo Baltierra señala que los signos o caracteres pueden ser desde un mero monosílabo hasta la más complicada complementación de caracteres alfabéticos cruzados por diversas direcciones, incluso podrían ser signos no alfabéticos.[1051]

Finalmente cabe señalar que, si bien la firma autógrafa es un medio comúnmente usado para expresar el consentimiento, no es posible señalar que sea un método de autenticación totalmente fiable ya que puede darse el caso de que se reconozca la firma, pero el documento podría no ser integro, es decir podría haber sido alterado o modificado a lo largo del tiempo.[1052]

Firma electrónica

Jonathan Gabriel Garzón Galván

A través de los medios electrónicos, las transacciones se pueden realizar casi desde y hasta cualquier punto geográfico sin requerimientos o formalidades presenciales o físicas. Los procesos se han agilizado y optimizado para concretar transacciones en tiempos cortos y con el menor número de recursos posibles. Sin embargo, la forma de autenticar dichas transacciones comerciales electrónicas ha cobrado fuerte relevancia y la firma electrónica es el recurso más práctico y utilizado.

1048 Tesis aislada. Tribunales Colegiados de Circuito, agosto 2007: Demanda de amparo. Debe tenerse por no interpuesta cuando el escrito relativo no se encuentre firmado por el que aparece como promovente, sin tener que prevenirlo para que la firme.

1049 Jurisprudencia. Pleno Suprema Corte de Justicia de la Nación, junio 2002: pagaré, la cantidad a pagar es un requisito de existencia de esa clase de títulos de crédito, por lo que su señalamiento no puede ser satisfecho con posterioridad a su firma.

1050 Tesis aislada. Tribunales Colegiados de Circuito, junio 2002: Desechamiento del recurso de, por carecer de firma el escrito de expresión de agravios relativo a la revisión.

1051 Baltierrea, A. (2017). "La firma autógrafa en el derecho bancario", en *Biblioteca Virtual del Instituto de Investigaciones Jurídicas de la UNAM*, p. 18. Disponible en: https://revistas-colaboracion.juridicas.unam.mx/index.php/rev-facultad-derecho-mx/article/view/30813/27804

1052 Reyes, A. (2005). "El Derecho como impulsor del comercio electrónico en México", en *Tecnologías de la Información y de las Comunicaciones: Aspectos Legales*, coord. Navarro Isla, Jorge. México. Porrúa, p. 109.

La firma electrónica se ha vuelto el medio mediante el cual la firma autógrafa se puede plasmar en los medios electrónicos. Como observaremos, esta definición no involucra el uso de alguna tecnología en particular en cumplimiento con el principio de neutralidad, aunque una de las técnicas más usadas es la criptografía y el cifrado de la información.

El primer antecedente internacional relacionado con la firma electrónica se da en mayo de 1995 en Utah, Estados Unidos, donde fue emitida la primera ley sobre firmas digitales conocida como *Utah Digital Signature Act*.[1053] El objetivo de esta ley es facilitar las transacciones mediante mensajes electrónicos y firmas digitales, definiendo a estas últimas como la transacción de un mensaje empleando un criptosistema asimétrico en el cual una persona posee el mensaje inicial y la clave pública del firmante a fin de que pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación.[1054]

Poco más de un año después, en diciembre de 1996, se emitió la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (Ley Modelo), si bien ésta no trataba exclusivamente sobre la firma electrónica, sí hace referencia a ella en su artículo 7.[1055] Inclusive, el apartado 56 de su *Guía de Incorporación al Derecho Interno* especifica: "Este artículo se centra en las dos funciones básicas de cualquier tipo de firma, solo que explicando su aplicación en medios electrónicos: la identificación del autor y la confirmación de que el autor aprueba el contenido del documento".[1056]

En julio de 2001 es adoptada por la misma comisión la Ley Modelo sobre Firmas Electrónicas. Ambas regulaciones buscan mitigar el riesgo de que distintos países adopten criterios legislativos diferentes en relación al comercio electrónico y a las firmas electrónicas, buscando normativas uniformes. Los estados partes en estos instrumentos, al implementarlos en su derecho interno, dispondrán de un medio para reconocer la validez de los medios electrónicos, sin necesidad de negociar algún tratado en particular. Esta segunda Ley Modelo incluye en su artículo 2 una definición de firma electrónica:

> a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos.

En México, la primera normativa en regular específicamente la firma electrónica fueron diversas circulares del Banco de México. Para ello, dicho banco central diseñó la Infraestructura Extendida de Seguridad (IES) la cual fue, inicialmente, regulada por dos circulares: telefax 1/2002 y 19-2002 para que, posteriormente, se integraran ambas a la circular 6/2005.[1057] El texto compilado actual establece una definición de firma electrónica muy

1053 Reyes, A. (2008). *La firma electrónica y las entidades de certificación*. 2da. edición. México. Porrúa, p. 109.

1054 Téllez, J. (2004). *Derecho informático*. 3ra. edición. México. Mc Graw Hill, p. 205.

1055 Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf
Artículo 7. Firma. 1) Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos y b) si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente. (…)

1056 Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno, pp. 40 y 41, véase: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

1057 Circular-Telefax 6/2005 publicada el 15 de marzo de 2005, incluyendo sus modificaciones dadas a conocer mediante la Circular-Telefax 6/2005 Bis publicada el 23 de diciembre de 2005 y la Circular 23/2010 publicada el 2 de agosto de 2010, véase: http://www.banxico.org.mx/disposiciones/normativa/circular-telefax-6-2005/%7BBB92DE-

apegada a la de la Ley Modelo de Firmas Electrónicas:

> Firma Electrónica. - Al conjunto de datos que se agrega o adjunta a un mensaje de datos, el cual está asociado en forma lógica a éste y es atribuible al titular una vez utilizado el dispositivo de verificación de firma electrónica.

Posteriormente, y para incorporar las recomendaciones de la Ley Modelo en materia de firmas electrónicas en el comercio, el 29 de agosto de 2003 se publicaron en el *Diario Oficial de la Federación* diversas modificaciones al Código de Comercio, incluyendo la incorporación de la definición de firma electrónica y firma electrónica avanzada al artículo 89:

> Artículo 89.- (…)
>
> En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente Código se deberán tomar en cuenta las siguientes definiciones: (…)
>
> Firma Electrónica: Los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el Firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma electrónica avanzada o fiable es aquella firma electrónica que cumple con los requisitos contemplados en las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a firma digital, se considerará a ésta como una especie de la firma electrónica.

Por su parte, la Ley Federal del Trabajo (LFT)[1058] establece una definición de firma electrónica que mantiene la esencia de las ya existentes.

Como se puede apreciar de todas las definiciones anteriores, es posible observar que una firma electrónica está compuesta por:

a) información o datos electrónicos que
b) estén consignados, relacionados o asociados a
c) un mensaje de datos (documento electrónico) y
d) que cumplan dos principales funciones:
   - identificación del firmante
   - vinculación del firmante al contenido del mensaje de datos (atribución).

Estas últimas dos funciones son las que también realiza una firma autógrafa o manuscrita, la diferencia es la forma (física o electrónica) en la que los datos son expresados. En el entorno físico no fue necesario un marco regulatorio que explicara el funcionamiento y/o efectos de la firma autógrafa.[1059]

Como se mencionó, una de las técnicas más comunes para lograr lo anterior es la criptografía,[1060] la cual usa algoritmos matemáticos que en conjunto permiten, a través del uso

---

DD-FD64-3A5C-455F-576C696C3CB8%7D.pdf

1058 Ley Federal del Trabajo última reforma DOF 22/06/2018, véase: http://www.diputados.gob.mx/Leyes Biblio/pdf/125_220618.pdf
Artículo 836- B. Para el desahogo o valoración de los medios de prueba referidos en esta sección, se entenderá por: (…) j) Firma electrónica: conjunto de datos que en forma electrónica son vinculados o asociados a un mensaje de datos por cualquier tecnología y que son utilizados para identificar al firmante en relación con el mensaje de datos para indicar que aprueba la información contenida en el mensaje de datos; (…)

1059 Davara, I. (2007, noviembre). "Firma electrónica en México su problemática jurídica", en *Revista Política Digital*, no. 39.

1060 La criptografía es una rama de las matemáticas aplicadas que se ocupan de transformar, mediante un procedimiento sencillo, mensajes en forma aparentemente ininteligibles y devolverlas a su forma original. Reyes, A. (2008). *La firma electrónica y las entidades de certificación*. 2da Edición. México. Porrúa, p. 143.

de claves, cifrar y descifrar información, es decir, convertirla en ilegible y nuevamente en legible, permitiendo que solo aquellas personas en posesión de las correspondientes claves puedan realizar dichas conversiones.

Los métodos comunes de cifrado utilizados para las firmas electrónicas son el cifrado de clave única, clave secreta o simétrico, el cifrado de par de claves y clave pública o cifrado asimétrico. El primero es utilizado para cumplir con los requisitos de la firma electrónica simple, donde para cifrar y descifrar se utiliza una clave única que comparten tanto el emisor como el receptor de la información. Este tipo de cifrado requiere de alta confianza entre las partes que intervienen dado que comparten una sola clave. La existencia de una clave única puede generar ciertos problemas, por ejemplo, entre más personas intervienen en la comunicación, la secrecía de la clave puede irse perdiendo y puede ser intervenida o compartida con mayor facilidad.

Algunos ejemplos de este tipo de cifrado son las contraseñas, *pines*, números de identificación personal, *tokens* y equipos OTP (*one time password*) comúnmente usados en el sector bancario, donde la transacción es cifrada por el cliente utilizando este tipo de claves y un algoritmo matemático que posteriormente es enviada a la institución bancaria, quien la recibe y descifra la transacción utilizando el mismo algoritmo matemático y la clave que también conoce.

El cifrado asimétrico o de clave pública se utiliza para cumplir los requisitos de la firma electrónica avanzada. Este tipo de cifrado requiere —para el intercambio de la información— de dos claves complementarias entre sí: la clave pública y la clave privada. Lo que se cifra con una de las claves solo se podrá descifrar con la otra pues ambas tienen la misma capacidad técnica de cifrar y descifrar.

Finalmente, es importante resaltar que tanto la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[1061] y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[1062] disponen que cuando se traten datos sensibles se podrá obtener el consentimiento expreso y por escrito del titular, a través de su firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, con lo cual estas normativas también observan la validez legal y equivalencia funcional entre firma electrónica y firma autógrafa.

Firma electrónica avanzada

Jonathan Gabriel Garzón Galván

Este tipo de firma también es conocida como firma electrónica fiable. El primer acercamiento a su diferenciación lo encontramos en el artículo 6 de la Ley Modelo sobre Firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDIM):[1063]

> La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1 si:
>
> A. los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;

1061 Artículo 9 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el DOF 05/07/2010, véase: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

1062 Artículo 21 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el DOF 26/01/2017, véase: http: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

1063 Ley Modelo de la CNUDMI sobre firmas electrónicas y su guía para su incorporación al derecho interno, véase: http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf

B. los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;

C. es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma y

D. cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

En este tenor, el 29 de agosto de 2003, se publicaron en el *Diario Oficial de la Federación* (DOF) diversas modificaciones al Código Comercio[1064] incluyendo la incorporación, en el artículo 89, de la definición de firma electrónica avanzada y sus requisitos:

Artículo 89.- (…)

En los actos de comercio y en la formación de los mismos podrán emplearse los medios electrónicos, ópticos o cualquier otra tecnología. Para efecto del presente código, se deberán tomar en cuenta las siguientes definiciones: (…)

Firma electrónica avanzada o fiable: aquella firma electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. (…)

Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una firma en relación con un mensaje de datos, se entenderá satisfecho dicho requerimiento si se utiliza una firma electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese mensaje de datos.

La firma electrónica se considerará avanzada o fiable si cumple por lo menos los siguientes requisitos:

I. Los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante.

II. Los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante.

III. Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma.

IV. Respecto a la integridad de la información de un mensaje de datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una firma electrónica; o presente pruebas de que una firma electrónica no es fiable.

1064 Código de Comercio, última reforma DOF 28/03/2018, véase: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_280318.pdf

Estas definiciones resultan ser las más convenientes para analizar las características de la firma electrónica avanzada o fiable a pesar de que en la regulación mexicana existan diversos cuerpos normativos con definiciones adicionales como las que se encuentran en la Ley Federal del Trabajo,[1065] la Ley Federal del Procedimiento Contencioso Administrativo[1066] y la Ley Federal de Firma Electrónica Avanzada.[1067]

En materia de protección de datos personales, la fracción VIII del artículo 3 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones definen la firma electrónica avanzada como:

Firma electrónica avanzada (FIEL): conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.[1068]

De las definiciones de la Ley Modelo de Firmas Electrónicas, el Código de Comercio y los lineamientos antes señalados establecen que una firma electrónica avanzada o fiable, cuenta con las mismas características que una firma electrónica simple, pero establece requisitos adicionales, como la integridad y el no repudio, que se resuelven de forma general con el método criptográfico asimétrico[1069] y con una entidad certificadora de confianza (prestador de servicios de certificación):

Los datos de creación de firma (clave privada) corresponden exclusivamente al firmante (no repudio).	El prestador de servicios de certificación (PSC) acredita la identidad de la persona que solicita un certificado digital y verifica los datos contenidos de identidad relacionados a la clave pública, la cual está matemáticamente relacionada con la clave privada y, por lo tanto, si todo es correcto en el proceso, se garantiza que ambas claves corresponden exclusivamente al firmante.

1065 Ley Federal del Trabajo última reforma DOF 22/06/2018, véase: http://www.diputados.gob.mx/Leyes Biblio/pdf/125_220618.pdf
Artículo 836- B. Para el desahogo o valoración de los medios de prueba referidos en esta sección, se entenderá por: (…)
k) Firma electrónica avanzada: al conjunto de caracteres que permite la identificación del firmante en los documentos electrónicos o en los mensajes de datos, como resultado de utilizar su certificado digital y clave privada y que produce los mismos efectos jurídicos que la firma autógrafa; (…)

1066 Ley Federal del Procedimiento Contencioso Administrativo, última reforma DOF 27/01/2017, véase: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf
Artículo 1-A. Para los efectos de esta Ley se entenderá por: (…)
XI. Firma electrónica avanzada: conjunto de datos consignados en un mensaje electrónico adjuntados o lógicamente asociados al mismo que permita identificar a su autor mediante el sistema de justicia en línea, y que produce los mismos efectos jurídicos que la firma autógrafa. La firma electrónica permite actuar en juicio en línea. (…)

1067 Ley Federal de Firma Electrónica Avanzada, última reforma DOF 11/01/2012. Véase: http://www. diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf
Artículo 2. Para los efectos de la presente Ley se entenderá por: (…)
XIII. Firma electrónica avanzada: el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa; (…)

1068 DOF (2015) "Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones". *Diario Oficial de la Federación*, 19 de diciembre de 2015. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5419449&fecha=09/12/2015

1069 El cifrado de clave pública, o asimétrico, es aquel que se utiliza para cumplir los requisitos de la firma electrónica avanzada. Este tipo de cifrado requiere para el intercambio de la información de dos claves complementarias entre sí: la clave pública (certificado digital) y la clave privada. Lo que se cifra con una de las claves solo la otra lo descifra, ambas tienen la misma capacidad técnica de cifrar y descifrar.

Para cumplir con los requerimientos III y IV antes señalados se utiliza generalmente el siguiente proceso de cifrado asimétrico: se cifra un "hash", digestión o resumen del mensaje de datos (documento electrónico) con la clave privada, ya que esta no se comparte y solo puede ser usada por su titular al estar protegida con una contraseña de acceso. El resultado al cifrar el resumen y adjuntarlo al documento electrónico original, es la firma electrónica avanzada. En ningún momento deberá considerarse que la firma electrónica avanzada es el certificado digital (clave pública certificada) o la clave privada, estos elementos únicamente sirven para su creación y validación.

La función "hash", tiene mucha relevancia para la validación de la firma electrónica avanzada. Dado que este resumen es aquel que se cifra y acompaña al mensaje de datos principal, al momento de realizar la validación correspondiente el receptor separa la firma (resumen cifrado) del mensaje de datos y hace tres procesos: a) por un lado descifra el resumen; b) por el otro, genera nuevamente el resumen por medio del mensaje de datos principal y c) compara ambos resúmenes. Si es posible descifrar el resumen y ambos resúmenes son exactamente iguales, quiere decir que el titular es aquel que emitió el mensaje y que ni el mensaje, ni la firma fueron alterados.

Este método de cifrado soluciona carencias de seguridad del cifrado simétrico, ya que la responsabilidad de mantener una de las claves (clave privada) de forma segura es solo de su titular y ésta no debe ser compartida. La otra clave (clave pública) es compartida abiertamente para descifrar los mensajes y no es necesario un canal seguro para compartirla. Tampoco es necesario que se tenga un par de claves por cada persona o grupo de personas con las que se pretenda intercambiar la información de forma segura, un mismo par de claves servirá para que una persona pueda cifrar la información y solo aquellos con quienes se comparta la clave pública podrán descifrarla y sabrán que solo el autor pudo ser el titular de la clave privada.

Por todo lo anterior, la firma electrónica avanzada es un medio de identificación del autor de un determinado documento electrónico o mensaje de datos que permite probar que éste aprueba, autoriza o acepta su contenido, siendo equivalente funcionalmente a la firma autógrafa[1070] o incluso más fiable. Esto último debido a que puede darse el caso de que se reconozca la firma autógrafa, pero el documento físico podría no ser integro, es decir podría haber sido alterado o modificado a lo largo del tiempo, cosa que se puede verificar con la firma electrónica avanzada.[1071]

Fuente de acceso público

Olivia Andrea Mendoza Enríquez

Una fuente de acceso público refiere a una base de datos que puede ser consultada por cualquier persona, cuyo requisito, en su caso, es el pago de una contraprestación por el servicio. No requiere del consentimiento del titular del dato personal para acceder a éste.

La totalidad de ordenamientos en materia de protección de datos personales en México prevén una definición de este concepto.

1070 García, R. (2006). *La Firma Electrónica desde el punto de vista jurídico*. México. Porrúa, p. 106.

1071 Reyes, A. (2005). "El derecho como impulsor del comercio electrónico en México", en *Tecnologías de la Información y de las Comunicaciones: Aspectos Legales*, coord. Navarro Isla, Jorge. México. Porrúa, p. 109.

Solo a manera de un marco comparativo general, es importante mencionar la definición de fuente de acceso público prevista por la Ley Orgánica 15/1999 de España, la cual señala que son "aquellos ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación".[1072]

Dicho lo anterior a manera de preámbulo para el lector, es importante precisar que cuando hablamos de acceder a datos personales normalmente asociamos la idea con el necesario consentimiento del titular de los mismos. No obstante, una de las excepciones de la obligación de recabar el consentimiento del titular de un dato personal para el acceso a éste por parte de un tercero es que dicha información obre en una fuente de acceso público.

En este sentido, las fuentes de acceso público son bases de datos, públicas o privadas, cuyo acceso es libre o sujeto a una contraprestación, generalmente un pago previo. Estas bases de datos se configuran, por lo general, de dos maneras. Una es estableciendo que ciertas bases de datos en particular serán de libre acceso, atendiendo más a la fuente que a los datos que la conforman y la otra corresponde a determinar mediante la ley qué tipos de datos pueden ser de acceso libre, dándole mayor relevancia a ese aspecto que a los bancos que los contienen.[1073]

Dicho lo anterior, revisemos las disposiciones expresas en materia de fuentes de acceso público en la normativa de protección de datos para el sector privado.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) señala que las fuentes de acceso público son aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).[1074]

También señala, como excepción del consentimiento[1075] para el tratamiento de los datos personales, aquellos datos que figuren en fuentes de acceso público.[1076]

Por otro lado, el Reglamento de la LFPDPPP señala que se consideran fuentes de acceso público:

a) los medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;
b) los directorios telefónicos en términos de la normativa específica;
c) los diarios, gacetas o boletines oficiales, de acuerdo con su normativa y
d) los medios de comunicación social.

Para que un supuesto sea considerado fuente de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa.

1072 Artículo 3 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750. Fecha de consulta: 13 de agosto de 2018.

1073 Alvarado, F. (2014). "Las fuentes de acceso público a datos personales", en *Revista Chilena de Derecho y Tecnología*, p. 207. Disponible en: file:///D:/Docs/Downloads/33276-1-124483-4-10-20150423.pdf. Fecha de consulta 20 de agosto de 2018.

1074 Artículo 3, fracción X de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Fecha de consulta 15 de agosto de 2018.

1075 De acuerdo con la fracción IV del artículo 3 de la LFPDPPP, el consentimiento se debe entender como la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

1076 Artículo 10, fracción II de la LFPDPPP.

No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.[1077]

El tratamiento de datos personales obtenidos a través de fuentes de acceso público respetará la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por la LFPDPPP.[1078]

Por otro lado, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) define las fuentes de acceso público como aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la LGPDPPSO y demás normativa aplicable.[1079]

La misma normativa de datos aplicable al sector público establece que se considerarán como fuentes de acceso público:

a) las páginas de internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;
b) los directorios telefónicos en términos de la normativa específica;
c) los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;
d) los medios de comunicación social y
e) los registros públicos conforme a las disposiciones que les resulten aplicables.[1080]

El mismo ordenamiento en materia de protección de datos personales, aplicable al sector público, establece que el responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales cuando los datos personales figuren en fuentes de acceso público.[1081]

Funciones de seguridad

Christian Paredes González

Las funciones de seguridad se encuentran referidas en el artículo 59 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) que establece la obligación del responsable de desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin con el objeto de establecer y mantener de manera efectiva las medidas de seguridad.[1082]

1077 Artículo 7 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

1078 Artículo 7 LFPDPPP.

1079 Artículo 3 fracción XVII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

1080 Artículo 5 de la LGPDPPSO.

1081 Artículo 22, fracción VIII de la LGPDPPSO.

1082 Funciones de seguridad
Artículo 59. Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.

De acuerdo con el *Diccionario de la Real Academia de la Lengua Española* (DRAE), una función se define como la "tarea que corresponde realizar a una institución o entidad, o a sus órganos o personas".

Incluso la *Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP) establece que como parte del Paso 3 como parte de las funciones de seguridad que el responsable debe determinar y proveer los recursos necesarios para establecer, implementar, operar y mantener el Sistema de Gestión de Seguridad de Datos Personales (SGSDP). Incluso enlista serie de consideraciones para asegurar que la gestión de los datos personales sea parte de los valores de la organización de manera efectiva.[1083]

Tratándose del tema de seguridad de los datos personales, se entiende que las funciones de seguridad se refieren a las actividades y/o tareas que debe de realizar el responsable del tratamiento, ya sea por sí mismo o mediante el apoyo de terceros, para garantizar la seguridad de los datos personales bajo su custodia.

Fundamentación y motivación

Jean Claude Tron Petit

1. ¿Qué y para qué es la fundamentación y motivación?

El primer párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM)[1084] consagra como derecho en favor de los gobernados la obligación relativa a que cualquier acto de autoridad cuyo objeto pueda causar molestia o perturbación deba ser emitido por autoridad competente, en forma escrita, fundando y motivando la causa legal del procedimiento.

Esta garantía se engloba dentro de las llamadas "garantías de legalidad y seguridad jurídica" que, en conjunto con otras previstas dentro del propio texto constitucional, como la garantía de audiencia y las formalidades esenciales del procedimiento,[1085] protegen la eficacia de todo el sistema jurídico, proscribiendo o estableciendo un interdicto, ya sea a la arbitrariedad o, incluso, a la insuficiencia o deficiencia jurídica en las decisiones de las autoridades, posibilitando la defensa en contra del acto, ante la propia autoridad o ante una diversa, a través de la jurisdicción contenciosa administrativa o los mecanismos de control constitucional —juicio de amparo.

La esencia de esta garantía es proteger la seguridad y certeza jurídica de los particulares frente a los actos de las autoridades que afecten o lesionen sus intereses con el fin de que puedan examinar si dicho acto es acorde al sistema legal y posibilitar la defensa respecto de un acto que no cumpla con los requisitos normativos o presupuestos necesarios para su emisión.

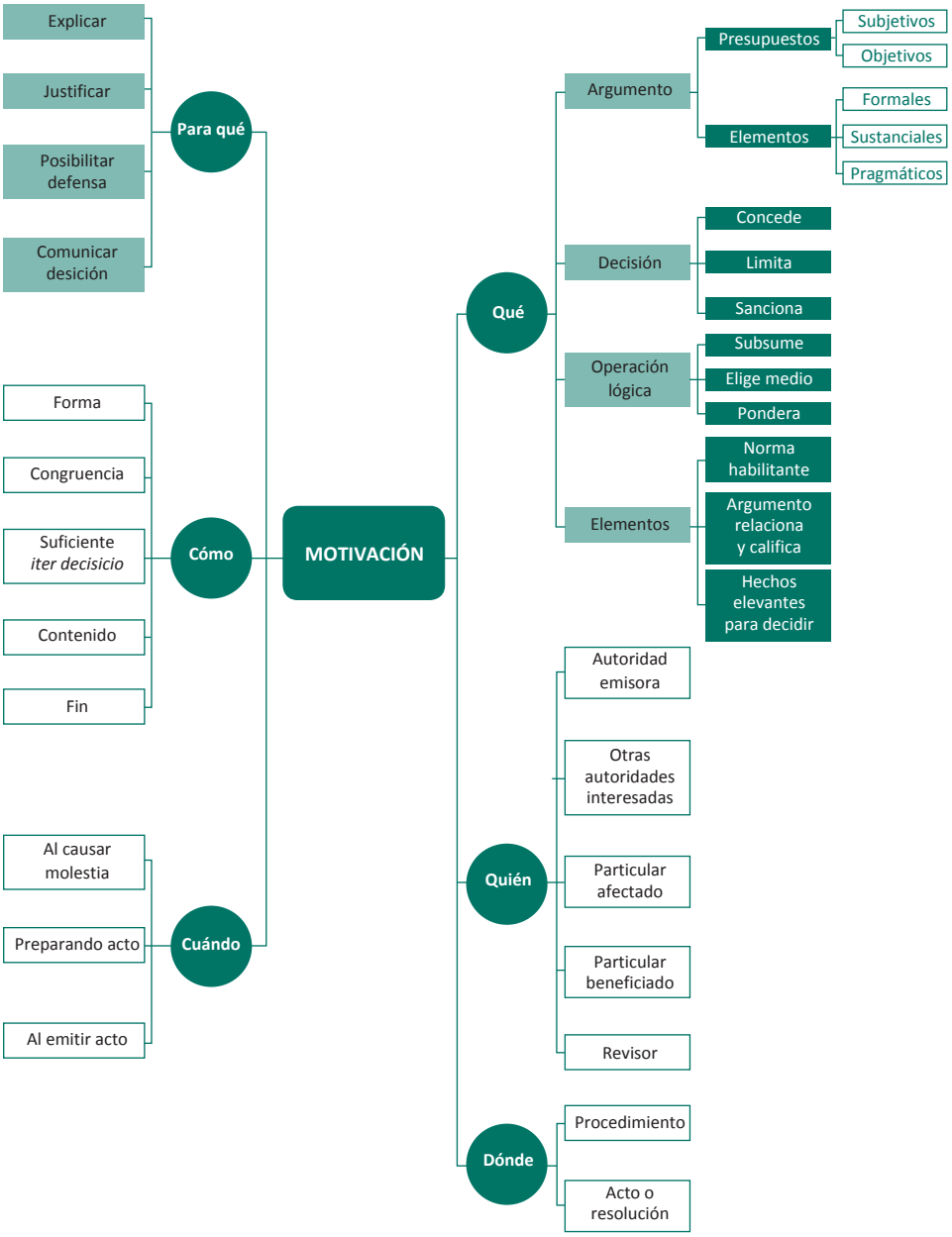
Al respecto, un criterio de jurisprudencia señala que el aspecto formal de esta garantía y su finalidad se traducen en explicar, justificar, posibilitar la defensa y comunicar la decisión:

1083 INAI. (2015). *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

1084 Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

1085 Véase el artículo 14 de la CPEUM.

Motivación: mapa conceptual



FUNDAMENTACIÓN Y MOTIVACIÓN. EL ASPECTO FORMAL DE LA GARANTÍA Y SU FINALIDAD SE TRADUCEN EN EXPLICAR, JUSTIFICAR, POSIBILITAR LA DEFENSA Y COMUNICAR LA DECISIÓN. El contenido formal de la garantía de legalidad prevista en el artículo 16 constitucional relativa a la fundamentación y motivación tiene como propósito primordial y ratio que el justiciable conozca el "para qué" de la conducta de la autoridad, lo que se traduce en darle a conocer en detalle y de manera completa la esencia de todas las circunstancias y condiciones que determinaron el acto de voluntad, de manera que sea evidente y muy claro para el afectado poder cuestionar y controvertir el mérito de la decisión, permitiéndole una real y auténtica defensa. Por tanto, no basta que el acto de autoridad apenas observe una motivación pro forma pero de una manera incongruente, insuficiente o imprecisa, que impida la finalidad del conocimiento, comprobación y defensa pertinente, ni es válido exigirle una amplitud o abundancia superflua, pues es suficiente la expresión de lo estrictamente necesario para explicar, justificar y posibilitar la defensa, así como para comunicar la decisión a efecto de que se considere debidamente fundado y motivado, exponiendo los hechos relevantes para decidir, citando la norma habilitante y un argumento mínimo pero suficiente para acreditar el razonamiento del que se deduzca la relación de pertenencia lógica de los hechos al derecho invocado, que es la subsunción.[1086]

Conviene destacar que la dinámica social exige, cada día, obtener la máxima promoción, protección y disfrute de los derechos fundamentales —incluyendo, por supuesto, a los derechos económicos, sociales, culturales y ambientales (DESCA)— para lo cual se requieren intervenciones, especialmente de la administración, a efecto de satisfacer de la mejor manera, el interés general de una manera equilibrada.

Obtener estas consecuencias que al parecer están tensión —eficacia de los derechos fundamentales frente a potestades pertinentes y necesarias para satisfacer el interés general— exige que cada día los derechos e intereses deban ser reconfigurados y puntualizados al momento de su aplicación en casos concretos.

Un ejemplo es cómo se han venido decantando los aspectos de la confidencialidad (vida privada, datos personales y secretos) frente a exigencias de transparencia, siempre con matices que los operadores deben conformar o diseñar al tomar decisiones en casos particulares, lo que, por supuesto, exige motivar esas conclusiones como las más idóneas o razonables.

Conviene recordar que el orden jurídico, no solo protege aspectos jurídicos formales, sino que incluye variados intereses, valores, políticas públicas, etc. por lo que criterios y exigencias de fundamentación y motivación[1087] (FyM) deben escalar y adaptarse a estos objetivos. El propósito es que, sin desatender la mejor y más eficiente satisfacción del interés general como ratio de la administración, éste debe irse construyendo, pero sin restringir de manera irrazonable o innecesaria, el ejercicio de derechos y libertades.

En síntesis, puede decirse que en esencia, la FyM es un argumento que da cuenta, de marea justificada que la decisión de una autoridad es la más efectiva, y que además que evita o causa la menor molestia posible.

2. ¿A quiénes se dirige?

Esta garantía, como todas, tiene dos sujetos: a) sujeto activo: titular del derecho y b) sujeto pasivo: Estado u obligado a dar cumplimiento al derecho.

Todas las autoridades que forman parte del Estado mexicano están obligadas a fundar y motivar los actos de molestia. Desde luego, están incluidos en este conjunto todos los

1086 Jurisprudencia I.4o.A. J/43, del Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito.

1087 En lo subsecuente FyM.

entes que forman parte de la administración pública, del Poder Legislativo[1088] y Judicial e[1089] incluso los órganos constitucionales autónomos como entidades que forman parte del Estado son sujetos pasivos y están vinculados a su cumplimiento. En algunos casos los particulares también son sujetos pasivos cuando actúan en funciones de autoridad, encontrándose obligados a fundar y motivar sus actos.

Por otra parte, el sujeto activo se identifica con el titular de la mencionada garantía, aclarando que el texto constitucional no hace distinción entre personas físicas o morales. Esto implica que dentro del universo de sujetos pasivos protegidos se encuentra cualquier persona, sea individual o colectiva, por lo que, siempre que resulte afectada por un acto de autoridad, podrá exigir a la autoridad que funde y motive su acto.

Por regla general, esta garantía tiene por sujeto de protección al administrado o gobernado, sin embargo, el Pleno de la Suprema Corte de Justicia de la Nación (SCJN) también ha señalado que las personas de derecho público pueden alegar infracción a los principios de fundamentación, motivación e irretroactividad de la Ley, especialmente en los casos que ello sea relevante a efecto de resolver los problemas competenciales formulados en una controversia constitucional, lo que sucede, por ejemplo: 1) tratándose de actos en los que un poder revisar los de otro, 2) cuando el sistema jurídico prevé distintas modalidades de actuación a cargo de algún poder público (ordinarias y extraordinarias) y/o 3) cuando existe un régimen normativo transitorio que altera los alcances de las atribuciones del órgano respectivo, tomando en cuenta que la violación de dichos principios en tales supuestos podría generar un pronunciamiento de invalidez por incompetencia constitucional, y no solo para efectos.[1090]

3. ¿Cuándo y dónde es necesario fundar y motivar?

El artículo 16 constitucional señala que tratándose de actos de molestia existe un deber de FyM. Sin embargo, también es necesario cumplir con este deber en caso de actos privativos. Jurisprudencialmente se ha entendido por actos de molestia aquellos provenientes de una autoridad que restringe de manera provisional o preventiva un derecho con el objeto de proteger determinados bienes jurídicos, mientras que los llamados actos privativos tienen por objeto la disminución, menoscabo o supresión definitiva de un derecho del gobernado.

Dichos actos pueden derivar de un procedimiento administrativo o implicar un acto o resolución de carácter administrativo o jurisdiccional. De ahí que se afirme que todo acto de autoridad debe fundarse y motivarse para cumplir con el mandamiento constitucional.

4. ¿Cómo se cumple con esta obligación?

En cuanto al grado o forma de cumplir esta garantía, la respuesta a esta interrogante la encontramos en el artículo 16 constitucional, al disponer que el acto de molestia debe emitirse por escrito por autoridad competente en la que funde y motive la causa legal del procedimiento.

1088 Época: Séptima época. Registro: 232351. Instancia: Pleno. Tipo de Tesis: Jurisprudencia. Fuente*: Semanario Judicial de la Federación*. Volumen 181-186, Primera Parte. Materia(s): constitucional, común. Tesis: Página: 239. "Fundamentación y motivación de los actos de autoridad legislativa".

1089 Época: Novena época. Registro: 176546. Instancia: Primera Sala. Tipo de Tesis: jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo XXII, diciembre de 2005. Materia(s): común. Tesis: 1a./J. 139/2005. Página: 162. Fundamentación y motivación de las resoluciones jurisdiccionales, deben analizarse a la luz de los artículos 14 y 16 de la constitución política de los estados unidos mexicanos, respectivamente.

1090 Época: Novena época. Registro: 177331. Instancia: Pleno. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo XXII, septiembre de 2005. Materia(s): constitucional. Tesis: P./J. 109/2005. Página: 891. "Controversia constitucional. Las personas de derecho público pueden alegar infracción a los principios de fundamentación, motivación e irretroactividad de la ley".

La FyM puede ser considerada un razonamiento práctico que legitime el actuar de las autoridades cuando impongan u ocasionen molestias a los particulares gobernados. En dicho razonamiento se deben expresar: i) antecedentes y presupuestos, ii) circunstancias del caso, iii) disposiciones que habiliten o justifiquen la conducta de la autoridad (competencia, procedimentales y sustantivas), iv) afectación o molestia que se infiere, v) razones o argumentos que den cuenta de anteriores aspectos, vi) soporte documental, vii) firma de quien emite la orden (autógrafa o electrónica).

La FyM entendida como un razonamiento tiene los siguientes elementos:

- Fundamentación (premisa jurídica):
  a) Cita de preceptos sustantivos, adjetivos y competenciales.
  b) Norma individualizada, en casos de lagunas o del resultado de ponderar principios, cuando no haya regla expresa idónea debe construirse, argumentalmente, la disposición pertinente.
- Motivación (premisa fáctica):
  a) Causa del procedimiento.
  b) Razonamientos legítimos, suficientes, congruentes y convincentes.
  c) Invocar hechos relevantes, cualificados del caso y encuadrables en el marco previsto por la ley.
  d) Correspondencia o subsumir hechos particulares del caso en la hipótesis de la norma.
  e) Adecuación entre norma fundante y caso concreto para legitimar consecuencias o efectos.
  f) Racionalidad o razonabilidad como soporte argumental.

Al respecto, el máximo tribunal ha señalado que, de acuerdo con el artículo 16 de la Constitución Federal, todo acto de autoridad debe estar adecuada y suficientemente fundado y motivado, entendiéndose por lo primero que ha de expresarse con precisión el precepto legal aplicable al caso y, por lo segundo, que deben señalarse, con precisión, las circunstancias especiales, razones particulares o causas inmediatas que se hayan tenido en consideración para la emisión del acto; siendo necesario, además, que exista adecuación entre los motivos aducidos y las normas aplicables, es decir, que en el caso concreto se configuren las hipótesis normativas.[1091]

Lo anterior implica que para fundamentar es menester expresar cuáles son las disposiciones normativas aplicables al caso en concreto. Mientras que para motivar es necesario explicar por qué dichas normas se están aplicando, en relación los hechos invocados, siendo necesario que, a partir de un ejercicio de subsunción, se puedan relacionar las premisas fácticas con las premisas normativas aplicadas.

Tratándose de actos administrativos, la autoridad debe ser explícita y señalar con exactitud su denominación, fundar su competencia, el lugar y la fecha de la expedición del acto administrativo, a fin de que el particular esté en posibilidad de conocer el carácter de quien lo emitió, si actuó dentro de su circunscripción territorial y en condiciones de conocer los motivos que originaron el acto, los fundamentos legales que se citen y si existe adecuación entre estos elementos, así como la aplicación y vigencia de los preceptos que, en todo caso, se contengan en el acto administrativo, para estar en aptitud de preparar adecuadamente su defensa, pues la falta de tales elementos en un acto autoritario implica dejar al gobernado en estado de indefensión ante el desconocimiento de los elementos destacados.[1092]

1091 Emitida por la Segunda Sala de la Suprema Corte de Justicia de la Nación, visible en la página 166. Tomo VI. Materia común del apéndice 2000.

1092 Época: Novena época. Registro: 191486. Instancia: Segunda Sala. Tipo de Tesis: jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo XII, Julio de 2000. Materia(s): constitucional, administrativa. Tesis: 2a./J.

Por otra parte, la SCJN ha señalado que tratándose de actos que no trasciendan de manera inmediata a la esfera jurídica de los particulares sino que se verifican solo en los ámbitos internos del gobierno, es decir, entre autoridades,[1093] la FyM se cumple: a) con la existencia de una norma legal que atribuya a favor de la autoridad, de manera nítida, la facultad para actuar en determinado sentido y, asimismo, mediante el despliegue de la actuación de esa misma autoridad en la forma precisa y exacta en que lo disponga la ley, es decir, ajustándose escrupulosa y cuidadosamente a la norma legal en la cual encuentra su fundamento la conducta desarrollada y b) con la existencia constatada de los antecedentes fácticos o circunstancias del hecho que permitan colegir con claridad que sí procedía aplicar la norma correspondiente y, consecuentemente, que justifique con plenitud que la autoridad haya actuado en determinado sentido y no en otro. A través de la primera premisa se dará cumplimiento a la garantía de debida fundamentación y mediante la observancia de la segunda, a la de debida motivación.[1094]

Un caso particular a destacar se da cuando el acto de autoridad se funda en una norma compleja, supuesto en el que la Segunda Sala de la SCJN ha señalado que debe transcribirse la parte correspondiente con la finalidad de especificar con claridad, certeza y precisión, las facultades que le corresponden, pues considerar lo contrario significaría que el gobernado tiene la carga de averiguar, en el cúmulo de normas legales que señale la autoridad en el documento que contiene el acto de molestia, si tiene competencia por grado, materia y territorio para actuar en la forma que lo hace, dejándolo en estado de indefensión, pues ignoraría cuál de todas las normas legales que integran el texto normativo es la específicamente aplicable a la actuación del órgano del que emana.[1095]

Cabe mencionar que cuando estamos ante facultades discrecionales de la autoridad administrativa, cuyo ejercicio implica la posibilidad de optar entre dos o más decisiones, esa actuación sigue sujeta a los requisitos de FyM exigidos por el artículo 16 de la CPEUM, debiendo dar razones respecto a la elección asumida dentro del rango concedido en el entendido que discrecionalidad no es sinónimo de arbitrariedad, todo lo cual permite que los actos discrecionales sean controlados por la autoridad jurisdiccional.[1096]

Tratándose del derecho sancionador —que incluye al penal y al administrativo sancionador— la teoría del caso implica una narrativa que explique cómo los hechos del caso satisfacen la teoría jurídica que se invoca, por tanto, no solo es la cita de preceptos, sino un enlace sistémico, concatenado y contextualizado que son la base o clave de la *ratio decidendi*

61/2000. Página: 5. "Actos administrativos. Para cumplir con la garantía de legalidad prevista en el artículo 16 constitucional deben contener el lugar y la fecha de su emisión".

1093 Época: Novena época. Registro: 192076. Instancia: Pleno. Tipo de tesis: jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo XI, Abril de 2000. Materia(s): constitucional. Tesis: P./J. 50/2000. Página: 813. "Fundamentación y motivación. Su cumplimiento cuando se trate de actos que no trasciendan, de manera inmediata, la esfera jurídica de los particulares".

1094 Época: Novena época. Registro: 192076. Instancia: pleno. Tipo de Tesis: jurisprudencia. Fuente*: Semanario Judicial de la Federación y su Gaceta.* Tomo XI, Abril de 2000. Materia(s): Constitucional. Tesis: P./J. 50/2000. Página: 813. "Fundamentación y motivación. Su cumplimiento cuando se trate de actos que no trasciendan, de manera inmediata, la esfera jurídica de los particulares".

1095 Época: Novena época. Registro: 177347. Instancia: Segunda Sala. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo XXII, septiembre de 2005. Materia(s): administrativa. Tesis: 2a./J. 115/2005. Página: 310. "Competencia de las autoridades administrativas. el mandamiento escrito que contiene el acto de molestia a particulares debe fundarse en el precepto legal que les otorgue la atribución ejercida, citando el apartado, fracción, inciso o subinciso, y en caso de que no los contenga, si se trata de una norma compleja, habrá de transcribirse la parte correspondiente".

1096 Época: Novena época. Registro: 195530. Instancia: pleno. Tipo de tesis: aislada. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo VIII, septiembre de 1998. Materia(s): administrativa. Tesis: P. LXII/98. Página: 56. "Facultades discrecionales. Apreciación del uso indebido de las concedidas a la autoridad".

que se pretende adopte el decisor. En efecto, la *ratio decidendi* son razones normativas que informan y justifican lo decidido, es decir, el razonamiento o principio normativo aplicable al caso que da respuesta a la *quaestio iuris*. Entendiendo que el razonamiento jurídico-práctico pretende dar respuestas a preguntas o problemas acerca de lo que, en un caso determinado, es debido hacer u omitir con base en lo que dispone el ordenamiento jurídico.

En el caso de resoluciones jurisdiccionales, el cumplimiento a esta garantía requiere del análisis exhaustivo de los puntos que integran la litis, es decir, en el estudio de las acciones y excepciones del debate, apoyándose en el o los preceptos jurídicos que permiten expedirla y que establezcan la hipótesis que genere su emisión, así como en la exposición concreta de las circunstancias especiales, razones particulares o causas inmediatas tomadas en consideración para la emisión del acto, siendo necesario, además, que exista adecuación entre los motivos aducidos y las normas aplicables al caso.[1097]

En este sentido, la motivación de las resoluciones jurisdiccionales no implica únicamente expresar argumentos explicativos del por qué se llegó a una decisión concreta, sino también demostrar que tal decisión no es arbitraria, incorporando en ella el marco normativo aplicable, los problemas jurídicos planteados, así como la exposición concreta de los hechos jurídicamente relevantes, probados y las circunstancias particulares consideradas para resolver. Consecuentemente, para determinar si una resolución jurisdiccional cumple con una adecuada FyM los razonamientos judiciales utilizados deben justificar la racionalidad de la decisión con el fin de dar certeza a los gobernados de por qué se llegó a tal conclusión y por qué es la más acertada, en tanto: (i) permiten resolver el problema planteado, (ii) responden a los elementos de hecho y de derecho relevantes para el caso y (iii) si la decisión es consistente respecto de las premisas dadas con argumentos razonables.[1098]

Por último, en el caso de actos materialmente legislativos como la expedición de normas por el Congreso de la Unión, la SCJN ha señalado que por FyM de un acto legislativo se debe entender la circunstancia de que el Congreso que expide la ley esté constitucionalmente facultado para ello, ya que estos requisitos, tratándose de actos legislativos, se satisfacen cuando actúa dentro de los límites de las atribuciones que la CPEUM correspondiente le confiere (*vid* fundamentación) y cuando las leyes que emite se refieren a relaciones sociales que reclaman ser jurídicamente reguladas (*vid* motivación). Sin embargo, el cumplimiento de esta garantía no implica que todas y cada una de las disposiciones que integran estos ordenamientos deben ser necesariamente materia de una motivación específica.

5. Jurisprudencia

"Fundamentación y motivación, concepto de". Tesis: I. 4o. P. 56 P, Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito, Registro: 209986. Octava época. Registro: 209986. Instancia: Tribunales Colegiados de Circuito. Tipo de Tesis: Aislada. Fuente: Semanario Judicial de la Federación. Tomo XIV, Noviembre de 1994. Materia(s): Penal. Página: 450.

"Artículo 16 constitucional. Fundamentación y motivación de los mandamientos de la autoridad". 2ª Sala Registro: 801680. Sexta época. Registro: 801680. Instancia: Segunda Sala. Tipo de Tesis: Aislada. Fuente: *Semanario Judicial de la Federación*. Volumen LII, Tercera Parte. Materia(s): Administrativa, constitucional. Tesis: Página: 63.

1097 Época: novena época. Registro: 176546. Instancia: Primera Sala. Tipo de tesis: jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Tomo XXII, diciembre de 2005. Materia(s): común. Tesis: 1a./J. 139/2005. Página: 162. "Fundamentación y motivación de las resoluciones jurisdiccionales, deben analizarse a la luz de los artículos 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos, respectivamente".

1098 Juicio de amparo directo 67/2018 del índice del Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito.

Tesis: 1a./J. 139/2005. Página: 162. "Fundamentación y motivación de las resoluciones jurisdiccionales, deben analizarse a la luz de los artículos 14 y 16 de la constitución política de los Estados Unidos Mexicanos, respectivamente." Novena época. Registro: 176546. Instancia: Primera Sala. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Tomo XXII, diciembre de 2005. Materia(s): Común.

Tesis: P./J. 50/2000. Página: 813. "Fundamentación y motivación. Su cumplimiento cuando se trate de actos que no trasciendan, de manera inmediata, la esfera jurídica de los particulares". Novena época. Registro: 192076. Instancia: Pleno. Tipo de Tesis: *Jurisprudencia. Fuente: Semanario Judicial de la Federación y su Gaceta.* Tomo XI, abril de 2000. Materia(s): Constitucional.

Tesis: 2a./J. 115/2005. Página: 310. "competencia de las autoridades administrativas. el mandamiento escrito que contiene el acto de molestia a particulares debe fundarse en el precepto legal que les otorgue la atribución ejercida, citando el apartado, fracción, inciso o subinciso, y en caso de que no los contenga, si se trata de una norma compleja, habrá de transcribirse la parte correspondiente". Novena época. Registro: 177347. Instancia: Segunda Sala. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Tomo XXII, septiembre de 2005. Materia(s): Administrativa.

Tesis: P. LXII/98. Página: 56. "Facultades discrecionales. Apreciación del uso indebido de las concedidas a la autoridad". Época: Novena época. Registro: 195530. Instancia: Pleno. Tipo de Tesis: Aislada. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Tomo VIII, septiembre de 1998. Materia(s): Administrativa.

Tesis: 2a./J. 61/2000. Página: 5. "Actos administrativos. Para cumplir con la garantía de legalidad prevista en el artículo 16 constitucional, deben contener el lugar y la fecha de su emisión". Novena época. Registro: 191486. Instancia: Segunda Sala. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Tomo XII, julio de 2000. Materia(s): Constitucional, Administrativa.

Tesis: P./J. 109/2005. Página: 891. "Controversia constitucional. Las personas de derecho público pueden alegar infracción a los principios de fundamentación, motivación e irretroactividad de la ley". Novena época. Registro: 177331. Instancia: Pleno. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Tomo XXII, septiembre de 2005. Materia(s): Constitucional.

"Fundamentación y motivación de los actos de autoridad legislativa". Séptima época. Registro: 232351. Instancia: Pleno. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación.* Volumen 181-186, Primera Parte. Materia(s): Constitucional, Común. Tesis: Página: 239.

Tesis: 1a./J. 139/2005. "Fundamentación y motivación de las resoluciones jurisdiccionales, deben analizarse a la luz de los artículos 14 y 16 de la constitución política de los Estados Unidos Mexicanos, respectivamente". Novena época. Registro: 176546. Instancia: Primera Sala. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Tomo XXII, diciembre de 2005. Materia(s): Común. Página: 162.

Tesis: I.4°A.39K (10ª): "Fundamentación y motivación. En tratándose de resoluciones judiciales". Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito.

"Normas complejas. Su naturaleza depende de la pluralidad de hipótesis que las componen". Décima época. Registro: 159997. Instancia: Tribunales Colegiados de Circuito. Tipo de Tesis: Jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta.* Libro XI, agosto de 2012, Tomo 2. Materia(s): Constitucional, Administrativa. Tesis: I.7o.A. J/65 (9a.). Página: 1244.

NOTAS

NOTAS

NOTAS

NOTAS

Geolocalización

José Soto Galindo

Geolocalización refiere a una tecnología que utiliza las coordenadas geográficas (latitud y longitud) de un objeto (radar, un teléfono móvil o un ordenador conectado a internet) para posicionarlo en un mapa con la mayor precisión posible. Este método es indispensable para completar servicios de telecomunicación y para la entrega y envío de datos a través de terminales móviles.

La geolocalización tiene distintas aplicaciones. En materia de seguridad pública se utiliza para localizar equipos de comunicación móvil en situaciones de urgencia a través del número 911 de operación nacional. En los servicios financieros de base tecnológica o *fintech* —por la contracción de los términos en inglés *financial* y *technology*— se utiliza para ubicar geográficamente transacciones digitales o como herramienta para inhibir el fraude y el lavado de dinero. En la jurisdicción de la Ciudad de México, la geolocalización es una herramienta de uso obligatorio por las empresas de transporte privado como medida de seguridad de los consumidores.[1099]

La geolocalización también se utiliza en los servicios de "mapas y navegación, servicios geográficos personalizados (como puntos de interés próximos), realidad aumentada, etiquetado geográfico de contenidos en Internet, rastreo del paradero de amigos, control de los hijos y publicidad basada en la ubicación"[1100] o para fines de colaboración de operadores de servicios de telecomunicaciones con autoridades de seguridad y justicia, como herramienta para la investigación o diligencia de investigación sobre la comisión de un delito y de su autoría.[1101]

1099 La obligatoriedad de contar con un sistema de geolocalización se instituyó mediante una reforma al "acuerdo por el que se reforman y adicionan disposiciones del acuerdo que modifica el diverso por el que se crea el registro de personas morales que operen y/o administren aplicaciones y plataformas informáticas para el control, programación y/o geolocalización en dispositivos fijos o móviles, a través de las cuales los particulares pueden contratar el servicio privado de transporte con chofer en el Distrito Federal, publicado en la *Gaceta Oficial de la Ciudad de México*, el 12 de Agosto de 2016", publicada en la *Gaceta Oficial de la Ciudad de México*, el 18 de agosto de 2018. Disponible de consulta: https://data.consejeria.cdmx.gob.mx/portal_old/uploads/gacetas/fab7c94f3cdc42a0545cca07ceb07a3c.pdf Fecha 30 de septiembre de 2018.

1100 Grupo de trabajo sobre protección de datos establecido por el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea (2011, 16 de mayo). Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. Bruselas: Comisión Europea, p. 3. Disponible en: https://www.apda.ad/system/files/wp185_es.pdf recuperado el 30 de septiembre de 201 8.

1101 Esta materia está regulada por los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión y los Lineamientos de Colaboración en Materia de Seguridad y Justicia emitidos por el Instituto Federal de Telecomunicaciones (IFT).

Con los datos generados por la ubicación geográfica de los aparatos de comunicación móvil se puede "disponer de una panorámica detallada de los hábitos y pautas del propietario de estos dispositivos y establecer unos perfiles exhaustivos. A partir de un periodo de inactividad nocturna puede deducirse el lugar donde duerme la persona, y a partir de una pauta de desplazamientos regulares por la mañana, la localización de su empresa. El perfil puede incluir, asimismo, datos derivados de las pautas de movimientos de sus amigos, sobre la base de lo que se conoce como gráfica social".[1102]

La jurisprudencia en México considera que el uso de la geolocalización en una investigación judicial, incluso si representara una injerencia a la vida privada de las personas (véase, intervención de comunicaciones privadas), no se trata de un acto privativo sino de un acto de molestia que persigue un fin legítimo y es necesaria, idónea y proporcional para proteger la vida o la integridad física de las víctimas del delito[1103] o evitar que se oculte o desaparezca el objeto del delito.[1104]

Para el Tribunal de Justicia de la Unión Europea no hay duda que con la información obtenida a partir de las tecnologías de geolocalización se pueden "extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan".[1105] Esto representa, a juicio del Tribunal Europeo, una injerencia en los derechos humanos que "resulta de gran magnitud y debe considerarse especialmente grave".[1106]

1. La geolocalización en tiempo real

La geolocalización en tiempo real refiere a la ubicación geográfica de un equipo de comunicación móvil en el momento de su activación o conexión con las redes de telecomunicaciones. La fracción XXXV del artículo 3 de la Ley Federal de Telecomunicaciones y Radiodifusión la define como "la ubicación aproximada en el momento en que se procesa una búsqueda de un equipo terminal móvil asociado a una línea telefónica determinada".

En materia de investigación judicial, el régimen jurídico mexicano considera la geolocalización en tiempo real de un equipo de comunicación móvil asociado a una línea de telecomunicaciones como una medida urgente y excepcional legalmente válida y que facilita localizar geográficamente un equipo de comunicación probablemente vinculado con la comisión de delitos.[1107]

1102 Grupo de trabajo sobre protección de datos establecido por el artículo 29 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea (2011, 16 de mayo). Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes. Bruselas: Comisión Europea, p. 7. Disponible en: https://www.apda.ad/system/files/wp185_es.pdf recuperado el 30 de septiembre de 2018.

1103 Tesis 2a. XLIV/2016 (10a.). Segunda Sala de la Suprema Corte de Justicia de la Nación. Décima época. *Gaceta del Semanario Judicial de la Federación*. Libro 33, agosto de 2016, p. 1305.

1104 Resolución del Pleno de la Suprema Corte de Justicia de la Nación a la Acción de Inconstitucionalidad 32/2012 promovida por la Comisión Nacional de los Derechos Humanos en contra del Congreso de la Unión y del presidente de los Estados Unidos Mexicanos en enero de 2014. La ponencia estuvo a cargo de la ministra Margarita Beatriz Luna Ramos.

1105 La Gran Sala del Tribunal de Justicia de la Unión Europea (TJUE) en las sentencias C-293/12 y C-594/12 del 8 de abril de 2014 declaró la invalidez de Directiva 2006/24/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Recuperado de: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=303366. Fecha de consulta: 30 de septiembre de 2018.

1106 La Gran Sala del Tribunal de Justicia de la Unión Europea (TJUE) en las sentencias C-293/12 y C-594/12 del 8 de abril de 2014 declaró la invalidez de Directiva 2006/24/CE del Parlamento Europeo y del Consejo de la Unión Europea, del 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

1107 Resolución del Pleno de la Suprema Corte de Justicia de la Nación a la acción de inconstitucionalidad 32/2012 promovida por la Comisión Nacional de los Derechos Humanos en contra del Congreso de la Unión y del presidente de los Estados Unidos Mexicanos en enero de 2014. La ponencia estuvo a cargo de la ministra Margarita Beatriz Luna Ramos.

El uso de la geolocalización para la investigación judicial se encuentra en distintos ordenamientos, como el Código Nacional de Procedimientos Penales (CNPP)[1108] y la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR).[1109] En términos técnicos, está descrita en los Lineamientos de Colaboración en Materia de Seguridad y Justicia emitidos por el Instituto Federal de Telecomunicaciones (IFT), el 2 de diciembre de 2015.[1110] Estos lineamientos son resultado de la reforma de la Ley Federal de Telecomunicaciones y Radiodifusión de 2014 que incluyó el título octavo sobre la colaboración obligatoria de los concesionarios y autorizados de telecomunicaciones con las autoridades de seguridad, procuración y administración de justicia.

El artículo 303 del CNPP identifica dos tipos de datos generados a partir del uso de las telecomunicaciones móviles:

1. la localización geográfica en tiempo real para ubicar geográficamente un aparato vinculado a una persona concreta al momento de su activación o conexión con las redes de telecomunicaciones y
2. el registro y control de los datos producidos por los aparatos móviles de telecomunicación al momento de su activación o conexión con las redes de telecomunicaciones a lo largo del tiempo.

Esta información puede ser requerida por el ministerio público (MP) cuando se considere que una línea telefónica se encuentra relacionada con los hechos que se investigan, de acuerdo con el artículo 303 del Código Nacional de Procedimientos Penales:

> Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados
>
> Cuando el MP considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente.

La Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN) especificó que las autoridades facultadas para solicitar la localización geográfica en tiempo real de los equipos de comunicación móvil son:[1111]

(I) el procurador general de la república, así como los procuradores de las entidades federativas y, en su caso, los servidores públicos en quienes deleguen esta facultad, en términos del artículo 21 de la Constitución Federal;

1108 Artículo 303, reformado mediante decreto en el *Diario Oficial de la Federación* el 17 de junio de 2016.

1109 El artículo 190 del título octavo obliga a los concesionarios y autorizados de telecomunicaciones a "colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes".

1110 Estos Lineamientos fueron modificados el 2 de abril de 2018 mediante un acuerdo publicado en el *Diario Oficial de la Federación* por el Instituto Federal de Telecomunicaciones (IFT). La modificación eliminó normas sobre manejo de datos personales, pues el pleno del IFT consideró que esa obligación ya estaba contemplada en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados promulgada el 26 de enero de 2017.

1111 Tesis 2a. XLIV/2016 (10a.). Segunda Sala de la Suprema Corte de Justicia de la Nación. Décima época. *Gaceta del Semanario Judicial de la Federación*. Libro 33, agosto de 2016, p. 1305.

(II) la Policía Federal, conforme a lo previsto en el artículo 8, fracción XXVIII, de la ley que la regula; y,

(III) la autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional en los supuestos establecidos en su artículo 5.

Estas autoridades pueden solicitar la localización geográfica en tiempo real de los equipos de comunicación móvil "cuando se presuma que existe un peligro para la vida o la integridad de las personas, lo que implica que dicha facultad no se circunscribe a un catálogo de delitos determinado, sino que encuentra su razón jurídica en la tutela de los derechos humanos a la vida y a la integridad personal, como valor supremo a cargo del Estado mexicano".[1112]

2. Las especificaciones descritas en las leyes

Los Lineamientos de Colaboración en Materia de Seguridad y Justicia describen las características técnicas de la geolocalización en México a partir de instrucciones precisas que deben seguir los concesionarios y autorizados de telecomunicaciones al momento de colaborar con las autoridades de seguridad, procuración y administración de justicia en la localización geográfica de una determinada línea telefónica.

El lineamiento cuadragésimo impone mínimos de precisión a partir de tecnologías basadas en la red celular (triangulación)[1113] o en el dispositivo móvil (GPS). Por triangulación, el lineamiento hace referencia a tecnologías como ToA (Time of Arrival), AoA (Angle of Arrival), UTDOA (Uplink Time Difference of Arrival), AECID (Adaptive Enhanced Cell-ID), WLS (Wireless Location Signatures) y tecnologías de localización basadas en la identidad celular, como Cell Global Identity (CGI Cell) o Cell ID. Por GPS, el lineamiento considera tecnologías como Global Position System (GPS), Assisted GPS (AGPS), Observed Time Difference (OTD) y Enhanced Observed Time Difference (EOTD).

Para la triangulación se determinan los siguientes alcances:

Tipo de Localidad	Precisión	Rendimiento
Urbana	< 100 m	67%
Suburbana	< 200 m	67%
Rural	< 500 m	67%

Para tecnologías basadas en el dispositivo móvil, los siguientes alcances:

Tipo de Localidad	Precisión	Rendimiento
Urbana	< 50 m	50%
Suburbana	< 50 m	67%
Rural	< 50 m	67%

1112 Ibídem.

1113 La triangulación refiere a un método de localización geográfica que utiliza dos antenas cuyo posicionamiento es conocido para captar la señal de una terminal de comunicación móvil y a partir de su distancia y dirección determinar su respectivo posicionamiento. Cfr. Unión Internacional de Telecomunicaciones (2011). *Manual de comprobación técnica del espectro*. Ginebra: Unión Internacional de Telecomunicaciones, p. 321.

El lineamiento cuadragésimo precisa que "en caso de que el concesionario esté imposibilitado técnicamente para llevar a cabo la localización geográfica mediante triangulación, debido a que no cuenta con la infraestructura de tres radio bases instaladas, como mínimo o, mediante GPS, el concesionario deberá indicar, al menos, el identificador de celda y la distancia aproximada a la que se encuentra el dispositivo o equipo terminal móvil, derivada de la interacción del dispositivo o equipo terminal móvil con la radio base". Las celdas y las radio bases refieren a la infraestructura que posibilita, a través de antenas, la transmisión y retransmisión de las señales de telecomunicaciones, como la telefónica o la recepción o envío de mensajes de textos (SMS) o de un paquete datos (conexión a internet).

Como hemos visto, la geolocalización tiene múltiples aplicaciones y puede representar un tratamiento de datos personales que otorgue, a través de su análisis, un perfil muy representativo de los usuarios de los objetos monitorizados con esta tecnología.

Grupo de empresas

Luis Manuel C. Meján

El grupo de empresas es un concepto de trascendental importancia para la materia de manejo de datos personales puesto que, tanto la legislación mexicana como los cuerpos normativos internacionales, obligan a las entidades adscritas a un control común a adoptar esquemas de protección de datos personales igualitarios que será analizado a partir de lo construido por la doctrina internacional y con referencia a cómo es tratado el fenómeno en la legislación mexicana.

1. Noción

El grupo de empresas, grupo de sociedades, grupo de empresas comerciales, grupo de empresas mercantiles, grupo corporativo o grupo societario puede definirse como el "conjunto de entidades jurídicas dedicadas a actividades empresariales dominadas por una de ellas que ejerce el control y que presentan una unidad de propósito empresarial".

La empresa "unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativos"[1114] es una realidad que consta de elementos objetivos: un patrimonio y elementos subjetivos: las personas que ejercitan profesionalmente una actividad económica con fines de producción de bienes o servicios.[1115]

El uso del término "grupo societario" parte del supuesto que sus integrantes son precisamente "sociedades", pero no hay que olvidar que existen otros fenómenos jurídicos que reproducen la idea del patrimonio independiente diferenciado, afecto a un fin sin que concurra el fenómeno de la pluralidad de sujetos (los fideicomisos, las sociedades unimembres, las unidades económicas, etc.) que pueden formar parte de un grupo de empresas o de sociedades.

Otros términos usados son "agrupación", el cual muestra la idea de que se trata de una realidad que conjunta voluntariamente a varios integrantes y "grupo corporativo" pues es lo referente a una corporación, término equivalente a "sociedad" que se ha hecho popular por su uso en el derecho anglosajón. [1116]

1114 Real Academia de la Lengua Española

1115 Peña, V. (2014). *Concurso Mercantil de Grupos Empresariales*. México. Editorial Tirant Lo Blanch, pp. 50 a 55.

1116 Black's Law Dictionary. "*Corporation*: *An entity having authority under law to act as a single person distinct from the shareholders who own it and having rights to issue stock and exist indefinitely*" or "[...] *a legal personality distinct from the natural persons who make it up, exists indefinitely apart from them and has legal powers that its constitution gives it*".

2. Elementos integradores

De las descripciones fenomenológicas que da la doctrina[1117] y de la observación empírica de la realidad se pueden deducir los siguientes elementos constitutivos de un grupo de sociedades:

A. Pluralidad de entidades

Debe entenderse que se trata de más de una entidad cada una con su personalidad, patrimonio y objeto propios.

- Naturaleza de los integrantes

Lo común es que sean sociedades mercantiles, pero puede haber entidades de cualquier otro tipo que permita la ley o, incluso fideicomisos, sucursales, contratos de asociación, *joint ventures*, etcétera. Las empresas pueden ser públicas o privadas, nacionales o extranjeras e incluso empresas de participación estatal.

- Tipos: vertical, horizontal

Existen dos formaciones estructurales básicas de grupos de sociedades: la horizontal y la vertical. En la primera, la sociedad madre es la que controla directamente al conjunto de todas las sociedades operando al mismo nivel. En la segunda, la sociedad matriz controla directamente a su filial, quien a su vez controla a una subfilial.

A partir de estos dos diseños básicos se pueden extender las estructuras grupales *ad infinitum* creando controladoras, subcontroladoras, grupos y subgrupos, trascender fronteras y regímenes jurídicos que las regulen, incorporar inversionistas y asociados, etcétera, como es el caso de los grandes consorcios y conglomerados internacionales.

- Objeto estructurado, objeto diverso

Los objetos sociales de las empresas afiliadas a un grupo pueden ser similares, complementarios o absolutamente disímbolos. A partir de estos tres esquemas básicos se pueden conformar grupos de sociedades sencillos o muy complejos o diversas secciones de un conglomerado empresarial muy grande. La unidad empresarial puesta por la sociedad dominante les da a los integrantes su común denominador.

3. El control

Se requiere que uno de los integrantes del grupo ejerza un control sobre los demás "la sociedad dominante" o en el léxico usual, la "controladora". Es el factor que aglutina, de *jure* o de *facto*, al grupo de sociedades. "Control: capacidad de determinar, directa o indirectamente, la política operacional y financiera de una empresa".[1118]

Una sociedad es dominante en virtud de factores aislados o combinados:

a) ser propietaria de una parte suficientemente importante del capital de las demás que forman el grupo,
b) tener la capacidad de designar los órganos corporativos y
c) poder decidir sobre las políticas directivas, administrativas u operacionales de la detentada.

1117 "Frente a una unidad empresarial en sentido económico existe una pluralidad de entidades cada una con personalidad jurídica propia". Oriol, J. (1993). *Grupos de entidades de crédito*. Madrid. Editorial Civitas, p. 90. "Situación de varios empresarios (generalmente sociedades) jurídicamente independientes que, por estar sometidos a una dirección única de contenido general que constituyen una unidad económica" Duque, J. (s. f.). *Concepto y significado institucional de los grupos de empresas.* Madrid. Junta de Decanos de los Colegios Notariales.

1118 ONU. (2012). *Guía Legislativa de CNUDMI sobre el régimen de la insolvencia. Tercera Parte: Trato otorgable a los grupos de empresas en situaciones de insolvencia.* Nueva York. Naciones Unidas, p. 2.

Se da también el caso de las empresas que adquieren la totalidad o una parte significativa de los productos o servicios que genera la otra, pues la amenaza de dejar de hacerlo puede ser suficiente para que la empresa dominada acepte las decisiones de la dominante.

El poder de control debe darse de una manera estable, una coyuntura temporal no parecería ser suficiente para definir la existencia de un grupo.

El concepto de control llega a ser el elemento determinador de un grupo: éste será el conjunto de entidades que estén sujetas al mismo poder.

La existencia del control no significa que quienes integran el grupo no puedan tomar decisiones en forma independiente. Cierta independencia es incluso parte de lo que se desea al constituir un grupo: que cada integrante se maneje por sí mismo, aunque en las grandes decisiones o lineamientos se ejerza un control centralizado.

De una sociedad que ejerce el control dependen las demás que se han venido designando en la práctica como sociedades subsidiarias, filiales o afiliadas, detentadas, controladas, etc., términos con los que se subraya el concepto de estar sujetas al control directo o indirecto de la sociedad dominante o controladora.

4. El común denominador: la unidad empresarial

Se trata de un concepto que no es de naturaleza jurídica: compartir el mismo sentido de dirección y de propósitos económicos con similitud en los estilos de operación que le da cohesión al complejo. Considerar dos elementos:

a) Unidad de propósito empresarial

En el fondo todas quieren lo mismo: el quehacer de las diversas empresas debe coincidir en un propósito conjunto. Económicamente todos tienen el mismo propósito lucrativo.

En toda empresa existe una cultura empresarial, cuando esa cultura contagia a las demás empresas del grupo se establece un muy fuerte común denominador entre todas ellas.

La visión fiscal, de competencia económica y financiera de las empresas lleva a que la operación de un grupo sea vista como una sola unidad y considerada como tal.[1119]

b) Propósito de diversificación de riesgo

La diversificación de riesgos es el propósito mercantil más claro en un grupo. La directiva empresarial decide aventurarse en una nueva empresa (constituyéndola o adquiriéndola) pero no desea que el éxito o fracaso de la misma contamine la marcha de las otras empresas que forman el grupo. Se trata del mismo socio capitalista, la misma dirección y filosofía empresarial pero independiente, por salud de ese negocio, de los demás y, en último término, del propio socio capitalista. Puede tratarse de un proyecto al que se invita un socio minoritario con el que no se comparten los demás negocios.

Esta posibilidades de diversificación y de flexibilidad ha hecho más grande el concepto de grupos de sociedad y ha formado los llamados "conglomerados" o "consorcios" es decir, un grupo conformado por varios grupos.

1119 Por ejemplo, el Código de Comercio Francés requiere que las sociedades que forman un grupo establezcan y publiquen anualmente contabilidades consolidadas y un informe de la gestión grupal. "*Article L233-16 I. Les sociétés commerciales établissent et publient chaque année à la diligence du conseil d'administration, du directoire, du ou des gérants, selon le cas, des comptes consolidés ainsi qu'un rapport sur la gestion du groupe, dès lors qu'elles contrôlent de manière exclusive ou conjointe une ou plusieurs autres entreprises , dans les conditions ci-après définies".*

5. Naturaleza jurídica del grupo de sociedades

Una serie de motivos extrajurídicos motivan la creación de los grupos de sociedades. Estos motivos son de índole fiscal, laboral, de administración de recursos, de legislaciones con marcos jurídicos diversos, de mercados, geográficas, políticas adoptadas por los inversionistas, obligaciones impuestas por autoridades, etcétera.

De las legislaciones que han tratado el fenómeno[1120] se desprende que el impulso o el *élan* jurídico en la formación de un grupo se da conforme dos posibles sistemas:

El sistema orgánico, en donde la ley asigna consecuencias a lo que las partes, voluntaria o inadvertidamente, han deseado, colocándose en el supuesto de hecho (y de derecho) de una situación de dependencia. A lo hecho por las partes, el sistema normativo les regula las consecuencias de derecho que se darán entre los integrantes, frente a accionistas, mayoritarios y minoritarios, frente a trabajadores y frente a terceros.[1121]

El sistema contractual consiste en crear un grupo de sociedades a partir de un acto jurídico contractual por medio del cual una variedad de sociedades preexistentes y con conformaciones de capital diversas deciden formarse en un grupo pactando cómo se ejercerá el poder y las líneas decisorias del grupo. Esta es la figura que el derecho alemán ha llamado *konzern*:[1122] "Cuando una empresa dominante y una o más empresas dependientes están subsumidas bajo la dirección unificada de la empresa dominante, forman un grupo (*konzern*); las empresas, individualmente, son empresas grupales (*konzernunternehmen*). Empresas entre las cuales existe un contrato de dominación o de las cuales una ha sido incorporada a la otra deben ser consideradas como subsumidas bajo una dirección unificada. Se presume que una empresa dependiente forma un grupo con la empresa dominante".[1123]

El contrato respectivo se ha llamado contrato de dominación, pues somete la vida social al poder directivo de la sociedad que se ha designado como dominante y regula las relaciones con accionistas minoritarios, con acreedores, con el manejo de las pérdidas, etcétera.[1124]

El grupo no es una entidad con personalidad jurídica, sino una entidad de tipo económico con una estructura jurídica detrás. El derecho reconoce la existencia del fenómeno. De las legislaciones donde se encuentra un tratamiento de agrupación de sociedades, pueden desprenderse algunas características integradoras de esta realidad jurídica, por ejemplo el tratamiento fiscal que se consolida para tributar como una sola entidad o —en el caso de las entidades financieras (banca y similares) que consideran a las entidades que se relacionan entre sí como una unidad para efecto de conceder crédito hasta determinados topes agregando el otorgado a cada una de las entidades para limitar el riesgo financiero—; el concepto de "partes relacionadas" que lleva a modular las relaciones jurídicas que sostie-

1120 Existen tratamientos ad hoc en Francia, Alemania, Estados Unidos de América, Brasil, Portugal, España, Argentina por citar unos cuantos.

1121 Sistema seguido en Bélgica, España, Italia, Francia y Reino Unido.

1122 Sistemas en Brasil, Portugal y Taiwán. Argentina contempla un "consorcio de cooperación"

1123 Ley de Sociedades por Acciones (*aktiengesetz*) §18 I Citado por Manóvil, R. (1998). Grupos de Sociedades en el derecho comparado. Abeledo Perrot. Buenos Aires, p. 195. Disponible en: http://www.edkpublicaciones.com/up/index.php/indice-11/agrupacion-de-empresas-y-sociedades.

1124 "Constitución del grupo. Según exista o no una relación de dominio entre la sociedad que dirige el grupo y las que se someten a su poder de dirección, se suele distinguir entre dos tipos de grupos de sociedades: el grupo jerárquico o de subordinación y el paritario o por coordinación… ambos supuestos constituyen una modificación de la vertiente organizativa y patrimonial de las sociedades que lo componen". Memento Práctico Francis Lefebvre. "*Sociedades Mercantiles*". Ediciones Francis Lefebvre. Madrid, 2008. Página 1381., citado en Luis Manuel C. Méjan. (2018). "Agrupación de Empresas y Sociedades", en *Perspectiva Jurídica*, No. 11, Facultad de Derecho, Universidad Panamericana, campus Guadalajara. Disponible en: http://www.edkpublicaciones.com/up/index.php/indice-11/agrupacion-de-empresas-y-sociedades

nen los integrantes de un grupo entre sí o frente a terceros; la posibilidad de que un grupo de sociedades adopte un nombre que los identifique como tal, distinto a la denominación formal de cada una de las entidades que lo conforman.

6. Los grupos de empresas en la legislación mexicana

El fenómeno "grupo de sociedades" no está tratado en la legislación. Sin embargo, está presente en varias leyes pero para servir a los propósitos de la propia ley y no a los del concepto corporativo, por ello es necesario acudir a la doctrina y a la analogía para resolver los casos prácticos que se presenten.

6.1 Ley General de Sociedades Mercantiles

Esta ley, que lógicamente debiera abordar el tema, es omisa en ello.[1125]

6.1.1 Ley de Concursos Mercantiles

Esta ley trata el fenómeno solo desde el punto de vista procesal previendo la acumulación y manejo por cuerda separada de los concursos mercantiles de las empresas que forman el grupo, concepto conocido como coordinación procesal.[1126]

6.2 Ley Federal de Competencia Económica

Esta ley utiliza la expresión "grupo de interés económico" para referirse al fenómeno de grupos de sociedades sin definirlo y admite que puede contribuir a una de las prácticas que esta ley regula, previene y sanciona, pues al amparo de las diversas personalidades jurídicas de las empresas que lo conforman, puede darse un monopolio o una práctica monopólica.

6.3 Legislación financiera

Estas leyes abordan el tema y conceptos relacionados con el fenómeno, con diversos propósitos propios.

En el caso del mercado bursátil, el tópico tiene relevancia para efectos de transparencia de la información que recibe el gran público inversionista. La Ley del Mercado de Valores y la Ley de Instituciones de Crédito introducen las definiciones que se muestran en el cuadro siguiente y que son reproducidas en las demás leyes del sistema financiero.

Es más clara la creación de las agrupaciones financieras (que nacieron en la ley de 1990 que fue abrogada por la nueva de enero de 2014), esta ley regula un verdadero grupo corporativo. Los grupos financieros estarán constituidos por una sociedad controladora y por lo menos dos entidades financieras. Esa realidad (grupo financiero) no tiene ni personalidad jurídica, ni patrimonio, ni órganos propios, el control lo ejerce la sociedad controladora que no puede tener por objeto social otro que el de detentar el capital de las controladas. La existencia de un grupo de control[1127] apunta hacia el hecho de que el

1125 De ella solo puede concluirse que no podrá integrar un grupo de sociedades, como controlada, una sociedad por acciones simplificada ya que los socios de ésta deben ser personas físicas que no sean socios de ninguna otra sociedad. Algo similar pasa con las sociedades cooperativas, cuyos socios deben ser necesariamente personas físicas. LGSC. Art. 2; LGSM. Art.260

1126 "Administración coordinada de dos o más procedimientos de insolvencia abiertos contra diversas empresas de un grupo. Cada empresa sigue siendo una entidad separada y distinta, con su propio activo y pasivo". CNUDMI. (2010). *Guía legislativa de la CNUDMI sobre el régimen de la insolvencia, tercera parte: tratamiento de los grupos de empresas en situaciones de insolvencia.* ONU. Nueva York, p. 2

1127 Ley Para Regular las Agrupaciones Financieras: "Artículo 28 en el supuesto de que una persona o grupo de personas, accionistas o no, pretenda adquirir directa o indirectamente el veinte por ciento o más de las acciones representativas de la serie o del capital social de la sociedad controladora, o bien, el control, estas deberán solicitar previamente autorización de la secretaría [...]".

control no solo depende de la tenencia de capital, sino que puede obedecer a otras realidades. También hay una presencia interesante del sistema contractual: se ordena celebrar un convenio entre la controladora y cada una de las entidades que lo integran, a efecto de que aquella responda subsidiaria e ilimitadamente de las obligaciones y pérdidas de cada una de estas, sin que esa responsabilidad se establezca entre las entidades que conforman el grupo.

Estas leyes usan los conceptos para propósitos de transparencia y control, así como para regular las asociaciones que se pueden dar entre instituciones financieras y grupos de negocios no financieros.

Definiciones de conceptos relacionados de las leyes financieras[1128]

Concepto	Definición
Grupo empresarial	Es el conjunto de personas morales organizadas bajo esquemas de participación directa o indirecta del capital social, en las que una misma sociedad mantiene el control de dichas personas morales. Asimismo, se considerarán como grupo empresarial a los grupos financieros constituidos conforme a la Ley para Regular las Agrupaciones Financieras.
Grupo de personas	Las personas que tengan acuerdos de cualquier naturaleza para tomar decisiones en un mismo sentido, salvo prueba en contrario, constituyen un grupo de personas, ejemplos de grupos de personas son: a) las personas que tienen parentesco por consanguinidad, afinidad o civil hasta el cuarto grado, los cónyuges, la concubina y el concubinario. b) las sociedades que forman parte de un mismo consorcio o grupo empresarial y la persona o conjunto de personas que tengan el control de dichas sociedades.
Control	Es la capacidad de una persona o grupo de personas, de llevar a cabo cualquiera de los actos siguientes: a) imponer, directa o indirectamente, decisiones en las asambleas generales de accionistas, de socios u órganos equivalentes, o nombrar o destituir a la mayoría de los consejeros, administradores o sus equivalentes, de una persona moral, b) mantener la titularidad de derechos que permitan, directa o indirectamente, ejercer el voto respecto de más del cincuenta por ciento del capital social de una persona moral y c) dirigir, directa o indirectamente la administración, la estrategia o las principales políticas de una person a moral, ya sea a través de la propiedad de valores, por contrato o de cualquier otra forma.
Consorcio	Es el conjunto de personas morales vinculadas entre sí por una o más personas físicas que integran un grupo de personas y tienen el control de las primeras.
Vínculo de negocio	Es el que se deriva de la celebración de convenios de inversión en el capital de otras personas morales, en virtud de los cuales se obtiene una influencia significativa, quedando incluidos cualquier otro tipo de actos jurídicos que produzcan efectos similares a tales convenios de inversión.
Vínculo patrimonial	Es el que se deriva de la pertenencia por parte de una institución a un consorcio o grupo empresarial, al que también pertenece la persona moral a que se refiere el artículo 86 de esta Ley.
Grupo financiero	Es aquella agrupación integrada por la sociedad controladora y por entidades financieras, autorizada por la Secretaría de Hacienda y Crédito Público para funcionar como tal en términos del artículo 11 de esta Ley.

1128 Véase el artículo 2 de la LMV, 45-P de la Ley de Instituciones de Crédito y 11 de la Ley para Regular las Agrupaciones Financieras.

6.4 La legislación fiscal

La Ley del Impuesto sobre la Renta ofrece la posibilidad de establecer un régimen consolidado para efectos fiscales tanto en empresas nacionales como en grupos multinacionales, cuando la integradora detente al menos 51 por ciento del capital.

7. Los grupos de empresas y manejo de datos personales

La Ley Federal de Protección de Datos en Posesión de Particulares (LFPDPPP) no define los conceptos pero los usa cuando se refiere a las transferencias nacionales o internacionales de datos o a su comunicación a terceros. Estas transferencias son válidas y pueden darse sin necesidad del consentimiento del titular de los mismos (es decir de la persona física a la que corresponden los datos personales). La LFPDPPP indica que tal cosa puede suceder: "III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas".[1129]

Esto es, se parte de un concepto genérico de grupo de sociedades sin una definición legal. No se aclara el concepto de sociedad controlada y se utilizan referencias a subsidiarias o afiliadas o cualquier sociedad del mismo grupo. Se exige que se opere bajo los mismos procesos y políticas internas, lo cual significa, ni más ni menos, el concepto de "control" como se ha explicado arriba.

El Reglamento de la LFPDPPP contempla la existencia de un grupo sin personalidad jurídica (artículo 8). Ya se ha establecido que los grupos de sociedades no tienen personalidad jurídica, por lo tanto debe entenderse que se está refiriendo a las sociedades que integran un grupo de sociedades. Posteriormente, al regular la disposición comentada anteriormente, el artículo 70 del RLFPDPPP establece la obligación para todos los integrantes del grupo de conservar las mismas obligaciones que tiene el responsable receptor de los datos personales. La problemática aquí consiste en dilucidar qué puede entenderse por los términos usados por la LFPDPP y su reglamento, pues no los definen. Esos términos son: "grupo empresarial", "controladora", "subsidiaria", "afiliada" y "matriz".

La trascendencia que tiene la comprensión de dichos términos es que la excepción de obtener el consentimiento del titular que se da dentro del seno de un grupo representa un alivio en las cargas operacionales que tiene el responsable en la obtención de los datos, en la conservación del comprobante del consentimiento y en la seguridad que le da operar cuando el consentimiento no es necesario.[1130]

Para ello habrá que acudir a tres herramientas:

a) los conceptos que en el lenguaje común y en los diccionarios de la lengua se atribuyen a dichas expresiones.
b) usar por analogía el trato que otros cuerpos legales del marco legislativo mexicano asignan a tales conceptos.
c) usar cuerpos normativos internacionales que refieren a la misma realidad dentro del campo del tratamiento de los datos personales.

En este último terreno cabe señalar la existencia de dos cuerpos legales de referencia: a) Los Estándares de Protección de Datos para los Estados Iberoamericanos (Estándares

1129 LFPDPP, artículo 37, fracción III.

1130 Véase en este mismo diccionario la voz "consentimiento".

Iberoamericanos)[1131] y b) el Reglamento General de Protección de Datos del Parlamento Europeo (el RGPD o GDPR por sus siglas en inglés) que, además de ser una referencia internacional, incide en las relaciones que titulares y responsables mexicanos tienen con los países europeos y latinoamericanos.

Los Estándares Iberoamericanos[1132] indican: "5.4. Cuando el tratamiento de datos personales lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control deberá considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine efectivamente otra de las empresas del grupo". Aunque la norma busca tan solo situar el lugar de ubicación del grupo, da luz al concepto de "sociedad controladora" (la que ejerce el control).

Por su parte el RGPD (cuyo considerando 36 es similar al de la ubicación del grupo usado en los Estándares Iberoamericanos) es más preciso cuando determina que "una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, grupo empresarial".[1133] Congruente con su artículo 4, inciso 19 que define grupo empresarial como: grupo constituido por una empresa que ejerce el control y sus empresas controladas.

El artículo 88, inciso 2 del RGPD define "grupo empresarial " como: "unión de empresas dedicadas a una actividad económica conjunta".

El RGPD tiene, además, varias referencias a los conceptos de grupo empresarial y de empresas afiliadas.[1134]

En suma, debe concluirse que los conceptos usados en la legislación mexicana y en especial en las normas que tratan el manejo, recopilación, conservación, uso y transmisión de datos personales deben de entenderse en los siguientes términos:

Grupo de sociedades o empresas: una pluralidad de entidades que se encuentran vinculadas porque una de ellas ejerce el control sobre las demás derivado de la tenencia de capital mayoritario o de cualquier otro mecanismo que le permite influir en la toma de decisiones respecto de la designación de los integrantes de sus órganos corporativos y en las políticas generales financieras y de operación, manifestando una unidad de propósito empresarial.

Por sociedades subsidiarias, afiliadas o filiales, controladas, detentadas, etcétera, debe entenderse a aquellas entidades jurídicas sobre las cuales, por cualquier mecanismo directo o indirecto, una sociedad ejerce el control, definido como en el párrafo que antecede.

1131 Emitidos por la Red Iberoamericana de Protección de Datos de la que México forma parte a través del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

1132 http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

1133 Reglamento Europeo de Protección de Datos. Párrafo 37 de los considerandos. https://www.boe.es/legislacion/codigos/codigo.php?id=55&modo=1&nota=0

1134 Véanse los considerandos 36, 37, 48, 110 y los artículos 4 (incisos 19, 20), 36 (inciso 3, subinciso b), 37 (inciso 2) 47 (incisos 1a), 2 a) h) j) l) m) y 88 (inciso 2).

NOTAS

NOTAS

NOTAS

NOTAS

Impacto

Christian Paredes González

Desde una acepción general, de acuerdo con el *Diccionario de la Real Academia Española* (DRAE) el término impacto se define como el "efecto producido en la opinión pública por un acontecimiento, una disposición de la autoridad, una noticia, una catástrofe, etcétera".

Por otra parte, las Recomendaciones en Materia de Seguridad de Datos Personales para el Sector Privado (Recomendaciones de Seguridad),[1135] la *Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales*, publicada en 2015[1136] (GISGSDP) y las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales[1137] definen "impacto" en idénticos términos y señalan que es "una medida del grado de daño a los activos o cambio adverso en el nivel de objetivos alcanzados por una organización".

Incidente de seguridad

Andrés Velázquez Olavarrieta

La *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP), (marzo 2014) define al incidente como "el escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades". También define a la amenaza como "circunstancia o evento con la capacidad de causar daño a una organización" y a la vulnerabilidad como "la falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas".

En términos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) las vulneraciones de seguridad son incidentes ocurridos en cualquier fase del tratamiento datos. El Artículo 63 de la LFPDPPP considera cuatro situaciones: la pérdida o destrucción no autorizada; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado y el daño, alteración o modificación no autorizada.

1135 Publicadas el 30 de octubre de 2013 en el *Diario Oficial de la Federación*.

1136 INAI. (2015). *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

1137 INAI. (2018). *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

Partiendo de lo anterior, un incidente de seguridad es un evento adverso o una violación a la política de seguridad de la información que compromete o puede comprometer la seguridad de la información implícita o explícitamente.

Información confidencial

Jimena Moreno González

Para abordar el concepto y el alcance de lo que significa información confidencial es necesario revisarlo desde sus orígenes. Un antecedente importante es el concepto de derecho a la vida privada. En 1881 la revista *Harvard Law Review* publicó un artículo al que tituló "The right to privacy" (que se ha traducido en el derecho a estar solo) que tuvo un impacto importante en el caso "Griswold vs. Connecticut". El caso mencionado se originó cuando Estelle Griswold, directora ejecutiva de la liga de *Planned Parenthood* de Connecticut, proporcionó información, instrucción y otros consejos médicos a las parejas casadas con respecto al control de la natalidad. Estelle Griswold y su colega Lee Buxton, ginecólogo de la Escuela de Medicina de la Universidad de Yale, fueron condenados de acuerdo con la legislación de Connecticut que penalizó la provisión de asesoría y otros tratamientos médicos a las personas casadas con el propósito de prevenir la concepción. La pregunta relevante en este caso fue la siguiente: ¿la Constitución protege el derecho de privacidad conyugal contra las restricciones estatales sobre la capacidad de una pareja para recibir asesoramiento en el uso de anticonceptivos? Y la conclusión fue que aunque la Constitución no protege explícitamente un derecho general a la privacidad, las diversas garantías dentro de la Declaración de Derechos crean penumbras o zonas que establecen un derecho a la privacidad. Juntas, la primera, la tercera, la cuarta y la novena enmiendas crean un nuevo derecho constitucional: el derecho a la privacidad en las relaciones matrimoniales. El estatuto de Connecticut está en conflicto con el ejercicio de este derecho y, por tanto, es nulo".[1138]

Un antecedente previo se da en el derecho inglés en el caso "John Entick (Clerk) vs. Nathan Carrington y otros tres".[1139] En 1762 en Westminster, Inglaterra, Nathan Carrington y oficiales gubernamentales, bajo las órdenes del secretario de Estado, irrumpieron mediante la fuerza, sin consentimiento y en contra de su voluntad la casa del Sr. Entick. Se entrometieron en sus pertenencias y las de su familia, revisaron todas las habitaciones de la casa, los libros, documentos y toda la información personal del Entick con la justificación de que estaban buscando panfletos y documentos que presuntamente iban en contra del rey.

En 1762 John Entick demandó por allanamiento. En esta sentencia el juez Lord Camden señaló que los oficiales del gobierno no pueden irrumpir en la casa del Entick sin una autorización, misma que debe estar prevista en una ley o en el *common law*. Esta sentencia ha servido como precedente para la interpretación de la cuarta enmienda de la constitución de los Estados Unidos de América[1140] y como antecedente del artículo 8 del Convenio Europeo para la protección de los Derechos Humanos y de las Libertades Fundamentales en lo referente al derecho al respecto a la vida privada y familiar.[1141]

1138 Oyez. (2017). "*Griswold vs. Connecticut*". Disponible en: https://www.oyez.org/cases/1964/496

1139 Bailii. (1765). *"Entick vs. Carrington and three others".* Disponible en: http://www.bailii.org/ew/cases/EWHC/KB/1765/J98.html.

1140 Hickman, T. (2016). "Entick vs. Carrington and analogues in modern law". En *Judicial Review.* Disponible en: https://www.tandfonline.com/doi/full/10.1080/10854681.2016.1183356

1141 Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales.

Adicionalmente, "antes de la Carta de las Naciones Unidas (firmada el 26 de junio de 1945) ya existían ciertos elementos de internacionalización de los derechos humanos relacionados con el respeto a la vida privada. Sin embargo, a partir de la Segunda Guerra Mundial y la ruptura de los valores más elementales por los regímenes totalitarios, se hizo evidente la necesidad de la protección internacional de los derechos humanos como condición esencial para la paz y el progreso de la humanidad. Tal necesidad quedó plasmada en una serie de documentos (el discurso sobre el estado de la Unión de 1941 —denominado de las cuatro libertades, del presidente norteamericano Franklin D. Roosevelt; la Conferencia de Dumbarton Oaks de 1944, entre las potencias aliadas, sobre las bases de la sociedad internacional y creación de la ONU; la Conferencia Interamericana de Chapultepec de 1945, sobre problemas de la guerra y de la paz y la Conferencia de San Francisco de 1945, en la que se adoptó la Carta de las Naciones Unidas, que contribuyeron a fijar el contenido definitivo de lo que sería la Declaración Universal de los Derechos Humanos (DUDH)".[1142]

Es así que el artículo 12 de la DUDH contempla el derecho a la vida privada estableciendo que el derecho a la vida privada es un derecho humano.[1143] Dicho artículo es retomado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de Naciones Unidas, el cual consagra al respecto que "1) nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, o lugar físico, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación y 2) toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Asimismo, en el artículo 11 de la Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica se establece que "1) toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad, 2) nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación y 3) toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

El derecho a la vida privada es un concepto muy amplio que va más allá del derecho a la privacidad y que no se puede definir de manera limitativa, así ha concluido en reiteradas ocasiones la Corte Interamericana de Derechos Humanos (CIDH).[1144]

Para entender el desarrollo del concepto de información confidencial es preciso comenzar por analizar el tema desde el derecho comparado y posteriormente la manera en que ha sido abordado en el derecho mexicano.

La CIDH alemana afirma que "esta vinculación comunitaria del individuo reconocida por la Ley Fundamental de Bonn hace posible también el establecimiento de ciertos límites externos a los derechos fundamentales que son garantizados sin reservas." En idéntico

---

Artículo 8. Derecho al respeto a la vida privada y familiar.
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

1142 Roda, J. (2014). *La Declaración Universal de los Derechos Humanos*, p. 1. Disponible en: https://tirant.com/libreria/actualizaciones/Tema14_27abril.pdf

1143 Declaración Universal de Derechos Humanos (1948). "Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

1144 Corte Interamericana de Derechos Humanos. Casos*:* "Fernández Ortega y otros vs. México", "Rosendo Cantú y otros vs. México" y "Artavia Murillo y otros vs. Costa Rica".

sentido se pronuncia la corte constitucional italiana en su sentencia 1/1956 al expresar que "el concepto de límite está incluido en el concepto de derecho".[1145]

Asimismo, podemos ver que el mismo criterio se ha adoptado en México a la luz del artículo primero constitucional.[1146] Por lo que, partiendo de la premisa de que ningún derecho es absoluto, es necesario analizar las restricciones que presenta el derecho de acceso a la información. Para ello, es relevante hacer un análisis de derecho comparado, ya que este estudio y declaraciones importantes se han realizado a nivel internacional. En especial, "la Unión Europea es el lugar del mundo con mayor desarrollo en materia de protección de datos personales y de los derechos fundamentales. El tema principal ha sido encontrar el equilibrio que no puede ser dejado solamente a la deontología profesional, a la dinámica mercantil, a los intereses privados o a la idea de que los secretos de Estado deben ser protegidos".[1147]

Para la Unión Europea (UE) "el respeto del derecho a la vida privada en lo que respecta al tratamiento de los datos de carácter personal, reconocido por los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, se aplica a toda información sobre una persona física identificada o identificable. No obstante, de los artículos 8, apartado 2, y 52, apartado 1, de la Carta se desprende que, bajo ciertas condiciones pueden introducirse limitaciones a este derecho".[1148]

El derecho a la vida privada no se puede entender sin abordar el tema de datos personales y la clasificación que se debe realizar para su protección, lo cual ya ha sido analizado por cortes internacionales, mismas que han establecido antecedentes y jurisprudencia al respecto, en casos relevantes como la Directiva 95/46/CE que "constituye el texto de referencia, a escala europea, en materia de protección de datos personales. Crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la UE. Con ese objeto, la Directiva 95/46/CE fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales".[1149]

1995 significó una inflexión, al adoptarse la Directiva 95/46 sobre la protección de las personas físicas en el tratamiento de sus datos. La jurisprudencia del Tribunal de Justicia en la materia, hasta entonces dispersa y casuística, encontró un andamiaje más sólido en el que sustentar sus decisiones, pues la Directiva 95/46/CE delimita de forma detallada el objeto, los sujetos y los posibles remedios del individuo cuando circula información que le incumbe.

1145 Suárez, M. (2011). "La determinación de los límites a los derechos fundamentales en la Constitución Española de 1978". España. *Revista de la Facultad de Ciencias Jurídicas*. Núm. 12/13. 2007/2008, p. 130 Disponible en: http://www.servicios.ulpgc.es/publicaciones/JPortal25/images/revistas/CienciasJuridicas1617/Cap8REVCIENCIASJURIDICAS1617.pdf

1146 Constitución Política de los Estados Unidos Mexicanos. Última reforma publicada en *el Diario Oficial de la Federación* el 24 de febrero de 2017 "Artículo 1. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece [...]".

1147 Piñar, J. (coord). (2014). *Transparencia, derecho a la información y protección de datos*. España. Editorial Reus.

1148 Tribunal de Justicia. (2011). *Asuntos acumulados C-468/10 y C-469/10. Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra Administración del Estado.* Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62010CJ0468_SUM&qid=1461169628202&from=ES página 5/5.

1149 Directiva 95/46/CE del Parlamento Europeo y del Consejo, (24 de octubre de 1995), relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14012

En el décimo considerando de su exposición de motivos se plasma la vocación de la Directiva 95/46 como instrumento para la protección de los derechos fundamentales según se recogen en el CEDH. La sentencia *Österreichischer Rundfunk* confirmó que, aunque la Directiva 95/46 persiga velar por la libre circulación de datos, también presenta una importante vertiente de guardiana de los derechos fundamentales.[1150]

Sin embargo, "ninguno de los textos normativos franceses de naturaleza constitucional hace referencia, en la actualidad, al respeto a la intimidad. Por ello, el Consejo constitucional, a través del artículo 2 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789, lo ha vinculado con el derecho a la libertad y permite de este modo, la intervención del juez administrativo, junto con el juez judicial. Con el fin de proteger los aspectos fundamentales a la protección a la vida privada, se creó la Ley de 6 de agosto de 2004, en la que se ha establecido la prohibición de principio, salvo consentimiento dado por el interesado, pero a condición de que la ley no prohíba dicha excepción: se prohíbe la recogida o el tratamiento de datos de carácter personal que revelen, directa o indirectamente, los orígenes raciales de las personas, o que sean relativos a su salud o a su vida sexual".[1151]

Por otro lado, en el derecho anglosajón se entiende el *right to privicy* conforme a lo que "la jurisprudencia de la Corte Suprema de los Estados Unidos ha interpretado (en general) que lo privado incluye materias concernientes al cuerpo, la familia y las relaciones íntimas y personales del individuo. En este orden de ideas, Anguita Ramírez indica que la noción anglosajona del derecho a la privacidad en la tradición jurídica de la Europa continental (a la que pertenecen los países iberoamericanos) se identifica como derecho a la vida privada o también derecho a la intimidad".[1152]

Por su parte, la Corte Interamericana de Derechos Humanos en el caso "Omar Humberto Maldonado vs. Chile" se pronunció a favor de la protección de la privacidad al determinar que el derecho de acceso a la información bajo el control del Estado admite restricciones, pero que deben estar en la ley y dictadas en atención a un interés general, es decir, que satisfagan un interés público. [1153]

De lo anterior se concluye que tanto el Tribunal Europeo como la CIDH parten del derecho a la libertad de expresión e información para así crear las excepciones que se entienden también en beneficio del interés público y en razón de que deba existir un equilibrio entre ese derecho y el de privacidad. Por ejemplo, la Corte Interamericana, en la sentencia de 19 de septiembre de 2006 en el caso "Claude Reyes y otros vs. Chile", analiza la violación del derecho de acceder a la información bajo el control del Estado en relación con la tortura.

Es decir, el derecho de acceso a la información debe tener límites, al verse posiblemente afectado algún otro derecho humano, aún y cuando sea información que controla el Estado.

1150 *Asunto C553/07 College van burgemeester en* wethouders *van Rotterdam contra M.E.E. Rijkeboer* (2009) Disponible en: https://www.iberley.es/jurisprudencia/sentencia-supranacional-n-c-553-07-tjue-07-05-2009-47538919

1151 Piñar, J. (coord). (2014). *Transparencia, derecho a la información y protección de datos*. España. Editorial Reus, p. 27.

1152 Sanz, F. (2016). "Relación entre protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado", en *Revista Ius et Praxis*, volumen 22, núm. 1. Chile. Universidad de Talca. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122016000100010

1153 Corte Interamericana de Derechos Humanos, caso "Omar Humberto Maldonado vs. Chile", p. 31, numeral 90. "Con respecto a lo anterior, este Tribunal ha indicado en otros casos que el derecho de acceso a la información bajo el control del Estado admite restricciones, las cuales deben estar fijadas por ley, dictada por razones de interés general y con el propósito para el cual han sido establecidas", deben responder a un objetivo permitido por la Convención y ser necesarias en una sociedad democrática, "lo que depende de que estén orientadas a satisfacer un interés público imperativo". Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_300_esp.pdf

Dentro del marco del derecho comparado, la confidencialidad en materia de datos personales y datos personales sensibles debe definirse a partir de lo que se entiende por vida privada e intimidad, en aras de proteger al particular en su esfera íntima, no solo por posibles abusos de la autoridad sino también de particulares.

En la práctica mexicana, la restricción debe operar desde que existe una solicitud de información sobre datos personales, pues actualmente el solicitante no está obligado a motivar su solicitud de información aún en el caso de que se trate de datos personales. Sin embargo, la Comisión Europea —específicamente en el caso *Bavarian Lager*— consideró justificado que el solicitante deba demostrar la necesidad de transmitir los datos personales, pues de no realizar dicha justificación con algún argumento convincente, se impide verificar si no existían motivos para suponer que esa transmisión podría perjudicar los intereses legítimos de los interesados.

La información considerada como confidencial, al ser una excepción al principio de máxima publicidad, contemplado en el artículo 6, fracción I, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM)[1154] tiene como fin proteger no solo los datos personales, sino la vida privada y la intimidad de las personas. Por lo que nos encontramos ante dos derechos fundamentales previstos en los artículos 6 y 16 de la CPEUM, que deben ser equilibrados.[1155]

La definición de información confidencial en la legislación mexicana se encuentra en diversas disposiciones normativas y se define de la misma manera en los distintos ordenamientos.[1156] Los supuestos en los que las leyes consideran que la información es confidencial son los siguientes:

a) cuando contiene datos personales concernientes a una persona identificada o identificable,
b) los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil, y postal, cuya titularidad corresponda a particulares, sujetos de derechos internacional o sujetos obligados cuando no involucren el ejercicio de recursos públicos y
c) aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.

1154 Constitución Política de los Estados Unidos Mexicanos (última reforma publicada en el *Diario Oficial de la Federación* el 24 de febrero de 2017). "Artículo 6 fracción I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y solo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información".

1155 INAI. (2015). *Ley General de Transparencia y Acceso a la Información Pública*. "Artículo 116. Se considera información confidencial la que contiene datos personales concernientes a una persona identificada o identificable.
La información confidencial no estará sujeta a temporalidad alguna y solo podrán tener acceso a ella los titulares de la misma, sus representantes y los Servidores Públicos facultados para ello.
Se considera como información confidencial: los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.
Asimismo, será información confidencial aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales".

1156 Ley General de Transparencia y Acceso a la Información Pública, artículo 116.
Ley Federal de Transparencia y Acceso a la Información Pública, artículo 113.
Lineamientos Generales en materia de clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, capítulo VI.
Ley General de Archivos. Artículo 36.

Una característica importante de la información confidencial es que no está sujeta a ninguna temporalidad. Esto significa que siempre mantendrá su carácter confidencial y solo podrán tener acceso a ella los titulares de la misma, sus representantes y los servidores públicos facultados para ello.

Sin embargo, vale la pena señalar algunas excepciones expuestas en la tesis aislada emitida por tribunales colegiados de circuito en la que se establece:[1157]

> Tratándose de información confidencial, los sujetos obligados solo pueden divulgarla o permitir a terceros acceder a ella si cuentan con el consentimiento de los titulares, o bien, cuando mediante la prueba de interés público, que tiene por objeto distinguir qué información sensible de los gobernados puede ser objeto de divulgación, se corrobore la conexión entre la información confidencial y un tema de interés público, y ponderando el nivel de afectación a la intimidad que pueda.

Es decir, se permite la divulgación de la información pública si existe consentimiento o cuando se haya cumplido con la prueba de interés público.

A continuación se desarrollan los supuestos en los que opera la clasificación de confidencialidad de la información:

A. Datos personales concernientes a una persona identificada o identificable.

La protección de datos personales es información confidencial y debe garantizarse legalmente bajo estrictas condiciones y con un legítimo propósito. Como referencia tenemos el considerando 26 de la Directiva 95/46 en el sentido de aplicación de los principios de protección a cualquier información de una persona identificada o identificable, para lo cual se cita dicho considerando.

> Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento, o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; que los códigos de conducta con arreglo al artículo 27 pueden constituir un elemento útil para proporcionar indicaciones sobre los medios gracias a los cuales los datos pueden hacerse anónimos y conservarse de forma tal que impida identificar al interesado.[1158]

De lo anterior es destacable señalar que los elementos que se consideran para determinar a una persona identificada o identificable, van más allá de sus datos, pues además de eso se entiende que hay que considerar el conjunto de medios que puedan ser razonablemente utilizados por el responsable del tratamiento, es decir, su entorno y terceros.

En la legislación mexicana, es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), publicada en el *Diario Oficial de la Federación* (DOF) el jueves 26 de enero de 2017, la que establece qué son los datos personales y qué se considera dato personal sensible. En el artículo 3, fracciones IX y X[1159] se definen —de

1157 Datos personales. La publicación de los relativos al nombre o denominación de las partes en las listas de los asuntos ventilados ante los ´órganos jurisdiccionales, no precisa, por ende, de la anuencia de aquellas. *Semanario Judicial de la Federación*. Tribunales Colegiados de Circuito. Tesis: I.1o.A.E.229 A (10a.). Décima época. Publicación: viernes 04 de mayo de 2018 10:09 h. Tesis aislada. (Constitucional, administrativa). Registro 2016812.

1158 Directiva 95/46 Protección de Datos personales. (1945). Considerando 26. La confidencialidad y la seguridad del tratamiento. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14012

1159 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017). "Artículo 3, fracción IX. Datos personales: cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

manera enunciativa más no limitativa— los datos que hacen a una persona identificada o identificable y también aquellos datos sensibles que pueden revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.[1160]

En el artículo 6, fracción II de la CPEUM se establece que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijan las leyes. Con lo que esta fracción crea la base constitucional para establecer las excepciones al principio de máxima publicidad.

B. Los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derechos internacional o sujetos obligados cuando no involucren el ejercicio de recursos públicos

La clasificación de información confidencial que se indica en el artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) respecto de los secretos bancario, fiduciario y fiscal presenta una excepción a dicha regla, pues el artículo 117 de dicha ley indica que los sujetos obligados que se constituyan como fideicomitentes, fideicomisarios o fiduciarios en fideicomisos que involucren recursos públicos no podrán clasificar, por ese solo supuesto, la información relativa a su ejercicio como secreto bancario o fiduciario. Asimismo, el artículo 118 de la misma ley indica que los sujetos que se constituyan como usuarios o como institución bancaria en operaciones que involucren recursos públicos tampoco podrán clasificar, por ese solo supuesto, la información relativa al ejercicio de éstos, como es el caso del secreto bancario. Finalmente, el artículo 119 de la ley en cita indica que los sujetos que se constituyan como contribuyentes o como autoridades en materia tributaria tampoco podrán clasificar la información relativa al ejercicio de recursos públicos como secreto fiscal.[1161]

Al respecto fueron emitidos los Lineamientos Generales en Materia de Clasificación y Desclasificación de la Información, así como para la elaboración de versiones públicas, publicados en el *Diario Oficial de la Federación* el 15 de abril de 2016,[1162] mismos que precisan en el numeral cuadragésimo segundo que para la clasificación de información como secreto fiduciario o bancario se deberán acreditar los siguientes elementos: 1) que intervenga una institución de crédito realizando alguna de las operaciones referidas en la Ley de Instituciones de Crédito, 2) que se refiera a datos o información que se obtenga o genere con motivo de la celebración de dichas operaciones, 3) que sea requerida por una persona diversa al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario,

---

X. datos personales sensibles: aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual".

1160 Para mayor referencia, véase la definición de "dato personal" en este diccionario.

1161 Ley General de Transparencia y Acceso a la Información Pública. (2015), artículos 117, 118 y 119.
"Art.117. Los sujetos obligados que se constituyan como fideicomitentes, fideicomisarios o fiduciarios en fideicomisos que involucren recursos públicos, no podrán clasificar, por ese solo supuesto, la información relativa al ejercicio de éstos, como secreto bancario o fiduciario, sin perjuicio de las demás causales de clasificación que prevé la presente Ley.
Artículo 118. Los sujetos obligados que se constituyan como usuarios o como institución bancaria en operaciones que involucren recursos públicos, no podrán clasificar, por ese solo supuesto, la información relativa al ejercicio de éstos, como secreto bancario, sin perjuicio de las demás causales de clasificación que prevé la presente Ley.
Artículo 119. Los sujetos obligados que se constituyan como contribuyentes o como autoridades en materia tributaria, no podrán clasificar la información relativa al ejercicio de recursos públicos como secreto fiscal."

1162 *Lineamientos generales en materia de clasificación y desclasificación de la información*, así como para la elaboración de versiones públicas, publicados en el *Diario Oficial de la Federación* el 15 de abril de 2016. México, numeral cuadragésimo segundo.

comitente o mandante, a los representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio y 4) que refiera a información cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

Sobre este tema es importante mencionar un caso muy conocido resuelto por el otrora Instituto Federal de Acceso a la información y Protección de Datos Personales (IFAI) en el año 2015, en el que instruyó a la Comisión Nacional Bancaria y de Valores (CNBV) a hacer una versión pública de los créditos que los gobiernos estatales tenían contratados con el Grupo Financiero Interacciones, que quiso hacer valer que dicha información era secreto bancario y que no correspondía a ellos ni a la CNBV dar a conocer la información, sino a los gobiernos estatales. Sin embargo, a la luz de lo dispuesto en el artículo 134 constitucional, que dispone que los recursos económicos de que dispongan la Federación, los estados, los municipios, la Ciudad de México y los órganos político-administrativos de sus demarcaciones territoriales se administrarán con eficiencia, eficacia, economía, transparencia y honradez, el IFAI resolvió que era inoperante. Por lo cual, en ese tipo de casos, lo que podría o deberá probarse es alguna de las causales previstas en el artículo 113 de la LGTAIP, es decir, que sean causales de reserva de información que pueda poner en peligro la seguridad nacional o la estabilidad de las instituciones financieras, sin embargo, éstas son causales de reserva y no de información confidencial, como se verá más adelante. Por lo tanto, se considerarán información confidencial: los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

A *contrario sensu*, siempre que se involucren para su ejercicio, recursos públicos con que operen los sujetos obligados por esta ley, no es considerada información confidencial, ni el secreto bancario, fiduciario, industrial, comercial, fiscal, bursátil ni postal. Salvo la excepción de que se ponga en riesgo la seguridad nacional. Por lo que la potestad de las instituciones bancarias de no revelar toda la información sobre sus clientes a las administraciones públicas y la protección que los bancos e instituciones financieras deben otorgar a la información que tienen sobre sus clientes, puede protegerse, pero no mediante la confidencialidad (salvo que encuadre en lo antes expuesto), sino mediante la reserva, realizando versiones públicas de los documentos.

Por lo que hace al secreto industrial o comercial, el otrora IFAI emitió el Criterio 13/2013 en el que se dispone que "el supuesto de información reservada previsto en el artículo 14, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, relativo al secreto industrial o comercial previsto en el artículo 82 de la Ley de la Propiedad Industrial, solamente resulta aplicable a la información que pertenece a los sujetos obligados con motivo del desarrollo de actividades comerciales o industriales; es decir, cuando su titular sea un ente público. Lo anterior, en virtud de que es información de naturaleza gubernamental que refiere al quehacer del Estado, pero su acceso debe negarse temporalmente por una razón de interés público legalmente justificada. Por otro lado, la información propiedad de particulares (personas físicas o morales), entregada a los sujetos obligados, que corresponda a aquella que protege el secreto industrial o comercial, previsto en el citado artículo 82, deberá clasificarse como confidencial con fundamento en el artículo 18, fracción I, en relación con el diverso 19 de la Ley de la materia, a efecto de proteger un interés particular, jurídicamente tutelado y sin sujeción a una temporalidad determinada".

De lo anterior se desprende que el secreto comercial, entendido por ello lo dispuesto en el artículo 82 de la Ley de la Propiedad Industrial, sí puede clasificarse como confidencial cuando el titular sea un ente público, siempre que también se niegue por una razón de interés público.

Es importante señalar que el artículo 3, fracción IX, de la Ley Federal de Competencia Económica[1163] define la información confidencial como: "Aquella que de divulgarse pueda causar un daño o perjuicio en la posición competitiva de quien la haya proporcionado, contenga datos personales cuya difusión requiera su consentimiento, pueda poner en riesgo su seguridad o cuando por disposición legal se prohíba su divulgación".

Por lo que este tipo de información también debe protegerse y ser incluida en los supuestos anteriormente mencionados, así se establece en la tesis de los tribunales colegiados de circuito[1164] al señalar que esta información debe "incluirse en la categoría de información confidencial, aquella exhibida con el informe justificado en el juicio de amparo, distinta de los secretos comerciales, pero que su revelación perjudicaría significativamente a una persona o empresa, en función de las circunstancias específicas de cada caso, como sucedería con la información proporcionada por terceras partes sobre empresas que permitan a éstas ejercer presiones de carácter económico, el riesgo de medidas de represalia comercial sobre sus competidores o sobre sus socios comerciales, clientes o proveedores, o que sirva a las partes para identificar a los denunciantes o a otros terceros cuando éstos deseen, justificadamente, permanecer en el anonimato.

Asimismo, es pertinente mencionar la tesis de los tribunales colegidos de circuito que establece que el derecho al acceso a la información tiene restricciones y una de ellas es la relación con los datos personales, la cual es confidencial y "que merece ser manejada con confidencialidad, como son los secretos (industriales, comerciales, profesional, fiscal, etcétera), considerados como bienes preciados y que también merecen tutela conforme al artículo 16 de la CPEUM, a la par de los datos personales y la vida privada, que igualmente tienen fundamento y protección constitucionales, ostentando este conjunto de información el carácter o cualidad de confidencial. Por tanto, en los casos de tensiones entre los derechos fundamentales que protegen la confidencialidad y el derecho de defensa, debe ponderarse, en cada caso particular, el valor de los intereses en juego y el grado de afectación efectivo o real, para concluir la norma individualizada o regla pertinente, lo que no significa que dejen de observarse los diversos principios constitucionales y legales como la legalidad, igualdad, seguridad jurídica, debido proceso, acceso efectivo a la justicia y cosa —juzgada— o las restricciones que prevé la Norma Fundamental, ya que, de no hacerlo, se provocaría un estado de incertidumbre en los destinatarios de la función judicial".[1165]

En materia fiscal, el artículo 119 de la LGTAIP dispone que no aplica el secreto fiscal para clasificar la información relativa al ejercicio de recursos públicos cuando los sujetos obligados se constituyen como contribuyentes o como autoridades en materia tributaria.

Es importante señalar que el organismo garante tiene la obligación de aplicar la prueba de interés público para el caso de que, por razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros, se requiera la publicación de información confidencial y deberá fundamentar la proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de la información confidencial y el interés público de la información (fracción IV del artículo 120 de la LGTAIP). Es decir, se debe establecer un vínculo entre la divulgación de la información confidencial y el interés público por conocerla.

1163 Publicada en el *Diario Oficial de la Federación* el 27 de enero de 2017.

1164 Información clasificada como confidencial exhibida con el informe justificado. Esa categoría incluye aquella distinta de los secretos comerciales, cuya revelación perjudicaría significativamente a una persona o empresa. *Semanario Judicial de la Federación*. Tribunales Colegiados de Circuito. Tesis: I.1o.A.E.53 K (10a.). Décima época. Registro número: 2011726. Tesis aislada (común). Publicación: viernes 27 de mayo de 2016 10:27 h.

1165 Información clasificada como confidencial en términos de la ley federal de competencia económica, exhibida con el informe justificado. Ponderación que debe realizar el juzgador de amparo para permitir o negar el acceso a ésta. *Semanario Judicial de la Federación*. Tribunales Colegiados de Circuito. Tesis: I.1o.A.E.52 K (10a.) Décima época. Registro número: 2011557. Publicación: viernes 29 de abril de 2016 10:29 h. Tesis aislada. (Constitucional, común).

La información confidencial es el límite a derecho de acceso a la información como lo señala la SCJN.[1166] La información confidencial es, en primera instancia, una excepción al principio de máxima publicidad y se extiende a través de terceros en aras de proteger el derecho a la vida privada, a la intimidad de las personas como es la información concerniente a su familia, sexualidad, salud, historial médico, religión y su imagen pública (lo que es enunciativo más no limitativo). Así como todos aquellos datos que invadan la privacidad de las terceras personas identificadas en los documentos, que pueden llegar a estar protegidos bajo esta excepción.

C) Aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.

Finalmente, es información confidencial aquella que presenten los particulares a los sujetos obligado de conformidad con las leyes y tratados internacionales. Las excepciones y límites deben ir acorde conforme a los tratados internacionales y vale la pena mencionar como ejemplo el principio de la mancomunidad de naciones (*Commonwealth of Nations*) según el cual las excepciones al derecho de acceso deben ser "limitadas" y "formuladas en términos estrechos" y la declaración de principios sobre libertad de expresión de la Comisión Interamericana de Derechos Humanos (en adelante CIDH), declaración que considera que el acceso a la información pública "solo admite limitaciones excepcionales que deben estar establecidas previamente por la ley, para el caso que exista un peligro real e inminente que amenace la seguridad nacional en sociedades democráticas".[1167]

Información pública

Jimena Moreno González

El concepto de información pública ha tenido una evolución constante. Si bien es cierto que la información pública "es aquella que se encuentra en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal o municipal, siempre que se haya obtenido por causa del ejercicio de funciones de derecho público".[1168] También es cierto que se

1166 Información confidencial. Límite al derecho de acceso a la información (Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental). *Semanario Judicial de la Federación y su Gaceta*. Tesis: 1a. VII/2012 (10a.). Décima época. Primera Sala. Registro número 2000233. Tesis aislada (constitucional). Libro V, febrero de 2012. Tomo 1.

1167 Sanz, F. (2016). "Relación entre protección de los datos personales y el derecho de acceso a la información pública en el derecho comparado", en *Revista Ius et praxis.* Chile. Universidad de Talca. Volumen 22. Núm. 1. Disponible en: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122016000100010.

1168 *Semanario Judicial de la Federación y su Gaceta*. Segunda Sala. Novena época. Tomo XXXI 64032. 2a. LXXXVIII/2010I, agosto de 2010, p. 463. Información pública. Es aquella que se encuentra en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, siempre que se haya obtenido por causa del ejercicio de funciones de derecho público. Dentro de un Estado constitucional los representantes están al servicio de la sociedad y no está al servicio de los gobernantes, de donde se sigue la regla general consistente en que los poderes públicos no están autorizados para mantener secretos y reservas frente a los ciudadanos en el ejercicio de las funciones estatales que están llamados a cumplir, salvo las excepciones previstas en la ley, que operan cuando la revelación de datos pueda afectar la intimidad, la privacidad y la seguridad de las personas. En ese tenor, información pública es el conjunto de datos de autoridades o particulares en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, obtenidos por causa del ejercicio de funciones de derecho público, considerando que en este ámbito de actuación rige la obligación de estos de rendir cuentas y transparentar sus acciones frente a la sociedad, en términos del artículo 6o., fracción I, de la Constitución Política de los Estados Unidos Mexicanos, en relación con los numerales 1, 2, 4 y 6 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
Contradicción de tesis 333/2009. Entre las sustentadas por el Tercer Tribunal Colegiado en Materia Administrativa del Primer Circuito y el Décimo Tribunal Colegiado en Materia Administrativa del Primer Circuito. 11 de agosto de 2010. Nota: Esta tesis no constituye jurisprudencia, ya que no resuelve el tema de la contradicción planteada. Disponible en http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/164/164032.pdf

han ampliado los sujetos que producen y ostentan la información por el ejercicio público de sus funciones. En la reforma constitucional publicada en el *Diario Oficial de la Federación* (DOF), el 7 de febrero de 2014, se modificó el artículo 6, inciso A, fracción I, para ampliar a los sujetos obligados y señalar que la obligación de otorgar acceso a la información pública se refiere a "cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal".

El derecho de acceso a la información pública tiene su fundamento en el artículo 6 de la CPEUM y en ella se establecen los principios por los que se rige el derecho de acceso a la información pública. La premisa fundamental de este artículo es que la información en posesión de los sujetos obligados es pública y en caso de interpretación de este derecho se deberá atender el principio de máxima publicidad. También señala la obligación de documentar y resguardar toda la información producto de sus actividades o funciones.

Este mismo artículo garantiza el acceso a la información pública sin tener que acreditar el interés alguno o justificar el uso de la misma. También se crea un órgano constitucional autónomo que será la institución garante del derecho de acceso a la información pública.[1169]

La SCJN en la tesis aislada LXXXV/2016 señaló que el derecho de acceso a la información comprende tres características: i) el derecho a informar, que se hace a través de la difusión de la información de manera proactiva, ii) el derecho de acceso a la información, a través de la búsqueda de la información y iii) el derecho a ser informado.[1170]

1169 Constitución Política de los Estados Unidos Mexicanos. Artículo 6. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm
A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y solo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.
III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

1170 *Gaceta del Semanario Judicial de la Federación*. Tesis: 2a. LXXXV/2016 (10a.). Décima época. Segunda Sala. Libro 34, septiembre de 2016. Tomo I. Tesis aislada (constitucional). Registro 2012525, p. 839.
Derecho a la información. Garantías del.
De conformidad con el texto del artículo 6 constitucional el derecho a la información comprende las siguientes garantías: 1) el derecho de informar (difundir), 2) el derecho de acceso a la información (buscar) y, 3) el derecho a ser informado (recibir). Por un lado, el derecho de informar consiste en la posibilidad de que cualquier persona pueda exteriorizar o difundir, a través de cualquier medio, la información, datos, registros o documentos que posea. En ese sentido, exige que el Estado no restrinja ni limite directa o indirectamente el flujo de la información (obligaciones negativas), y por otro lado, requiere que el Estado fomente las condiciones que propicien un discurso democrático (obligaciones positivas). Por otro lado, el derecho de acceso a la información garantiza que todas las personas puedan solicitar información al Estado respecto de los archivos, registros, datos y documentos públicos, siempre que sea solicitada por escrito, de manera pacífica y respetuosa. Al respecto, exige que el Estado no obstaculice ni impida su búsqueda (obligaciones negativas), y por otro lado, requiere que establezca los medios e instrumentos idóneos a través de los cuales las personas puedan solicitar dicha información (obligaciones positivas). Finalmente, el derecho a ser informado garantiza que todos los miembros de la sociedad reciban libremente información plural y oportuna que les permita ejercer plenamente sus derechos, quedando obligado el Estado a no restringir o limitar la recepción de cualquier información (obligaciones negativas) y por otro lado, también exige que el Estado informe a las personas sobre aquellas cuestiones que puedan

Asimismo, en el artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) señala que "toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal, a que se refiere la Ley General de Transparencia y Acceso a la Información Pública y esta Ley, es pública, accesible a cualquier persona y solo podrá ser clasificada excepcionalmente como reservada de forma temporal por razones de interés público y seguridad nacional o bien, como confidencial. Los particulares tendrán acceso a la misma en los términos que estas leyes señalan".

El derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información. La Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) establece que "toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública".[1171]

También se establecen los principios que deberán aplicar en materia de transparencia y acceso a Información pública. Para efectos de este concepto solo nos referiremos a aquellos que rigen a la información pública.[1172]

Existe la prohibición expresa de la no discriminación en el ejercicio del derecho al acceso a la información. Como lo mandata la CPEUM, la información deberá ser pública, y además deberá estar completa, ser oportuna, gratuita,[1173] accesible, con un lenguaje claro, sencillo y en la medida de lo posible, velará por la traducción a las lenguas indígenas.[1174]

La Ley General de Archivos también hace referencia a que la información contenida en los archivos de los sujetos obligados es pública y el Estado mexicano deberá garantizar su conservación.[1175]

Derivado de lo anterior, es posible sostener que toda la información que produzcan los sujetos obligos es pública y solo se podrá limitar su divulgación de manera excepcional, cuando se trate de información reservada y confidencial de conformidad con lo establecido en la Constitución y en las leyes reglamentarias.

---

incidir en su vida o en el ejercicio de sus derechos, sin que sea necesaria alguna solicitud o requerimiento por parte de los particulares (obligaciones positivas).

1171 Ley General Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 4 de mayo de 2015. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf
Artículo 4. El derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información. Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados es pública y accesible a cualquier persona en los términos y condiciones que se establezcan en la presente Ley, en los tratados internacionales de los que el Estado mexicano sea parte, la Ley Federal, las leyes de las entidades federativas y la normatividad aplicable en sus respectivas competencias; solo podrá ser clasificada excepcionalmente como reservada temporalmente por razones de interés público y seguridad nacional, en los términos dispuestos por esta Ley.

1172 Véase sección segunda de los principios en materia de transparencia y acceso a la información pública de la LGAIP de los artículos 9 al 22.

1173 Artículo 17 de la Ley General de Acceso a la Información Pública Gubernamental. El ejercicio del derecho de acceso a la información es gratuito y solo podrá requerirse el cobro correspondiente a la modalidad de reproducción y entrega solicitada. En ningún caso los ajustes razonables que se realicen para el acceso de la información de solicitantes con discapacidad, será con costo a los mismos

1174 Artículo 13 de la LGAIPG. En la generación, publicación y entrega de información se deberá garantizar que ésta sea accesible, confiable, verificable, veraz, oportuna y atenderá las necesidades del derecho de acceso a la información de toda persona.
Los sujetos obligados buscarán, en todo momento, que la información generada tenga un lenguaje sencillo para cualquier persona y se procurará, en la medida de lo posible, su accesibilidad y traducción a lenguas indígenas.

1175 Artículo 6. Toda la información contenida en los documentos de archivo producidos, obtenidos, adquiridos, transformados o en posesión de los sujetos obligados, será pública y accesible a cualquier persona en los términos y condiciones que establece la legislación en materia de transparencia y acceso a la información pública y de protección de datos personales.
El Estado mexicano deberá garantizar la organización, conservación y preservación de los archivos con el objeto de respetar el derecho a la verdad y el acceso a la información contenida en los archivos, así como fomentar el conocimiento del patrimonio documental de la nación.

El acceso a la información, consagrado como un derecho fundamental, es indispensable en cualquier sociedad democrática y fortalece el estado de derecho ya que ayuda a entender el quehacer de los sujetos obligados y contribuye a transparentar la forma en cómo operan, cómo gastan y que tipo de información producen. Acceder a información pública también contribuye a tener un vínculo jurídico y cercano entre los gobernados y los sujetos obligados, fortalece la transparencia y la rendición de cuentas. La obligación no solo consiste en otorgar información, sino también en orientar al solicitante en el caso en que no sea la autoridad competente. En América Latina, los países que tienen leyes específicas que definen, regulan y garantizan a través de instituciones el acceso a la información pública son Brasil, Chile, México y Uruguay.

El acceso a la información pública también proporciona una herramienta útil para la toma de decisiones, en palabras de López Ayllón y Arellano Gault, (2008) "el acceso a la información pública es sin duda uno de los aspectos críticos del desarrollo democrático. Las sociedades requieren saber qué se hace en sus gobiernos, cómo se toman decisiones, con qué criterios legales, administrativos, formales se llevan a cabo las políticas públicas".[1176]

El acceso a la información pública requiere verse desde dos dimensiones, una individual en la que, como ya se mencionó anteriormente, establece una relación directa del gobernado con las autoridades, ayuda a comprender y dotar de información al ciudadano para el ejercicio de su derecho y una dimensión social que convergen en un pluralismo social y participativo en el que, a través del ejercicio de este derecho y accediendo a la información pública, se privilegie la transparencia y la rendición de cuentas, como lo ha señalado la Suprema Corte de Justicia de la Nación (SCJN) en la tesis segunda, LXXXIV/2016.[1177]

Sin duda el derecho de acceso a la información pública y su tutela a través del órgano garante nacional, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y los órganos garantes estatales son un gran avance en toda sociedad moderna y democrática. Tener instituciones cuya función fundamental es garantizar su ejercicio y tutelar el acceso a la información pública contribuye a fortalecer el estado de derecho, disminuir la corrupción y generar un diálogo directo entre los gobernados y los gobernantes.

1176 López-Ayllón, S. y Arellano, D. (2008). *Estudio en materia de transparencia de otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. México. Banco de Información para la Investigación Aplicada en Ciencias Sociales: Centro de Investigación y Docencia Económicas. p.p. 29. Disponible en: http://datos.cide.edu/bitstream/handle/10089/16074/ESTUDIO.pdf?sequence=1&isAllowed=y

1177 Derecho a la información. Dimensión individual y dimensión colectiva. *Gaceta del Semanario Judicial de la Federación*. Tesis: 2a. LXXXIV/2016 (10a.). Libro 34, septiembre de 2016, Tomo I. Segunda Sala. Tesis Aislada (constitucional. Amparo directo en revisión 2931/2015. p.p. 838.
Derecho a la información. Dimensión individual y dimensión colectiva.
El derecho a la información tiene una doble dimensión. Por un lado, tiene una dimensión individual, la cual protege y garantiza que las personas recolecten, difundan y publiquen información con plena libertad; formando parte indisoluble de la autodeterminación de los individuos, al ser una condición indispensable para la comprensión de su existencia y de su entorno; fomentando la conformación de la personalidad y del libre albedrío para el ejercicio de una voluntad razonada en cualquier tipo de decisiones con trascendencia interna, o bien, externa. Por otro lado, la dimensión colectiva del derecho a la información constituye el pilar esencial sobre el cual se erige todo Estado democrático, así como la condición fundamental para el progreso social e individual. En ese sentido, no solo permite y garantiza la difusión de información e ideas que son recibidas favorablemente o consideradas inofensivas e indiferentes, sino también aquellas que pueden llegar a criticar o perturbar al Estado o a ciertos individuos, fomentando el ejercicio de la tolerancia y permitiendo la creación de un verdadero pluralismo social, en tanto que privilegia la transparencia, la buena gestión pública y el ejercicio de los derechos constitucionales en un sistema participativo, sin las cuales no podrían funcionar las sociedades modernas y democráticas.

Información reservada

Jimena Moreno González

Una vez definida la información confidencial, nos encontramos también con información que debe diferenciarse y reservarse de manera temporal en razón de que su divulgación pudiera afectar el interés público, la seguridad nacional o cualquier otro supuesto establecido en el artículo 113 de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP). Es entonces un modo de darle prevalencia al derecho a la información. Es decir, se reserva dicha información de manera temporal únicamente en los supuestos previstos en la LGTAIP, en contraposición con el interés del solicitante. Para ello, la LGTAIP exige una prueba de daño a los sujetos obligados en la que se demuestre de manera fundada y motivada que divulgar la información requerida pudiera afectar los supuestos del artículo 113.[1178]

Existen excepciones específicas a la reserva de la información enumeradas en el artículo 5 de la LGTAIP que señala: "la información que esté relacionada con violaciones graves a derechos humanos o delitos de lesa humanidad, de conformidad con el derecho nacional o los tratados internacionales de los que el Estado mexicano sea parte no podrá reservarse". Es decir, tratándose de estos supuestos aplica siempre el principio de máxima publicidad.

Para clasificar la información reservada es necesario hacer la prueba de daño, la cual es el documento en el que se motiva y fundamenta la clasificación de reserva. Este documento es trascedente y debe estar debidamente fundado y motivado ya que está sujeto a interpretación y en la interpretación de ese derecho y de la LGTAIP deberá prevalecer el principio de máxima publicidad contenido en la artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en los tratados internacionales, así como en las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, así como las opiniones de los organismos nacionales e internacionales, en materia de transparencia (art. 7 de la LGTAIP).

La información reservada es una excepción al derecho de acceso a la información, los sujetos obligados realizarán un análisis caso por caso de la prueba de daño, tal y como se establece en el artículo 8 de la LGTAIP, de ahí que es importante que las causales sean claras en el ordenamiento jurídico, la prueba de daño esté fundada y motivada pues únicamente funciona como excepción al principio de máxima publicidad.

1178 Ley General de Transparencia y Acceso a la Información Pública. (2015). Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación: I. comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable; II. pueda menoscabar la conducción de las negociaciones y relaciones internacionales; III. se entregue al Estado mexicano expresamente con ese carácter o el de confidencial por otro u otros sujetos de derecho internacional, excepto cuando se trate de violaciones graves de derechos humanos o delitos de lesa humanidad de conformidad con el derecho internacional; IV. pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal; V. pueda poner en riesgo la vida, seguridad o salud de una persona física; VI. obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones; VII. obstruya la prevención o persecución de los delitos; VIII. la que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada; IX. obstruya los procedimientos para fincar responsabilidad a los servidores públicos, en tanto no se haya dictado la resolución administrativa; X. afecte los derechos del debido proceso; XI. vulnere la conducción de los Expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado; XII. se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el ministerio público, y XIII. las que por disposición expresa de una ley tengan tal carácter, siempre que sean acordes con las bases, principios y disposiciones establecidos en esta Ley y no la contravengan; así como las previstas en tratados internacionales.

Asimismo, es importante mencionar que para clasificar información como reservada se debe atender a las causales que expresamente se señalan en las fracciones del artículo 113 de la LGTAIP. Entre ellas, algunas de las más relevantes son: que se comprometa la seguridad nacional, seguridad pública o la defensa nacional, que pueda afectar las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país, entre otras.[1179]

Al invocar alguna de esas causales, se deberá realizar la mencionada prueba de daño, para demostrar de manera fundada y motivada que la información se reservará por las razones consideradas y mediante el fundamento correcto, así como con la aprobación del comité de transparencia y por una temporalidad máxima de cinco años pudiendo renovarse por un periodo de cinco años más, siempre y cuando se demuestre que existen las causales.

Infracción

Gabriel López López

Las infracciones son hechos o conductas exteriores cometidas por el sujeto infractor y contrarias a los dispositivos legales en la materia que los rija. Dichas conductas pueden consistir en acciones u omisiones. Las acciones implican la comisión de una conducta sancionable por una norma, mientras que las omisiones representan el incumplimiento de una obligación impuesta en la normatividad.

La palabra "infracción" proviene del latín *infractionis* o *infractio* que significa rotura o abatimiento interior que culmina con el quebrantamiento total de una norma.[1180]

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) establece, en su artículo 63,[1181] las diversas hipótesis normativas que se consideran infraccio-

1179 Ley General de Transparencia y Acceso a la Información Pública (2015). Artículo 113. Como información reservada podrá clasificarse aquella cuya publicación:
"I. Comprometa la seguridad nacional, la seguridad pública o la defensa nacional y cuente con un propósito genuino y un efecto demostrable;
II. Pueda menoscabar la conducción de las negociaciones y relaciones internacionales;
III. Se entregue al Estado mexicano expresamente con ese carácter o el de confidencial por otro u otros sujetos de derecho internacional, excepto cuando se trate de violaciones graves de derechos humanos o delitos de lesa humanidad de conformidad con el derecho internacional;
IV. Pueda afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal;
V. Pueda poner en riesgo la vida, seguridad o salud de una persona física;
VI. Obstruya las actividades de verificación, inspección y auditoría relativas al cumplimiento de las leyes o afecte la recaudación de contribuciones;
VII. Obstruya la prevención o persecución de los delitos;
VIII. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada;
IX. Obstruya los procedimientos para fincar responsabilidad a los servidores públicos, en tanto no se haya dictado la resolución administrativa;
X. Afecte los derechos del debido proceso;
XI. Vulnere la conducción de los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio, en tanto no hayan causado estado;
XII. Se encuentre contenida dentro de las investigaciones de hechos que la ley señale como delitos y se tramiten ante el Ministerio Público, y
XIII. Las que por disposición expresa de una ley tengan tal carácter, siempre que sean acordes con las bases, principios y disposiciones establecidos en esta Ley y no la contravengan; así como las previstas en tratados internacionales".

1180 González, C., *et al.* (2004). *Etimologías griegas.* México. Mc Graw Hill-UADY, p. 49.

1181 Artículo 63. Constituyen infracciones a esta Ley las siguientes conductas llevadas a cabo por el responsable:
I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos

nes al tenor de las conductas y umbrales establecidos en el diverso artículo 64 de la misma Ley, y que pueden ser cometidas por los particulares, personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales.

Concatenando el contenido de los artículos a que se ha hecho referencia, para efectos de la LFPDPPP, se considerará infractor a aquella persona física o moral de carácter privado que lleve a cabo el tratamiento de datos personales y que cometa alguna de las conductas siguientes:

a) No cumpla con la solicitud del titular para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición (ARCO) respecto del tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la LFPDPPP.
b) Actúe con negligencia o dolo en la tramitación y respuesta de solicitudes ARCO.
c) Declare dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en sus bases de datos.
d) De tratamiento a los datos personales en contravención a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.
e) Omita en su aviso de privacidad la identidad y domicilio del responsable que los recaba; las finalidades del tratamiento de datos; las opciones y medios que el responsable ofrezca para limitar el uso o divulgación de los datos; los medios para ejercer los derechos ARCO; las transferencias de datos que se efectúen; el procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad; y en el caso de datos personales sensibles, el señalamiento expreso de que se trata de este tipo de datos.
f) Mantengas datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.
g) No cumpla con el apercibimiento que le sea formulado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) para que lleve a cabo los actos solicitados por el titular, respecto de con la solicitud del titular para el ejercicio de sus derechos ARCO, sin razón fundada.

---

personales, sin razón fundada, en los términos previstos en esta Ley.
II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales.
III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable.
IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley.
V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley.
VI. Mantener datos personales inexactos cuando resulten imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.
VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64.
VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley.
IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12.
X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.
XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.
XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley.
XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.
XIV. Obstruir los actos de verificación de la autoridad.
XV. Recabar datos en forma engañosa y fraudulenta.
XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares.
XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.
XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley.
XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

h) Incumpla el deber de confidencialidad en cualquier fase del tratamiento de datos personales, inclusive aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

i) Cambie sustancialmente la finalidad originaria del tratamiento de los datos, sin obtener el consentimiento del titular.

j) Transfiera datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.

k) Vulnere la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.

l) Lleve a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la LFPDPPP.

m) Recabe o transfiera datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.

n) Obstruya los actos de verificación de la autoridad.

o) Recabe datos en forma engañosa y fraudulenta.

p) Continúe con el uso ilegítimo de los datos personales cuando se hubiese solicitado el cese del mismo por el INAI o los titulares.

q) Trate los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO.

r) Cree bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

s) Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la LFPDPPP.

Por su parte, el artículo 163 de la Ley General de Datos Personales en Posesión de Sujetos Obligados (LGDPPSO) previene que se consideran conductas sancionables:

a) Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO.

b) Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate.

c) Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales que se encuentren bajo su custodia o a los cuales tengan acceso o conocimientso con motivo de su empleo, cargo o comisión.

d) Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGDPPSO.

e) No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos exigidos por la LGDPPSO.

f) Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción solo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales.

g) Incumplir el deber de confidencialidad.

h) No establecer las medidas de seguridad en los términos establecidos en la LGDPPSO.
i) Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.
j) Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la LGDPPSO.
k) Obstruir los actos de verificación de la autoridad.
l) Crear bases de datos personales en contravención a lo dispuesto por la LGDPPSO.
m) No acatar las resoluciones emitidas por el Instituto y los organismos garantes.
n) Omitir la entrega del informe anual y demás informes exigidos por la LGTAIP o entregar los mismos de manera extemporánea.

Adicionalmente, para efectos de la cuantificación de las sanciones dentro de los umbrales a que se refiere el artículo 64[1182] de la LFPDPPP, el INAI deberá considerar, respecto del infractor, según lo ordenan tanto el artículo 65 de la misma Ley, como el cuarto párrafo del artículo 73 de los Lineamientos de los Procedimientos de Protección de Derechos de Investigación y Verificación y de Imposición de Sanciones (Lineamientos de Procedimiento), los siguientes elementos:

1. la notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos establecidos en la LFPDPPP,
2. el carácter intencional o no, de la acción u omisión constitutiva de la infracción,
3. la capacidad económica del infractor, y
4. la reincidencia.

La obligación descrita tiene su génesis en el artículo 16, párrafo primero, de la CPEUM que impone como garantía a favor del gobernado el que todo acto de autoridad se funde y motive, a fin de que pueda conocer con precisión los motivos y razones legales que se tomaron en cuenta para emitirlo.

1. Delimitación conceptual y conceptos relacionados

Para Rafael de Pina y Rafael de Pina Vara, la infracción constituye un acto realizado contra lo dispuesto en una norma legal o incumpliendo un compromiso contraído.[1183]

Tanto el derecho penal como el derecho administrativo sancionador resultan ser dos inequívocas manifestaciones de la potestad punitiva del Estado o *ius puniendi*, entendida como la facultad que tiene éste de imponer penas y medidas de seguridad ante la comisión de actos considerados como ilícitos en una norma.

El derecho administrativo sancionador tiene como propósito fundamental garantizar a la sociedad el desarrollo correcto y normal de las funciones reguladas en las leyes adminis-

1182 Artículo 64. Las infracciones a la presente Ley serán sancionadas por el Instituto con:
I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior.
II. Multa de 100 a 160 mil días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior.
III. Multa de 200 a 320 mil días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior.
IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320 mil días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

1183 De Pina, Rafael y De Pina Vara, Rafael, (1998). *Diccionario de Derecho*. 25a. ed. México. Porrúa, p. 320.

trativas, utilizando su potestad suprema para lograr los objetivos en ellas especificados, cuestión en la que además se encuentra inmerso el interés colectivo.

Así, el llamado derecho administrativo sancionador consiste en la competencia de las autoridades administrativas para imponer sanciones a las acciones y omisiones calificadas como antijurídicas por un ordenamiento normativo, es decir, las infracciones. De este modo, la pena administrativa es una función jurídica que tiene lugar como reacción frente a la infracción, ante la lesión del derecho administrativo.

El criterio extensivo sobre interpretación y traslación de los principios constitucionales que rigen en materia penal al derecho administrativo sancionador ha sido analizado en ciertos casos por la SCJN, considerando que los mismos constituyen una limitante del ejercicio del *ius puniendi* del Estado, con base en el cual, la CPEUM impide que los poderes Ejecutivo y Judicial configuren libremente delitos y penas o bien, infracciones y sanciones, es decir, el principio constitucional de legalidad exige que todo acto de los órganos del Estado debe encontrarse fundado y motivado y ser expedido conforme a las leyes establecidas con anterioridad al hecho que se sanciona.

De la acción de inconstitucionalidad 4/2006, promovida por el procurador General de la República, el Tribunal Pleno de la SCJN aprobó, el 15 de agosto de 2006, la Tesis de Jurisprudencia P./J. 99/2006 de la que se advierte que nuestro máximo tribunal consideró que tanto el derecho penal como el derecho administrativo sancionador resultan ser dos inequívocas manifestaciones de la potestad punitiva del Estado, entendida como la facultad que tiene éste de imponer penas y medidas de seguridad ante la comisión de ilícitos, por lo que dada la similitud y la unidad de la potestad punitiva, en la interpretación constitucional de los principios del derecho administrativo sancionador puede acudirse a los principios penales sustantivos, aun cuando la traslación de los mismos en cuanto a grados de exigencia no pueda hacerse de forma automática, porque la aplicación de dichas garantías al procedimiento administrativo solo es posible en la medida en que resulten compatibles con su naturaleza.[1184]

No existiendo duda alguna en que el principio constitucional de legalidad que rige en materia penal, previsto en el artículo 14 de la CPEUM, puede ser aplicado *mutatis mutandis* al derecho administrativo sancionador, resulta importante destacar que el mismo constituye un importante límite externo al ejercicio del *ius puniendi* del Estado, con base en el cual la CPEUM impide que los poderes Ejecutivo y Judicial —este último a través de la analogía y mayoría de razón— configuren libremente delitos y penas o bien, infracciones y sanciones; es decir, el mencionado principio exige que todo acto de los órganos del Estado debe encontrarse fundado y motivado conforme a las leyes establecidas con anterioridad al hecho que se sanciona.

El referido principio constitucional posee intrínsecamente dos principios: el de reserva de ley y el de tipicidad.

a) El principio de reserva de ley

Se traduce en que determinadas materias o ciertos desarrollos jurídicos deben estar respaldados por la ley o simplemente que la ley sea el único instrumento idóneo para regular su funcionamiento.

Dicho de otro modo, el principio de reserva de ley tiene como propósito impedir que los reglamentos y ordenamientos secundarios que el Ejecutivo federal expida, invadan la es-

1184 Tesis P./J. 99/2006. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo. XXIV, agosto de 2006, p. 1565.

fera de una ley formal y materialmente legislativa cuya expedición se encuentra atribuida al Congreso de la Unión.

b) El principio de tipicidad

Se manifiesta como una exigencia de predeterminación normativa clara y precisa de las conductas ilícitas y de las sanciones correspondientes. Dicho en otras palabras, el referido principio se cumple cuando consta en la norma una predeterminación inteligible tanto de la infracción como de la sanción, lo que supone en todo caso la presencia de una *lex certa* que permita predecir con suficiente grado de seguridad las conductas infractoras y las sanciones.

La descripción legislativa de las conductas ilícitas debe gozar de tal claridad y univocidad que el juzgador pueda conocer su alcance y significado al realizar el proceso mental de adecuación típica, sin necesidad de recurrir a complementaciones legales que superen la interpretación y que lo llevarían al terreno de la creación legal para suplir las imprecisiones de la norma.

Así, para garantizar debidamente la seguridad jurídica de los gobernados, no bastaría con una tipificación confusa o indeterminada que los condujera a tener que realizar labores de interpretación para las que no todos están preparados, y de esa manera tratar de conocer lo que les está permitido y lo que les está prohibido hacer. Es por ello esencial que toda formulación típica que sea lo suficientemente clara y precisa como para permitirles programar su comportamiento sin temor a verse sorprendidos por sanciones que en modo alguno pudieron prever.

En este orden de ideas, el principio de tipicidad, normalmente referido a la materia penal, también se hace extensivo a las infracciones y sanciones administrativas, como en la especie lo es la relativa a la protección de datos personales, de modo tal que si alguna disposición administrativa establece una multa por la comisión de alguna conducta atípica considerada infracción, ésta debe encuadrar exactamente en la hipótesis normativa previamente establecida, sin que resulte lícito ampliar ésta ni por analogía ni por mayoría de razón.

Aunado a ello, para respetar esta necesidad de certeza y seguridad jurídicas, el juzgador, en cumplimiento del principio de exacta aplicación de la ley, no tiene más que asegurarse de conocer el alcance y significado de la norma al realizar el proceso mental de adecuación típica y de la correlación entre sus elementos, sin que pueda rebasarse la interpretación y se incurra en una eventual creación normativa para superar las posibles deficiencias de la norma.

Dada esta convergencia de los principios de tipicidad y exacta aplicación de la ley en el principio de legalidad, la SCJN ha inferido de la interpretación de la norma constitucional, que la garantía de exacta aplicación de la ley no se circunscribe a los meros actos de aplicación, sino que abarca también a la propia ley que se aplica, la que debe quedar redactada de tal forma que los términos en los cuales especifique los elementos respectivos sean claros, precisos y exactos, esto es, el legislador no puede sustraerse al deber de consignar en las leyes penales que expida, expresiones y conceptos claros, precisos y exactos al prever las penas y describir las conductas antijurídicas, incluyendo todas sus características, elementos, condiciones, términos y plazos cuando ello sea necesario a fin de evitar confusiones en su aplicación o demérito en la defensa del gobernado, tal como al efecto se advierte de la tesis P. IX/95.[1185]

Conforme a lo expuesto, resta señalar que el principio de tipicidad, como consecuencia del principio de legalidad recogido en el artículo 14 de la CPEUM, implica que los caracteres esenciales de la conducta atípica y la forma, contenido y alcance de la infracción estén

1185 Tesis P. IX/95. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo I, mayo de 1995, p. 82.

consignados de manera clara y expresa en la ley, de tal forma que no quede margen para la arbitrariedad de las autoridades encargadas de su aplicación, ni tampoco de aquellos que juzguen su imposición.

Consecuentemente, en materia de protección de datos personales, respecto de aquellas conductas a que se refiere el artículo 63, de la LFPDPPP, resulta invariable que el INAI se encuentra obligado a observar los referidos principios, máxime cuando los mismos derivan del principio de legalidad a que se ha hecho referencia.

Infractor

Gabriel López López

Aquella persona física o moral[1186] que deliberada o involuntariamente vulnera o contraviene una norma, disposición o precepto establecido dentro de la legislación aplicable y que es de observancia obligatoria para los gobernados, por lo que su incumplimiento puede actualizar la comisión de una conducta tipificada como infracción, misma que a su vez puede dar lugar a la imposición de una sanción de carácter económico o no económico.

La palabra "infractor" deriva de *infracción* que proviene del latín *infractionis* o *infractio* que significa rotura o abatimiento interior que culmina con el quebrantamiento total de una norma.[1187]

La Real Academia Española (RAE) define el concepto de infractor como el que quiebra o el que rompe.[1188]

En materia de protección de datos personales, la fracción X, del artículo 3, de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación y de Imposición de Sanciones (Lineamientos de Procedimiento), expedidos por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), y publicados en el *Diario Oficial de la Federación* (DOF) el 9 de diciembre de 2015, definen el concepto "infractor" como la persona física o moral de carácter privado que da tratamiento a los datos personales, en contravención a las disposiciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).[1189]

1. Delimitación conceptual y conceptos relacionados

En el ámbito del ejercicio de facultades en cuanto al derecho administrativo sancionador se refiere, la autoridad encargada de garantizar el derecho a la protección de datos perso-

1186 Por lo que se refiere a los sujetos regulados por la LFPDPPP, su artículo 2 establece que son sujetos regulados por dicha Ley los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, exceptuando de ser sujetos regulados por dicha Ley, a las personas siguientes:
a) a las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
b) a las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

1187 González, C. *et al.* (2004). *Etimologías griegas.* México. Mc Graw Hill-UADY, p. 49.

1188 RAE. (2001). *Diccionario de la lengua española.* 22a. ed.

1189 Los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones señalan:
Artículo 3.- Además de las definiciones establecidas en los artículos 3º de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 2º de su Reglamento, para los efectos de los presentes Lineamientos se entenderá por:
[...]
X. Infractor: persona física o moral de carácter privado que da tratamiento a los datos personales, en contravención a las disposiciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
[...]

nales, así como de vigilar y sancionar la infracción a la normatividad aplicable en materia de protección de datos personales es el INAI. Por lo tanto, su objetivo principal como órgano autónomo es verificar el cumplimiento de las obligaciones, principios y deberes establecidos la ley por parte de los sujetos, personas físicas o morales que lleven a cabo el tratamiento de datos personales.

La LFPDPPP establece, en su artículo 63,[1190] las diversas hipótesis normativas que se consideran conductas sancionables al tenor de los umbrales establecidos en el diverso artículo 64 de la misma Ley, y que pueden ser cometidas por los particulares, personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales.

De los artículos referidos, se desprende que para efectos de la LFPDPPP se considerará como infractor a aquella persona física o moral de carácter privado que lleven a cabo el tratamiento de datos personales y que, cometa alguna de las conductas siguientes:

a) No cumpla con la solicitud del titular para el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición (ARCO) respecto del tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la LFPDPPP.
b) Actúe con negligencia o dolo en la tramitación y respuesta de solicitudes ARCO.
c) Declare dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en sus bases de datos.
d) De tratamiento a los datos personales en contravención a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.
e) Omita en su aviso de privacidad, la identidad y domicilio del responsable que los recaba; las finalidades del tratamiento de datos; las opciones y medios que el responsable ofrezca para limitar el uso o divulgación de los datos; los medios para ejercer los derechos ARCO; las transferencias de datos que se efectúen; el procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de

1190 Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:
I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;
II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;
III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;
IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;
V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;
VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;
VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;
VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;
IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;
X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;
XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;
XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;
XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;
XIV. Obstruir los actos de verificación de la autoridad;
XV. Recabar datos en forma engañosa y fraudulenta;
XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;
XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;
XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y
XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

privacidad; y en el caso de datos personales sensibles, el señalamiento expreso de que se trata de este tipo de datos.

f) Mantenga datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares.

g) No cumpla con el apercibimiento que le sea formulado por el INAI para que lleve a cabo los actos solicitados por el titular, respecto de con la solicitud del titular para el ejercicio de sus derechos ARCO, sin razón fundada.

h) Incumpla el deber de confidencialidad en cualquier fase del tratamiento de datos personales, inclusive aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

i) Cambie sustancialmente la finalidad originaria del tratamiento de los datos, sin obtener el consentimiento del titular.

j) Transfiera datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.

k) Vulnere la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable.

l) Lleve a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la LFPDPPP.

m) Recabe o transfiera datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible.

n) Obstruya los actos de verificación de la autoridad.

o) Recabe datos en forma engañosa y fraudulenta.

p) Continúe con el uso ilegítimo de los datos personales cuando se hubiese solicitado el cese del mismo por el INAI o los titulares.

q) Trate los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO.

r) Cree bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

s) Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la LFPDPPP.

Finalmente, cabe señalar que para efectos de la imposición y cuantificación de las sanciones a que se refieren los dispositivos referidos, la LFPDPPP considera, en su artículo 65, elementos atribuibles al sujeto responsable tales como la negativa de éste a realizar los actos solicitados por el titular, la intencionalidad en la comisión de la conducta, su capacidad económica y la reincidencia.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Sergio López Ayllón

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es el organismo garante en el ámbito federal responsable de promover, vigilar y garantizar el cumplimiento del derecho de acceso a la información pública y la protección de datos personales en los términos que establezcan las leyes aplicables en la materia, en particular la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), la Ley General de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

1. Delimitación conceptual y conceptos correlacionados

El INAI es el órgano que, en el ámbito federal, tiene como función garantizar el ejercicio de los derechos de acceso a la información y protección de datos personales en posesión de los sujetos obligados, es decir, cualquier ente que ejerza recursos públicos o que realice algún acto de autoridad en el ámbito federal.[1191] Junto con lo anterior, en materia de datos personales en posesión de los particulares, actúa como el órgano regulador en la materia y ejerce funciones administrativas cuasi jurisdiccionales frente a los particulares.

Conforme lo establecido en el artículo 6 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), el INAI se integra de manera colegiada por siete comisionados. De acuerdo con lo establecido en este artículo, corresponde a la Cámara de Senadores nombrar a los comisionados, a propuesta de los grupos parlamentarios, con el voto de las dos terceras partes de los miembros presentes, previa realización de una amplia consulta a la sociedad.[1192] Para esto, los senadores deberán emitir una convocatoria, con el objeto de realizar una amplia consulta pública nacional dirigida a toda la sociedad, para que presenten sus postulaciones de aspirantes a ocupar el cargo.[1193]

Por su parte, el artículo 20 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) establece que el Senado de la República deberá acordar el procedimiento que se debe llevar a cabo, los plazos y los pormenores del proceso de selección. Entre los mecanismos más relevantes para garantizar la publicidad del proceso y que tienen que decidirse por el senado se encuentran: 1) hacer pública la lista de las y los aspirantes a comisionado; 2) hacer públicos los documentos que hayan sido entregados para su inscripción en versiones públicas y 3) respecto al dictamen que se presente al Pleno a propuesta de los grupos parlamentarios, deberá hacerse público al menos un día antes de su votación.

Como autoridad especializada en materia de derechos humanos, la actuación del INAI se rige también por lo previsto en el artículo 1 de la CPEUM, es decir, tiene la obligación de promover, respetar, proteger y garantizar los derechos humanos reconocidos en la CPEUM y en los tratados internacionales en los que México es parte, favoreciendo en todo tiempo la protección más amplia a las personas.[1194]

1191 Artículo 3.- Además de las definiciones establecidas en los artículos 3º de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 2º de su Reglamento

1192 Artículo 33 de la Ley Federal de Transparencia y Acceso a la Información Pública.

1193 Artículo 19 de la Ley Federal de Transparencia y Acceso a la Información Pública.

1194 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Como autoridad del Estado, está obligado a promover, respetar, proteger y garantizar los derechos humanos, al interpretar el orden jurídico

Junto con lo anterior y, de conformidad con lo establecido en el artículo 6 de la CPEUM y como los otros organismos garantes, la actuación del INAI está sujeta a los principios de autonomía, especialización, imparcialidad, certeza, legalidad, independencia, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad. La explicación de estos principios se encuentra en la voz "organismos garantes" de este mismo diccionario.

Lo anterior es congruente con los Estándares Iberoamericanos de Protección de Datos Personales (Estándares Iberoamericanos), según los cuales las autoridades de control y supervisión en esta materia (como lo es el INAI) tienen que actuar con plena autonomía, imparcialidad e independencia en sus potestades, así como ajenas a toda influencia externa, ya sea directa o indirecta, por lo que no solicitarán ni admitirán orden ni instrucción alguna.[1195]

En materia de transparencia, acceso a la información y protección de datos en posesión de sujetos obligados, el INAI es el órgano competente en el ámbito federal y ejerce sus atribuciones frente a cualquier autoridad, entidad, órgano y organismos de los poderes Ejecutivo, Legislativo y Judicial, organismos con autonomía constitucional, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad.[1196]

Además de las facultades genéricas que le otorga la LGTAIP a los órganos garantes, el INAI tiene, en el ámbito federal, las siguientes competencias específicas: 1) interpretar, administrar, sancionar y aplicar la ley en la materia; 2) conocer de recursos de revisión interpuestos por particulares en contra de resoluciones de los sujetos obligados en el ámbito federal y en contra de las resoluciones emitidas por los organismos garantes de las entidades federativas; 3) conocer y resolver los recursos de revisión que por su interés o trascendencia así lo ameriten y, por último, 4) interponer acciones de inconstitucionalidad y controversias constitucionales. Además de lo anterior, el INAI es el encargado de encabezar y coordinar el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) y tiene la facultad de interponer acciones de inconstitucionalidad y controversias constitucionales. Además, es el responsable de evaluar de manera general la situación del acceso a la información pública en el país y de entregar al Senado un informe al sobre sus actividades y la evaluación general en materia de acceso a la información pública en el país.[1197]

El INAI tiene otro conjunto de atribuciones específicas en materia de protección de datos en posesión de sujetos obligados, entre las que destacan: 1) garantizar el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados; 2) conocer de recursos de revisión en esta materia en los mismos términos previstos en la LGTAIP; 3) garantizar condiciones de accesibilidad, lo que incluye coordinarse con las autoridades competentes para que las solicitudes para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) y los recursos de revisión que se presenten en lengua indígena, sean atendidos en la misma lengua; 4) definir y desarrollar el sistema de certificación en materia de protección de datos personales de conformidad con los parámetros de la LGPDPPSO; 5) llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales y sus prerrogativas, 6) emi-

de su competencia, favoreciendo en todo tiempo a las personas la protección más amplia. Décima época. Registro: 2015433. Instancia: Tribunales Colegiados de Circuito. Tesis aislada.

1195 Estándares Iberoamericanos de Protección de Datos Personales, capítulo VII. Autoridades de control. Artículos 42.1 y 42.2.

1196 Artículo 23, Ley General de Transparencia y Acceso a la Información.

1197 Artículo 41, Ley General de Transparencia y Acceso a la Información.

tir lineamientos para homologar el ejercicio de los derechos ARCO, 7) emitir criterios generales de interpretación para garantizar el derecho a la protección de datos personales y 8) diseñar, vigilar y, en su caso, operar el sistema de buenas prácticas en materia de protección de datos personales, así como el sistema de certificación en la materia.[1198]

En materia de datos personales en posesión de particulares, las funciones del INAI se modifican, pues en este caso actúa propiamente como un órgano regulador y se constituye como una autoridad frente a los particulares. Respecto a sus facultades en materia de protección de datos personales en posesión de los particulares, el INAI tiene como objeto difundir el conocimiento de este derecho, promover su ejercicio y vigilar su debida observancia. Además, entre otras cosas, tiene que 1) interpretar, vigilar y verificar el cumplimiento de la LFPDPPP; 2) propiciar apoyo técnico a los responsables; 3) emitir y divulgar tanto criterios como recomendaciones, estándares y buenas prácticas en materia de datos personales; 4) elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes; 5) cooperar con otras autoridades y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos y 6) conocer y resolver los procedimientos de protección de derechos y de verificación, así como imponer las sanciones que corresponda.[1199]

Respecto a su funcionamiento interno, el INAI tendrá personal que preste sus servicios de acuerdo con lo dispuesto en los artículos 6 y 132, apartado B de la CPEUM.[1200] Estos trabajadores se regirán por las bases del servicio profesional de carrera del mismo Instituto.

Integridad de la información

Christian Paredes González

La integridad se define, según el *Diccionario de la Real Academia de la Lengua* (DRAE) como la "cualidad de íntegro". Respecto a qué se considera íntegro, el mismo diccionario señala que hace referencia a algo que no carece de ninguna de sus partes.

Por otra parte, las Recomendaciones en materia de Seguridad de Datos Personales para el sector privado (Recomendaciones de Seguridad),[1201] la *Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales,* publicada en 2015[1202] (GISGSDP), y las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales[1203] definen "integridad" en idénticos términos y señalan que es la "propiedad de la información para salvaguardar la exactitud y completitud de la información".

La integridad supone que la información se mantenga inalterada ante accidentes o intentos maliciosos de forma que solo pueda ser modificad por personal debidamente autorizado. Es decir, se trata de la propiedad de la información que busca preservar los datos libres de modificaciones no autorizadas de modo que se conserve con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

1198 Artículo 89, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1199 Artículo 38, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

1200 Artículo 23, Ley Federal de Transparencia y Acceso a la Información Pública.

1201 Publicadas el 30 de octubre de 2013 en el *Diario Oficial de la Federación*.

1202 INAI. (2015). *Guía para implementar un sistema de gestión de seguridad de datos personales.* Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

1203 INAI. (2018). *Recomendaciones para el manejo de incidentes de seguridad de datos personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf

Así, la integridad garantiza que los datos permanezcan inalterados, excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.

Inteligencia artificial

Eric Huesca Morales

Resulta sorprendente la variedad de definiciones existentes respecto del concepto de inteligencia artificial (IA). El término fue utilizado por primera vez por el científico John McCarthy en 1955[1204] al explicar la capacidad de un programa de computadora para procesar datos y transformarlos en ideas, comportamientos y decisiones independientes de la intervención humana.

De las definiciones que hoy en día son más utilizadas para definir el concepto de IA podemos citar las siguientes:

- "La ciencia de hacer que las máquinas realicen cosas que requerirían del uso de inteligencia si fuesen realizadas por el hombre", (Marvin Minsky).
- "Para que pueda afirmarse que un sistema exhibe inteligencia artificial debe ser capaz de aprender de alguna manera y tomar acciones con base en dicho aprendizaje. Estas acciones se materializan en nuevos comportamientos o nuevas funcionalidades consecuencia de dicho aprendizaje", (Omar Abdelwahed).
- "La inteligencia artificial debe, de manera general, entenderse como una rama de las ciencias computacionales enfocada en diseñar sistemas que utilicen algoritmos, inspiradas en el conocimiento del cerebro humano, y capaces de realizar tareas que, si fuesen realizadas por el hombre, requerirían del uso de inteligencia" (*Future of Privacy Forum*).

Los sistemas informáticos con IA suelen crearse para enfrentar retos relacionados con: habilidades cognitivas, solución de problemas y reconocimiento de patrones.

Los expertos suelen decir que para que un sistema informático exhiba IA, deberá ser capaz de:

a) reconocer el ambiente en el que está;
b) analizar y adaptar la información que reciba y
c) responder mediante la actualización de sus propios procesos, idealmente, para lograr mejores resultados o predicciones.

La IA se divide en dos categorías: general y específica.

De acuerdo con el Foro del Futuro de la Privacidad, la IA general equivale a un sistema que es funcionalmente igual (o superior a) a la inteligencia humana, y describe la noción de máquinas que pueden exhibir toda la gama de capacidades cognitivas humanas. La capacidad de generalizar el conocimiento o las habilidades, tomar el valor experiencial de un campo y aplicarlo en un contexto diferente, es hasta ahora un logro estrictamente humano.

Por su parte, señalan que la IA específica es aquella que se aplica únicamente a una tarea particular. La principal diferencia entre la IA específica y la general es que la específica se limita a interactuar en campos reducidos del conocimiento y a la probable resolución de problemas preidentificados.

1204 McCarthy, J. et al. (1955). *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*.

Una vez visto el alcance del concepto de IA, resulta conveniente analizar el impacto que tiene el uso de esta tecnología en el derecho de protección de datos personales de las personas.

Sin lugar a duda, el uso avanzado de algoritmos o de técnicas para la recolección masiva de datos (*big data*) constituye, junto a la inversión económica, el incentivo de la IA para un desarrollo más amplio y constante para influir y tener así interacciones directas en la vida de las personas. Lo anterior, como adelantábamos, tiene un profundo impacto en el derecho de protección de datos personales de las personas.

El tratamiento de datos personales a través de *big data,* con o sin técnicas de IA, contiene particularidades que pueden no resultar compatibles con los principios y deberes rectores de las normatividades de protección de datos personales. Un claro ejemplo de lo anterior es el siguiente: las normatividades de protección de datos personales, como la mexicana, tiene al principio de información como unos de sus principios rectores del tratamiento, lo cual conlleva, explicado de manera general, que el responsable del tratamiento informe al titular de los datos personales, entre otras cosas, los fines para los cuales serán tratados sus datos personales. Ahora bien, no puede obviarse que, en tratamientos de *big data*, cumplir con el mencionado principio de información puede llegar a resultar imposible, puesto que una de las características del *big data* es que resulta impredecible, ya que, en la mayor parte de las veces, no se tiene certeza para qué fines puede llegarse a utilizar la información, o bien qué tipo de información nueva se puede llegar a generar. Entonces, si no es posible cumplir con el principio de información, tampoco podría cumplirse con el principio de consentimiento, ya que la propia legislación mexicana de protección de datos personales prevé que para cumplir con el principio de consentimiento es necesario que éste, entre otras cosas, sea informado, lo cual sucede cuando el titular conoce, previo al tratamiento, los datos personales que serán sujetos al tratamiento y los fines para los cuales serán tratados.

Como consecuencia de las mencionadas dificultades que en materia de protección de datos personales pueden presentarse como parte del uso de IA en conjunto con técnicas de *big data* para la aplicación de sistemas informáticos se ha vuelto indispensable que las empresas centren su atención en las siguientes tres cuestiones:

1) Transparencia: las empresas deben ser transparentes en cuanto a los algoritmos que utilizan.
2) Equidad: las empresas deben asegurarse de que las decisiones algorítmicas no creen impactos discriminatorios o injustos.
3) Responsabilidad proactiva: las decisiones basadas en información algorítmica tienen el potencial de un impacto social significativo y deben diseñarse e implementarse de manera pública y responsable, como la obligación de informar, explicar y justificar decisiones específicas, así como mitigar los impactos negativos y los daños potenciales.

Interés legítimo

Isabel Davara Fernández de Marcos,[1205]
Gregorio Barco Vega y
Alexis Cervantes Padilla

La expresión "interés legítimo" hace referencia a uno de los fundamentos jurídicos a partir de los cuales se puede legitimar el tratamiento de los datos personales de forma que éste sea lícito y leal conforme lo exige la normatividad de protección de datos personales aplicable.

El concepto de interés legítimo fue introducido por el artículo 7 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, el 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE), que ahora ha quedado superada por el Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés), la cual disponía que un tratamiento de datos personales sería considerado lícito si se encontraba sustentado en cualquiera de las siguientes bases jurídicas del tratamiento:

a) el consentimiento del interesado (titular en términos de la normatividad mexicana);
b) fuese necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado;
c) fuese necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento;
d) fuese necesario para proteger el interés vital del interesado;
e) fuese necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o
f) fuese necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la Directiva 95/46/CE.

Así, puede apreciarse que la figura de interés legítimo, introducida en la Directiva 95/46/CE, representaba una base jurídica o base de legitimación para permitir el tratamiento de los datos derivado de la necesidad de dar satisfacción a un interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros[1206] a los que se les comunicasen datos, con la condición de que no prevalecieran los intereses o los derechos y libertades fundamentales del titular de los datos personales. Derivado de esta condición, para que pudiera ser aplicable la figura de interés legítimo, la Directiva 95/46/CE exigía al responsable sujetar el tratamiento a una prueba de sopesamiento para ponderar el interés legítimo del responsable del tratamiento o del tercero o terceros a los que se comunicaran los

1205 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

1206 La LFPDPPP prevé una figura que se asemeja a la de interés legítimo en su artículo 37, fracción VI, el cual establece que el responsable podrá transferir datos personales de un titular cuando sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, pudiendo pertenecer dicho derecho a un tercero ajeno a las partes intervinientes en el tratamiento.

datos, en relación con los intereses o los derechos fundamentales de los interesados.[1207]

Por su parte, el RGPD, de forma similar y retomando lo dispuesto en la Directiva 95/46/CE, en su artículo 6 referente a la licitud del tratamiento, da cabida al concepto del interés legítimo al señalar que una de las bases de legitimación de cualquier tratamiento puede ser: "la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño […]".

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) retoman el citado concepto y las bases jurídicas de legitimación del tratamiento previstas en el RGPD al establecer en su artículo 11 previsiones específicas sobre lo que se ha denominado "principio de legitimación".

Así, los Estándares Iberoamericanos prevén que un responsable del tratamiento podrá llevar a cabo un tratamiento cuando éste "…sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del titular que requiera la protección de datos personales, en particular cuando el titular sea niño, niña o adolescente. Lo anterior, no resultará aplicable a los tratamientos de datos personales realizados por las autoridades públicas en el ejercicio de sus funciones […]".

No cabe duda que la figura de interés legítimo resulta imprescindible al momento de legitimar tratamientos referentes al entorno laboral, *big data*, inteligencia artificial, aprendizaje de *marketing*, investigaciones en materia de seguridad, salud, etc., ya que los mencionados tratamientos presentan muchas dificultades cuando se tienen que legitimar en otros supuestos como en el consentimiento del titular.

Una vez identificados los principales antecedentes y previsiones normativas que regulan la figura del interés jurídico, a continuación, pasamos a explicar en qué consiste dicha figura.

1207 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p.5

1. El concepto "interés"

En primer lugar, debe destacarse que el concepto "interés" está estrechamente relacionado con el concepto "finalidad"[1208] que está regulado en las normatividades de datos personales,[1209] aunque se trata de conceptos diferentes. En este sentido, se entiende por finalidad del tratamiento, el propósito, motivo o razón por el cual se tratan los datos personales. Es decir, el objetivo o la intención del tratamiento de los datos. Un "interés" en cambio, se refiere a una mayor implicación que el responsable del tratamiento pueda tener en el tratamiento o al beneficio que el responsable del tratamiento obtenga o que la sociedad pueda obtener del tratamiento.[1210]

2. El adjetivo "legítimo"

El interés debe estar articulado con la claridad suficiente para permitir que se realice una prueba de sopesamiento en contraposición a los intereses y los derechos fundamentales del interesado. De forma adicional, también se ha señalado que el interés en juego debe también ser "perseguido por el responsable del tratamiento".[1211] Es decir, se debe tratar de un interés real y actual, que se corresponda con actividades presentes o beneficios que se esperen en un futuro muy próximo. Sobre esta base explicativa, los intereses que sean demasiado vagos o especulativos no serán suficientes para sustentar el tratamiento de los datos personales.[1212]

El Grupo de Trabajo del Artículo 29 (GTA29 o WP29 por sus siglas en inglés) ha manifestado que la naturaleza del interés puede variar. Para el GTA29, algunos intereses pueden ser apremiantes y beneficiosos para la sociedad en general, tales como el interés de la prensa en publicar información sobre la corrupción gubernamental o el interés en llevar a cabo investigación científica (sujetos a las garantías adecuadas). Mientras que otros intereses pueden ser menos apremiantes para la sociedad en su conjunto o, en cualquier caso, el impacto de su búsqueda en la sociedad puede ser más dispar o controvertido. El GTA29 señala que esto puede, por ejemplo, aplicarse al interés económico de una empresa en aprender tanto como sea posible sobre sus potenciales clientes con el fin de orientar mejor la publicidad sobre sus productos y servicios.[1213]

Con base en lo anterior, el referido órgano consultivo ha precisado que el interés legítimo podría comprender una amplia gama de intereses, tanto triviales como muy apremiantes, tanto claros como controvertidos y proporciona una lista, no exhaustiva, de supuestos que podrían constituir un interés legítimo:

- El ejercicio del derecho a la libertad de expresión o información, que incluyen las situaciones en las que se ejerza dicho derecho en los medios de comunicación y en las artes.
- La prospección convencional y otras formas de comercialización o publicidad;
- Los mensajes no comerciales que no hayan sido solicitados, incluidos los pertenecientes a campañas políticas o de recaudación de fondos para organizaciones caritativas.

1208 Se recomienda consultar la definición de "principio de finalidad" en este *Diccionario de Protección de Datos Personales.*

1209 Por ejemplo, en el apartado 1 del artículo 5 del Reglamento General de Protección de Datos.

1210 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 29.

1211 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 50.

1212 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 50.

1213 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 51.

- La ejecución de derechos reconocidos en procedimientos judiciales, incluido el cobro de deudas mediante procedimientos extrajudiciales.
- La prevención del fraude, el uso indebido de servicios o el blanqueo de dinero.
- La supervisión de los empleados con fines de seguridad o de gestión.
- Los regímenes internos de denuncia de irregularidades.
- La seguridad física, la tecnología de la información y la seguridad en la red.
- El tratamiento con fines históricos, científicos o estadísticos.
- El tratamiento con fines de investigación (incluida la investigación de mercado).

Consecuentemente, el GTA29 declara que se puede considerar que un interés es legítimo siempre que el responsable del tratamiento pueda perseguir dicho interés de conformidad con las leyes relativas a la protección de datos y con el resto de la legislación (licitud del tratamiento).[1214]

Resumiendo, para que un interés resulte legítimo en términos de las disposiciones del actual régimen jurídico, debe ser lícito, estar articulado con la claridad suficiente para permitir que la prueba de sopesamiento se lleve a cabo en contraposición a los intereses y los derechos fundamentales del titular (es decir, suficientemente específico) y rrepresentar un interés real y actual (es decir, no especulativo).[1215]

Tal como se explicará a continuación, si el interés perseguido por el responsable del tratamiento no es apremiante, es más probable que el interés y los derechos del interesado prevalezcan sobre el interés legítimo —pero menos importante— del responsable del tratamiento. Del mismo modo, esto no significa que un interés menos apremiante del responsable del tratamiento no pueda prevalecer a veces sobre los intereses y derechos de los interesados: esto sucede normalmente cuando el impacto del tratamiento sobre los interesados es también menos importante.

En lo que respecta al concepto de "interés del afectado", éste tiene un alcance mucho más amplio de forma tal que no requiere ser legítimo. En palabras del GTA29, esto quiere decir que, si el responsable del tratamiento o la tercera parte pueden perseguir cualquier interés, siempre que no sea ilegítimo, el interesado a su vez tendrá derecho a que se tengan en cuenta todas las categorías de intereses que le afecten y a que se ponderen en relación con los intereses del responsable del tratamiento o la tercera parte, en tanto estén comprendidos en la normatividad aplicable.[1216]

Finalmente, en lo que toca a la denominada prueba de sopesamiento sobre el interés legítimo, el grupo consultivo antes citado destaca que es importante considerar, en primer lugar, la naturaleza y la fuente del interés legítimo, y si el tratamiento es necesario para perseguir dicho interés y las repercusiones para los interesados.[1217] Esto es, no puede considerarse al interés legítimo como una base de legitimación sencilla o *soft law* para el responsable, ya que debe pasar pruebas anteriores y en su caso ser capaz de demostrar posteriormente la viabilidad de su interés y la no afección a derechos de terceros.

1214 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 30.

1215 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 39.

1216 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 58.

1217 Grupo de Trabajo del Artículo 29. Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014, p. 59.

Interés público

Jimena Moreno González

Para abordar el tema de interés público, primero me referiré a la definición contenida en el *Diccionario Jurídico Mexicano* del Instituto de Investigaciones Jurídicas de la UNAM, el cual señala que el interés público es "el conjunto de pretensiones relacionadas con las necesidades colectivas de los miembros de una colectividad y protegidas mediante la intervención directa y permanente del Estado".[1218] Esta definición tiene dos elementos importantes que vale la pena destacar: i) se refiere a las necesidades de una colectividad y ii) éstas deben estar protegidas por el Estado. El Estado tiene la obligación de proteger a una colectividad determinada.

Estos elementos generales y abstractos generan incertidumbre respecto a su interpretación y aplicación. Como lo señala Carla Huerta (Huerta, 2007:134):

> El concepto de interés público, que actúa como justificante de determinadas acciones del Estado […] El interés público es un concepto abstracto cuya aplicación a casos concretos ha de determinarse y transformarse en decisiones jurídicas. La precisa definición del interés público o general se constituye en garantía de los intereses individuales y colectivos simultáneamente, y se concreta en normas protectoras de bienes jurídicos diversos que imponen límites a la actuación pública y privada.[1219]

Derivado de lo anterior, podemos señalar que una de las características esenciales del denominado interés público es la protección del Estado a determinadas necesidades de una comunidad, que tienen trascendencia y sirven para fines que van por encima de un interés particular o de un grupo de intereses específicos. "Aunque puede ser de interés público ayudar a cierto tipo de personas, no se debe confundir el interés particular de uno de esos grupos con el interés público mismo y cuando no esté en juego el interés de todos esos grupos protegidos, sino el de uno solo de ellos […]",[1220] así lo estableció el Primer Tribunal Colegiado en Materia Administrativa.

El artículo 3 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP)[1221] establece lo siguiente:

> Toda la información generada, obtenida, adquirida, transformada o en posesión de los sujetos obligados en el ámbito federal, a que se refiere la Ley General de Transparencia y Acceso a la Información Pública y esta Ley, es pública, accesible a cualquier persona y solo podrá ser clasificada excepcionalmente como reservada de forma temporal por razones de interés público y seguridad nacional o bien, como confidencial. Los particulares tendrán acceso a la misma en los términos que estas leyes señalan.

En este sentido, las razones de interés púbico juegan como una excepción al principio de máxima publicidad de la información debido a que se puede reservar de forma temporal aludiendo a este principio.

1218 Instituto de Investigaciones Jurídicas UNAM. (1984). *Diccionario jurídico mexicano*. México. Universidad Nacional Autónoma de México. Tomo IV, p. 167. En Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas. Disponible en: https://biblio.juridicas.unam.mx/bjv

1219 Huerta, C. (2007). "El Concepto de interés público y su función en materia de seguridad nacional", en seguridad pública. Segundo Congreso Iberoamericano de Derecho Administrativo, Fernández Ruiz, et al., coord. Instituto de Investigaciones Jurídicas. México. UNAM, p. 134.

1220 Suspensión interés social o interés público. Su demostración. Tribunales Colegiados de Circuito. Séptima época. Apéndicen1917 septiembre 2011. Tomo II. Procesal constitucional 1. Común segunda parte. TCCC. Novena sección. Suspensión del acto reclamado. Subsección 1. Reglas Generales, p. 2598.

1221 Publicada en el *Diario Oficial de la Feder*ación el 27 de enero de 2017. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

La Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)[1222] en el artículo 3, fracción XII, define la información de interés público y señala que ésta "se refiere a la información que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los sujetos obligados". Esta definición deja claro que el interés público está por encima del interés individual en relación a las actividades que deben llevar a cabo los sujetos obligados. Asimismo, los sujetos obligados deben difundir proactivamente información que se consideren de interés público.

La Suprema Corte de Justicia de la Nación (SCJN) en el amparo directo 3/2011 ha establecido que "el criterio de interés público debe fundarse en la información que el público considera relevante para la vida comunitaria, es decir, aquella que versa sobre hechos que puedan encerrar trascendencia pública y que sean necesarios para que sea real la participación de los ciudadanos en la vida colectiva".[1223]

Uno de los límites naturales al interés público es el derecho a la protección a la vida privada y a la protección de los datos personales. Sin embargo, estos derechos no son absolutos y podrían divulgarse en caso en que se considere que tienen una relevancia pública para la sociedad. "La relevancia pública dependerá, en todo caso, de situaciones históricas, políticas, económicas y sociales, que ante su variabilidad, se actualizará en cada caso concreto".[1224]

En materia fiscal tenemos que el artículo 69 del Código Fiscal de la Federación (CFF) protege los datos personales de los contribuyentes en posesión de las autoridades fiscales. Sin embargo, como se señaló en el párrafo anterior y como lo indica el artículo 6, fracción II de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) esta protección no es absoluta al señalar que "la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes".

En este mismo sentido, la SCJN en la tesis: 1a. CVII/2013 (10a.)[1225] en principio estableció la obligación de las autoridades tributarias de no revelar ningún tipo de información fiscal de los contribuyentes, posteriormente establece que este principio no es absoluto

1222 Publicada en el *Diario Oficial de la Federación* el 4 de mayo de 2015 y disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5391143&fecha=04/05/2015

1223 Libertad de expresión. La difusión de información sobre la vida privada de las personas puede ampararse por este derecho si se justifica su interés público. Décima época. Registro: 2003636. Instancia: Primera Sala. Tipo de tesis: aislada. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Libro XX, mayo de 2013. Tomo 1. Materia(s): constitucional. Tesis: 1a. CXXXII/2013 (10a.), p. 553.

1224 Derecho a la intimidad o vida privada. Noción de interés público, como concepto legitimador de las intromisiones sobre aquél. Novena época. Registro: 165051. Instancia: primera sala. Tipo de tesis: aislada. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo XXXI, marzo de 2010. Materia(s): constitucional. Tesis: 1a. XLII/2010, p. 923.

1225 Tesis: 1a. CVII/2013 (10a.), *Semanario Judicial de la Federación y su Gaceta.* Libro XIX, abril de 2013. Tomo 1, p. 970 de rubro y texto siguiente:
"Secreto fiscal. Concepto de. El artículo 69 del Código Fiscal de la Federación establece la obligación de reserva absoluta en lo concerniente a la información tributaria del contribuyente (declaraciones y datos suministrados por los contribuyentes o por terceros con ellos relacionados, así como los obtenidos en el ejercicio de las facultades de comprobación), a cargo del personal de la autoridad fiscal que intervenga en los trámites relativos a la aplicación de disposiciones fiscales. Así, en principio, dicha medida legislativa establece una concreta carga —de no hacer— impuesta al personal —servidores públicos— de la autoridad fiscal, consistente en que al aplicar las disposiciones fiscales no deben revelar de ninguna forma información tributaria de los contribuyentes. En esto precisamente, desde la perspectiva del derecho positivo, consiste el secreto fiscal". Por ende, la intervención legislativa por la cual se estableció el secreto fiscal no se encuentra diseñada normativamente como un principio o derecho fundamental, sino más bien como una regla-fin en los términos señalados. Pero la reserva del secreto fiscal no es absoluta, tal y como lo dispone el mismo artículo 69 con independencia de que en principio así se encuentre establecido textualmente, sino relativa al establecer dicho precepto distintas excepciones al respecto.

por lo que está a sujeto la excepción de poder divulgar información de los contribuyentes en caso de interés público.

En este caso, la excepción la establece el CFF, y la información se podrá dar a conocer cuando exista interés público mediante una prueba de interés público en la que se ponderarán los intereses en juego. Es decir, se deberá ponderar el interés público que se promovería con la divulgación de los datos personales y el interés público en mantener la privacidad de esa información. Es importante señalar que el interés público subsiste cuando hacer pública determinada información contribuye a la evaluación de la actuación de las autoridades con el objetivo de favorecer i) la transparencia en el ejercicio de sus funciones, ii) el manejo de recursos, iii) la rendición de cuentas y iv) la buena administración de los recursos públicos.

Una materia de amplio debate en la sociedad es el relativo a la colisión de diversos derechos, uno ejemplo clásico de ello es cuando por un lado se debe promover y garantizar la libertad de expresión y por el otro, se debe proteger el derecho a la intimidad, el derecho a la vida privada y el derecho a la protección de los datos personales.

La Primera SCJN se pronunció en el sentido en que el interés público es la justificación más importante cuando se trate de divulgar información íntima, en el caso en el que entren en conflicto estos derechos en el ejercicio legítimo del derecho a la libertad de información.[1226]

En la Ley General de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) se hace referencia a la información pública en el artículo 76, fracción IV al señalar que el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (SNT) podrá emitir criterios adicionales cuando la relevancia de datos personales tenga un impacto en el interés público. Asimismo, el artículo 130, fracción V, establece que el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) podrá ejercer su facultad de atracción en materia de protección de datos personales cuando la relevancia en el tratamiento de datos personales tenga un impacto en el interés público.[1227]

1226 Libertad de expresión. El interés público constituye una causa de justificación para difundir información privada.
Décima época. Registro: 2003628. Instancia: primera sala. Tipo de tesis: aislada. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Libro XX, mayo de 2013. Tomo 1. Materia(s): constitucional. Tesis: 1a. CLV/2013 (10a.), p. 549.
Libertad de expresión. El interés público constituye una causa de justificación para difundir información privada.
Sostener que la divulgación de cualquier información veraz está amparada por la libertad de expresión equivaldría a hacer nugatorio el derecho a la intimidad, toda vez que en la medida en la que los hechos en cuestión fueran verdaderos los medios de comunicación estarían en libertad de publicarlos. En este sentido, el interés público es la causa de justificación más relevante en los casos donde entran en conflicto libertad de información y derecho a la intimidad. Así, la identificación de un interés público en la difusión de información íntima actualizará una causa de justificación al estar en presencia del ejercicio legítimo de la libertad de información.

1227 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.
Artículo 76. El Sistema Nacional podrá emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales, de conformidad con lo dispuesto en el artículo anterior, en función de: …
IV. La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue.
Artículo 130. Para efectos de la presente Ley, el Pleno del Instituto, cuando así lo apruebe la mayoría de sus Comisionados, de oficio o a petición fundada de los organismos garantes, podrá ejercer la facultad de atracción para conocer de aquellos recursos de revisión pendientes de resolución en materia de protección de datos personales, que por su interés y trascendencia así lo ameriten y cuya competencia original corresponde a los organismos garantes, conforme a lo dispuesto en esta Ley y demás normativa aplicable.
Los recurrentes podrán hacer del conocimiento del Instituto la existencia de recursos de revisión que de oficio podría conocer. Por lo que hace a los lineamientos y criterios generales de observancia obligatoria que el Instituto deberá emitir para determinar los recursos de revisión de interés y trascendencia que está obligado a conocer, conforme a la Ley General

Finalmente, hemos visto como el concepto de interés público es amplio, abstracto y establece límites y restricciones a ciertos derechos en beneficio de una colectividad o comunidad. También hemos observado que tratándose de la vida privada y la protección de datos personales se requiere una prueba de interés público que ponga en valoración los distintos derechos que entran en conflicto.

Cabe señalar que: "El valor protegido es la vida privada o el patrimonio de las personas. Esta protección suele ser más amplia e impone una restricción absoluta a la divulgación de los documentos que contienen esta información. Sin embargo, pueden existir circunstancias excepcionales en que el interés público justifique su divulgación. Estas circunstancias excepcionales suponen una difícil y compleja valoración de los intereses en juego".[1228]

Internet de las cosas

Erik Huesca Morales

El término "internet de las cosas" (IoT por sus siglas en inglés) y también conocido como internet de los objetos se emplea para referirse a un conjunto bastante amplio de actividades en las que diversos objetos se conectan a internet para propósitos muy variados.

El IoT es la integración de objetos[1229] o "cosas"[1230] a la red de redes y que en estricto sentido no son computadoras. Estos objetos se conectan, por lo general, sin intervención humana y permiten la comunicación entre dispositivos intercambiando datos sobre alguna acción específica de las personas o de interés sobre el comportamiento de otros objetos.

Así, el término IoT ha sido descrito de muy diversas formas, como una red, como un paradigma, como un concepto, como una aplicación de internet y como una infraestructura de red global, por mencionar tan solo algunos ejemplos.

En cuanto a los componentes de la expresión IoT podemos destacar que, la palabra "objeto" (*things* en inglés) hace referencia a un objeto del mundo físico (objetos físicos) o del mundo de la información (objetos virtuales) que se puede identificar e integrar en las redes de comunicaciones. En la práctica, la palabra citada ha sido sustituida por diversos términos alternativos, dando lugar a diferentes variantes del IoT, como *internet of everything, internet of anything, internet of people* o *internet of signs*, entre otros ejemplos.

En el contexto del internet de los objetos, se entiende por dispositivo a una pieza de equipo con capacidad obligada de comunicación con otros dispositivos o computadoras utilizando una red pública o privada y con capacidad opcional de detección, adquisición, almacenamiento y procesamiento de datos.

En el internet de los objetos, resulta que no todos los dispositivos se conectan a internet ni usan el protocolo TCP/IP, sino pueden usar otras formas de comunicación como es

---

de Transparencia y Acceso a la Información Pública, adicionalmente en la atracción de recursos de revisión en materia de protección de datos personales se deberán considerar los siguientes factores: …
V. La relevancia del tratamiento de datos personales, en atención al impacto social o económico del mismo y del interés público para promover del recurso de revisión atraído.

1228 López, S. y Posadas, A. (2006). *Las pruebas de daño e interés público en materia de acceso a la información. Una perspectiva comparada*. México. Documentos de Trabajo del Centro de Investigación y Docencia Económicas. Núm. 18, p. 2.

1229 Objeto: En el contexto de IoT se trata de un objeto del mundo físico (objetos físicos) o del mundo de la información (objetos virtuales) que se puede identificar e integrar a las redes de comunicaciones de forma estática y dinámica. (Recomendación UIT.T Y.2060)

1230 Por la influencia de la palabra en inglés *things* que se traduce como cosa, pero que en un término más amplio en el español debería ser denotado como objeto.

bluetooth o protocolos propietarios del fabricante. Lo importante es que no son objetos o dispositivos conectados de forma aislada, sino siempre están integrados a una red, ya sea de área local o amplia y de uso privado o público. Sin embargo, si se toma como conexión primaria la denominada red de internet,[1231]el internet de los objetos o de las cosas que en sus siglas en inglés se conoce como IoT puede requerir de un despliegue masivo de direcciones válidas de IP para lograr una correcta identificación y funcionamiento de objetos físicos como: robots, automotores, sensores, activadores, electrodomésticos u objetos virtuales como contenidos multimedios y de *software* de aplicaciones que tradicionalmente no estaban conectados a la red y que hoy recaban datos de cualquier interacción, misma que contribuye cada día a que internet sea una red más compleja para la administración y operación de la misma.

Respecto a la producción de datos y su privacidad con el internet de los objetos, la problemática de privacidad puede potenciarse al no tener especificado claramente la forma que los dispositivos conectados comparten, almacenan y procesan los datos personales que capturan para su operación

Los datos recabados pueden permanecer en el dispositivo o almacenarse en repositorios de datos cuya ubicación geográfica no siempre corresponde a su espacio de operación y sí al diseño y uso para el que fue ideado. Por lo tanto, los objetos que interactúan de forma autónoma pueden intercambiar datos sin que el usuario conozca de su utilización.

Antes de abordar las definiciones de organizaciones como la Unión Internacional de Telecomunicaciones (ITU) o el Instituto de Ingenieros Eléctricos y en Electrónica (IEEE), se debe comentar que de forma reciente se asocia el concepto con otros, que si bien se encuentran relacionados, no son causa uno del otro, tal es el caso de la inteligencia artificial, *big data* (grandes volúmenes de datos), revolución 4.0 y *Blockchain* por mencionar algunos de los desarrollos de las ciencias de la computación que hoy están en su fase comercial.

El grupo de estudios 13 de la UIT-T llegó a un consenso sobre la definición de IoT en los siguientes términos, en el año 2012:

> Internet de los objetos (IoT): infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras.

En el reporte especial sobre internet de los objetos, que se llevó a cabo en 2014, la IEEE[1232] describe IoT como una red de objetos —cada uno embebido con sensores— los cuales se conectan a internet. La IEEE incorpora la capa de sensores a la definición:[1233]

> En términos generales, para la IEEE la IoT abarca muchas áreas que van desde tecnologías de apoyo y componentes de varios mecanismos para integrar de manera efectiva estos componentes de menor nivel. El *software* es entonces un factor discriminante para los sistemas de IoT. Los sistemas operativos IoT estén diseñados para funcionar con componentes de pequeña escala de la manera más eficiente posible, mientras que al mismo tiempo proporcionan funcionalidades básicas para simplificar y apoyar el sistema mundial de la IDO en sus objetivos y propósitos.

1231 Es la conexión entre computadoras utilizando el protocolo TCP/IP.

1232 El Instituto de Ingenieros Eléctricos y en Electrónica (IEEE) es la organización profesional más grande del mundo y define los estándares de muchos dispositivos. Existe un grupo de interés especial en definir los estándares de comunicación del internet de los objetos.

1233 IEEE Internet Initiative (2015, 13 de mayo). *Towards a definition of the Internet of Things (IoT)*. Issue 1. Disponible en: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf Fecha de consulta: agosto del 2018.

Middleware, capacidad de programación —en términos de interfaces de programación de aplicaciones (API)— y de gestión de datos parecen ser factores esenciales para crear un sistema de éxito en el ámbito de la IDO. Se necesitan capacidades de gestión con el fin de manejar adecuadamente los sistemas que potencialmente pueden crecer hasta millones de diferentes componentes. En este contexto, la autogestión y la auto-optimización de cada componente individual y / o el subsistema requisitos tal vez fuertes. En otras palabras, comportamientos autónomos podrían llegar a ser la norma en los sistemas grandes y complejos de la IDO. La seguridad de datos y privacidad jugarán un papel importante en las implementaciones de la IoT.

La Comisión Europea, al abordar el tema del IoT, ha destacado que esta tecnología "permite a los objetos compartir información con otros objetos/miembros en la red, reconociendo eventos y cambios que permitan reaccionar autónomamente en una forma adecuada. El IoT por tanto se construye sobre una comunicación entre cosas (máquinas, construcciones, coches, animales, etcétera) que guía a la acción y al valor de creación".[1234]

Por su parte, el Grupo de Trabajo del Artículo 29 señala que el IoT se refiere a una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos ("objetos" como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos y, al estar asociados a identificadores únicos, interactúan con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red.[1235]

Finalmente, la OCDE, en un reporte de mayo de 2016, definió al IoT como "un ecosistema en el cual las aplicaciones y servicios se conducen por medio de datos obtenidos de los dispositivos que perciben una interfaz con el mundo físico".[1236]

A pesar de que el IoT es una realidad compleja en el entorno tecnológico actual, tiene características bien definidas que la distinguen de otro tipo de tecnologías y sistemas. Siguiendo la recomendación UIT-T Y.2060, podemos resaltar las siguientes características del IoT:

a) Interconectividad: en el contexto de IoT, todo puede estar interconectado con la infraestructura mundial de la información y la comunicación.
b) Servicios relacionados con objetos: IoT es capaz de suministrar servicios relacionados con los objetos dentro de las restricciones de objetos, como protección de la privacidad y coherencia semántica entre los objetos físicos y sus correspondientes objetos virtuales.
c) Heterogeneidad: los dispositivos en IoT son heterogéneos dado que se basan en diferentes plataformas, *hardwares* y redes.
d) Cambios dinámicos: el estado de los dispositivos varía dinámicamente, por ejemplo, del modo reposo al activo, conectado y/o desconectado, así como el contexto del dispositivo, como la ubicación y velocidad.
e) Escala enorme: el número de dispositivos que ha de gestionarse y que se comunican entre sí puede ser incluso un orden de magnitud mayor que el número de dispositivos conectados actualmente a internet.

Derivado de sus características y funcionalidades, el IoT entraña importantes desafíos, uno de ellos es la garantía de los derechos de privacidad y protección de datos personales

1234 Comisión Europea. (2014). *Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination* , p. 18.

1235 Grupo de Trabajo del Artículo 29. Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, adoptado el 16 de septiembre de 2014. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_es.pdf

1236 OCDE. (2016). *The internet of things: seizing the benefits and addressing the challenges*, p. 9. Disponible en: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2015)3/FINAL&docLanguage=En

de los titulares cuando el IoT implica un tratamiento de datos personales, caso en el que deberán de observarse las disposiciones de la LFPDPPP y su Reglamento.

Por lo anterior, se ha insistido en que tecnologías como el IoT demandan un enfoque nuevo donde se busque algo más que el cumplimiento literal de la Ley y se encuentren opciones que se complementen con los esquemas actuales y que logren una ulterior protección a los derechos de las personas.

Intervención de las comunicaciones

José Soto Galindo

La intervención de comunicaciones privadas es un acto de investigación o diligencia de investigación sobre la comisión de un delito y de su autoría mediante la interceptación de las comunicaciones de sospechosos o imputados producidas con cualquier sistema de comunicación análogo o digital, como el correo o telégrafo, el teléfono alámbrico y móvil o las comunicaciones a través de internet. La intervención de comunicaciones privadas puede abarcar desde el contenido y el proceso de comunicación hasta los datos que identifican la comunicación y la localización geográfica del aparato tecnológico utilizado para el acto comunicativo (véase, geolocalización).

El dispositivo jurídico que mejor describe el alcance de la intervención de comunicaciones privadas se encuentra en el artículo 291 del Código Nacional de Procedimientos Penales: "La intervención de comunicaciones privadas abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real". La Ley Federal contra la Delincuencia Organizada contiene una descripción similar en el segundo párrafo del artículo 16.

La intervención de comunicaciones privadas debe considerarse una medida de carácter excepcional, pues constituye una injerencia a los derechos a la vida privada y a la protección de datos personales o, como ha dicho la Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN), a lo "que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás." Su práctica debe sujetarse al principio de legalidad y garantizar un estricto cumplimiento al marco constitucional y legal aplicable. Está expresamente prohibida cuando se investiguen asuntos en materia electoral, fiscal, mercantil, civil, laboral o administrativa y en el caso de las comunicaciones entre una persona detenida y su defensor.

1. La intervención de comunicaciones en la práctica

La intervención de comunicaciones privadas debe realizarse previa autorización de un juez federal, de acuerdo con el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), y mediante una solicitud ministerial escrita, fundada y motivada como una medida que persigue un fin legítimo y es necesaria, idónea y proporcional para los objetivos que se buscan con ella. Cuando la intervención se produce a través de la ubicación geográfica en tiempo real no es necesaria la autorización judicial, pues se considera que esta injerencia es excepcional y necesaria cuando se encuentra en riesgo la vida o integridad física de las personas o cuando existe el riesgo de que se oculte o desaparezca el objeto de un ilícito.

La intervención de comunicaciones privadas puede prolongarse por un periodo máximo de seis meses y si la autoridad ministerial solicitara una prórroga, ésta podrá solo autorizarse si existen nuevos elementos que lo justifiquen (Código Nacional de Procedimientos Penales, artículo 292).

La jurisprudencia señala que una violación al secreto de las comunicaciones privadas "se consuma cuando se escucha, graba, almacena, lee o registra, sin el consentimiento de los interlocutores o sin autorización judicial, una comunicación ajena". La intervención realizada por un particular es ilegal y constituye un delito constitucional que se castiga con sanción carcelaria y pecuniaria. Existen cuatro excepciones:

1. Cuando uno de los participantes en la comunicación privada la ofrezca de manera voluntaria y en cuyo caso corresponderá al juez valorarla siempre y cuando no se viole el "deber de confidencialidad que establezca la ley".
2. Cuando, tratándose de menores de edad, resulte imprescindible la intervención de las comunicaciones privadas del menor para proteger sus propios intereses, se presuma que su integridad física se encuentra en riesgo o se pudiera estar en presencia de un delito flagrante.
3. Cuando se trate de las comunicaciones privadas de una víctima de secuestro que no pueda dar su consentimiento expreso por estar desaparecida. Esta excepción permite al ministerio público la intervención de las comunicaciones privadas de la víctima sin autorización judicial, "con el objetivo principal de avanzar en la investigación para ubicar su paradero y, en su caso, lograr su liberación".
4. Cuando se requiere la localización geográfica en tiempo real de un equipo de comunicación móvil asociado a una línea de telecomunicaciones (véase el concepto de geolocalización) como una medida urgente y excepcional legalmente válida cuando se presume que existe un peligro para la vida privada o la integridad de las personas o cuando esté en riesgo el objeto del delito o éste pueda desaparecer.

La jurisprudencia ha permitido determinar tres tipos legales de intervención:

1. Del contenido, que refiere al conocimiento que puede tener la autoridad de lo dicho y manifestado por un sospechoso o imputado en sus comunicaciones privadas (por ejemplo, que la autoridad ingrese a su bandeja de correo electrónico y conozca lo que ahí se dice y se comunica). Para que la intervención sea eficaz en un proceso judicial, debe contar con autorización judicial previa o ser producto del levantamiento del secreto por uno de sus participantes.

   Esta intervención abarca los datos almacenados en teléfonos móviles o cámaras fotográficas o de video, así como datos o archivos en formato de texto, audio, imagen o video. Se considera que estos aparatos pueden guardar información privada y por tanto protegida por el derecho de inviolabilidad de las comunicaciones privadas.
2. De datos de tráfico de las comunicaciones, que refiere a los datos externos del proceso comunicativo, como "el registro de los números marcados por un usuario de la red telefónica, la identidad de los comunicantes, la duración de la llamada telefónica o la identificación de una dirección de protocolo de internet (IP)".[1237] En la tesis "*Derecho a la inviolabilidad de las comunicaciones privadas*, su objeto de protección incluye los

1237 Tesis 1ª CLV/2011.Pag 221. Derecho a la inviolabilidad de las comunicaciones privadas. Su objeto de protección incluye los datos que identifican la comunicación. Novena época, registro:161335 Instancia: Primera Sala, materia constitucional, tesis aislada, Fuente: *Semanario Judicial de la Federación* y su gaceta, Tomo XXXIV, agosto de 2011.

datos que identifican la comunicación",[1238] la Primera Sala determinó que, "si bien es cierto que los datos no se refieren al contenido de la comunicación, también lo es que en muchas ocasiones ofrecen información sobre las circunstancias en que se ha producido la comunicación, afectando así, de modo directo o indirecto, la privacidad de los comunicantes".

3. De la localización geográfica en tiempo real, también conocida como geolocalización, que refiere al conocimiento inmediato de la autoridad del lugar aproximado donde se encuentra un determinado equipo de comunicación móvil. Esta medida está dirigida a geolocalizar un equipo de comunicación determinado en el momento de su activación o conexión a las redes de telecomunicaciones, lo que de manera indirecta significa también la geolocalización de quien lo utiliza en ese momento específico.

La Segunda Sala de la Suprema Corte consideró que la solicitud de geolocalización "no viola el derecho humano a la intimidad, ya que persigue un fin constitucionalmente válido al facilitar la investigación y persecución de ciertas actividades ilícitas mediante el uso de tecnologías de vanguardia en materia de telecomunicaciones, todo lo cual justifica que se confiera su acceso a las instancias de procuración de justicia para que puedan tener una respuesta inmediata a su solicitud, a efecto de proteger la vida y la integridad de las personas, como valor supremo a cargo del Estado mexicano".[1239]

Las autoridades competentes para solicitar la localización geográfica de equipos de comunicación móvil son:

a. el titular de la Procuraduría General de la República o los titulares de las procuradurías o fiscalías estatales y, en su caso, las personas en las que éstos deleguen esta facultad;
b. la Policía Federal en los términos del artículo 8, fracción XXVIII, de la ley que la regula, que refiere a sus atribuciones y obligaciones para prevenir la comisión de delitos y las faltas administrativas que determinen las leyes federales, intervenir en materia de seguridad pública y realizar investigación u operaciones encubiertas para la prevención de delitos, y
c. la autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional en los supuestos establecidos en su artículo 5, relacionados con las amenazas a la seguridad nacional como actos de espionaje, sabotaje o terrorismo o actos que impidan a las autoridades actuar contra la delincuencia organizada.

Ley de Seguridad Nacional aplica su ejercicio en asuntos relacionados con los delitos de delincuencia organizada, contra la salud, secuestro, extorsión y amenazas, como una medida urgente para salvaguardar la vida, la seguridad, la libertad e integridad física de las personas y la salud pública.

La solicitud para intervenir comunicaciones privadas, además de fundada y motivada, debe expresar:

1238 Tesis 1ª CLV/2011.Pag 221. Derecho a la inviolabilidad de las comunicaciones privadas. Su objeto de protección incluye los datos que identifican la comunicación. Novena época, Registro:161335 Instancia: Primera Sala, materia constitucional, tesis aislada, Fuente: *Semanario Judicial de la Federación* y su gaceta, Tomo XXXIV, agosto de 2011.

1239 LOCALIZACIÓN GEOGRÁFICA EN TIEMPO REAL DE LOS EQUIPOS DE COMUNICACIÓN MÓVIL. EL ARTÍCULO 190, FRACCIÓN I, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIDIFUSIÓN QUE LA PREVEE NO TRANSGREDE EL DERECHO HUMANO A LA INVIOLABILIDAD DE LAS COMUNICACIONES. Amparo en revisión 964/2015. Carlos Alberto Brito Ocampo y otros. 4 de mayo de 2016. Cinco votos de los Ministros Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán; se apartaron de consideraciones Margarita Beatriz Luna Ramos y José Fernando Franco González Salas, este último respecto a las consideraciones relacionadas con los datos estructurados (megadatos). Ponente: Alberto Pérez Dayán. Secretario: Isidro Emmanuel Muñoz Acevedo.

a) el tipo de intervención de comunicaciones privadas a realizarse;
b) los sujetos cuyas comunicaciones privadas serán interceptadas y
c) la duración de la intervención.

2. Derechos y obligaciones

El régimen de intervención de comunicaciones privadas no obliga a respetar el derecho de notificación de la persona investigada ni durante ni después de la intervención. Tampoco exige explícitamente la aportación de indicios o pruebas sobre la probable participación en un hecho delictivo de la persona que será investigada. Sobre el valor probatorio pleno del resultado de la intervención de comunicaciones privadas, ha sido tarea de la jurisprudencia exigir la aplicación de protocolos de recolección "a guisa de cadena de custodia" para "constatar la veracidad de su origen y contenido" y "que el contenido que obra en la fuente digital sea el mismo que se aporta al proceso". En este régimen también se encuentra ausente la aplicación del principio de debido proceso, para garantizar medidas de remediación en caso de violación de derechos de las personas que fueron objeto de la intervención de sus comunicaciones privadas.

En materia de transparencia, las autoridades que realizan intervención de comunicaciones privadas deben presentar reportes estadísticos solo cuando la medida se practique con la colaboración de los proveedores de servicios de telecomunicaciones que obliga el título octavo de la Ley Federal de Telecomunicaciones y Radiodifusión. Las autoridades deben publicar y mantener actualizado "el listado de solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos de comunicación, que contenga exclusivamente el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente", ordena el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública.

Intimidad

Eduardo Ferrer Mac-Gregor

El derecho a la intimidad, al igual que otros conceptos afines como el derecho al honor, a la vida privada y el de privacidad, no tiene una definición generalmente aceptada y su concreción legal está sujeta a múltiples interpretaciones doctrinales y jurisprudenciales. No obstante, su estudio ha sido constante desde las perspectivas académicas y jurisprudenciales, habiéndose vertido importantes consideraciones sobre su alcance y contenido.

Para delimitar su alcance y contenido, resulta esencial referirse a su definición gramatical. El *Diccionario de la Real Academia Española* (DRAE) indica que por "intimidad" debe entenderse lo siguiente: "zona espiritual íntima y reservada de una persona o de un grupo, especialmente una familia".[1240] A partir de dicha definición se confeccionan los calificativos de íntimo y reservado[1241] que establecen lo que Warren y Brandeis[1242] adelantaban como el

1240 RAE. (2018). *Diccionario de la Real Academia Española*. Disponible en: http://dle.rae.es/?id=LyCn6I9. Fecha de consulta: 23 de agosto de 2018.

1241 Romero, X. (2008) "El alcance del derecho a la intimidad en la sociedad actual",en *Revista Derecho del Estado*. Colombia, no. 21, pp. 209-222.

1242 Warren, S. y Brandeis, L. (1890, diciembre). "The Right to Privacy", en *Harvard Law Review.* Boston. Volumen IV, núm. 5.

derecho a ser dejado solo (*the right of privacy is the right to be to alone)*, concepción que sigue plenamente vigente para un núcleo importante de realidades ligadas a la intimidad.[1243]

El concepto de intimidad es un concepto complejo, pues no ha sido estático en el tiempo ni en el espacio.[1244] Además de haber ido en evolución, varía en cada región del planeta donde existe una visión propia del mismo[1245] y por tanto de sus senderos prácticos.

Pese a que en la doctrina y en la jurisprudencia no hay voces unívocas sobre el alcance de este concepto, se admite que íntimo es aquello que está lo más adentro posible. Lo que está en el interior del hombre.[1246]

En la doctrina se han distinguido diversas concepciones del derecho a la intimidad. A manera de síntesis se pueden identificar[1247] como relevantes las siguientes:

a) Concepto objetivo: esta postura, entre otras cosas, precisa que este concepto tiene su desarrollo en la denominada "teoría de los círculos concéntricos" o "teoría de las esferas", a partir de la cual se considera que el núcleo, lo más interior, lo constituye lo íntimo; en una parte más externa encontramos lo familiar; en otra, lo secreto o confidencial; siendo la última esfera lo público.[1248] Esta postura es adoptada por el Tribunal Constitucional Español.[1249]

b) Concepto subjetivo: esta postura considera que "cada persona tiene derecho a controlar lo que de ella se conoce, los datos a ella relativos, y el ordenamiento jurídico debe establecer los mecanismos necesarios para que este derecho sea efectivo".[1250] En este contexto, se ha considerado que "el atributo más importante de la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstención de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusiva, como a la divulgación ilegítima de esos datos". [1251] Es decir, existe determinados aspectos como la vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado.[1252]

1243 Martínez de Pisón Cavero, J. (2016). "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional", en *Anuario de Filosofía del Derecho.* Estudios de teoría del derecho y filosofía del derecho. España, p. 413.

1244 El contenido del derecho a la intimidad o vida privada está destinado a variar, legítima y normalmente, tanto por motivos que podemos llamar internos al propio concepto como por motivos externos al mismo. *Vid,* Tesis: 1a. CCXIII/2009. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXX, diciembre de 2009, p. 276.

1245 Brena, I. (s.f.). "Privacidad y confidencialidad de los datos genéticos", en *Boletín Mexicano de Derecho Comparado*. México. UNAM, Instituto de Investigaciones Jurídicas, número conmemorativo, sexagésimo aniversario, pp. 109-125.

1246 Pfeffer, E. (2000). *Los derechos a la intimidad o privacidad, a la honra y a la propia imagen. Su protección frente a la libertad de opinión e información*. *Ius et Praxis* [en línea]. Disponible en: http://www.redalyc.org/articulo.oa?id=19760123 ISSN 0717-2877 Fecha de consulta: 23 de agosto de 2018.

1247 La identificación de las principales concepciones no es nuestra, sino que tomamos las aportaciones de Lucrecio Rebollo Delgado y Yolanda Gómez Sánchez, por lo que para una mayor referencia se remite a la consulta de dichos autores. Cfr. Rebollo, L. y Gómez Y. (2008). *Biomedicina y Protección de Datos*. Dykinson S.L. Madrid, pp. 41-45.

1248 Rebollo, L. y Gómez Y. (2008). *Biomedicina y Protección de Datos*. Dykinson S.L. Madrid, p. 41.

1249 Al respecto, el Tribunal Constitucional Español en la sentencia 207/1996, de 16 de diciembre de 1996, indicó lo siguiente: "En efecto, el derecho a la intimidad personal garantizado por el art. 18.1 C.E. tiene un contenido más amplio que el relativo a la intimidad corporal. Según doctrina reiterada de este Tribunal, el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 C.E.), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC 231/1988, 197/1991, 20/1992, 219/1992, 142/1993, 117/1994 y 143/1994), y referido preferentemente a la esfera, estrictamente personal, de la vida privada o de lo íntimo (SSTC 142/1993 y 143/1994)".

1250 Rebollo, L. y Gómez Y. (2008). *Biomedicina y Protección de Datos*. Dykinson S.L. Madrid, p. 43.

1251 Tribunal Constitucional Español, Sentencia 142/1993, de 22 de abril de 1993.

1252 Tribunal Constitucional Español, Sentencia 110/1984, de 26 de noviembre de 1984.

Se trata de proteger un espacio, en este caso íntimo, de la intromisión o injerencia de terceros, de decidir quién puede o no puede participar de las acciones, decisiones y de todo lo acaecido en ese ámbito que pertenece a los sujetos por el mero hecho de ser personas.[1253] El derecho a la intimidad —en cualquiera de sus dimensiones— hace referencia primariamente a un espacio restringido de libre disposición por parte del individuo.[1254]

La intimidad se concibe así "como barrera jurídica a la intromisión de terceros, tanto del Estado como de particulares".[1255] Como señala Guzmán García, este derecho "tiene la función de proteger, frente a cualquier invasión que pueda realizarse en el ámbito de la vida personal y familiar, aquella información que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad".[1256]

La naturaleza jurídica del derecho a la intimidad puede visualizarse así en la negación al configurarlo como un típico derecho de defensa exclusiva.[1257] Es decir, se concibe a este derecho "ya no solo como la potestad que tenemos de que un tercero conozca o no nuestra vida privada, sino también la posibilidad de controlar lo que otros conocen de nosotros mismos".[1258]

El derecho a la intimidad es "un derecho subjetivo, de defensa de una parcela de nuestra vida que queremos mantener reservada, y de la que tenemos plena disposición".[1259] El derecho a la intimidad, entonces, "se asocia con la existencia de un ámbito privado que se encuentra reservado frente a la acción y conocimiento de los demás y tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y conocimiento de terceros, ya sean simples particulares o bien los poderes del Estado".[1260]

El derecho a la intimidad como derecho humano atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia, garantizando el derecho a poseer la intimidad a efecto de disponer del control sobre la publicidad de la información tanto de la persona como de su familia, lo que se traduce en el derecho de la autodeterminación de la información, que supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede utilizarla.[1261]

1. Contenido

En cuanto a su contenido, destaca Guzmán García que este derecho confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, en otras palabras, deberes de no hacer.[1262] Como se mencionó antes, se trata de un derecho subjetivo oponible a terceros.

1253 Martínez de Pisón Cavero, J. (2016). "El derecho a la intimidad: de la configuración inicial a los últimos desarrollos en la jurisprudencia constitucional", en *Anuario de Filosofía del Derecho.* Estudios de teoría del derecho y filosofía del derecho. España, p. 412.

1254 Rebollo, L. y Gómez Y. (2008). *Biomedicina y Protección de Datos*. Dykinson S.L. Madrid, p. 43.

1255 Frígolis, E. (2010). "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", en Jareño, Leal, Ángeles (coord.) *La Protección jurídica de la intimidad*. Iustel. España.

1256 Gómez, P. (2010). "Intimidad y vida privada", en *Diccionario de Derecho de la Información.* Tomo II. UNAM-IIJ/Bosque de Letras. México, p. 131.

1257 Rebollo, L. y Gómez Y. (2008). Biomedicina y Protección de Datos. Dykinson S.L. Madrid, p. 33.

1258 Ídem.

1259 Rebollo, L. y Gómez Y. (2008). *Biomedicina y Protección de Datos*. Dykinson S.L. Madrid, p. 33.

1260 Tesis: I.3o.C.695 C. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVIII, septiembre de 2008, p. 1253.

1261 Tesis: I.3o.C.695 C. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVIII, septiembre de 2008, p. 1253.

1262 Guzmán, M. (2014). "Derecho a la intimidad", en Ferrer Mac-Gregor, Eduardo, Martínez Ramírez, Fabiola, *et al.,* (coords.), *Diccionario de derecho procesal constitucional y convencional*. 2a. ed. México. Instituto de investigaciones Jurídicas de la Universidad Nacional Autónoma de México, pp. 355-356.

En este contexto, se ha señalado que este derecho tiene un ámbito interno (*ad intra*) del individuo, y otro externo (*ad alia*). Es decir, por un lado, se constituye como una manifestación interna, es un neto derecho de defensa, y del otro extremo, en su carácter externo, es un derecho con una interpretación expansiva, la facultad que tenemos de decidir lo que queremos que otros conozcan de lo que a nosotros pertenece.[1263]

Hay autores que han destacado que este concepto cubre una multitud de aspectos como la violación de correspondencia, las escuchas telefónicas, la captura de fotografías, el voyerismo, etcétera, en tanto que son prácticas que pueden ser agresivas a la intimidad y que pueden generar, y de hecho han generado, mucha normatividad de protección, desde la legislación penal hasta la legislación sobre comunicaciones o incluso hasta un reglamento municipal sobre la apertura de ventas en edificios.[1264] Por ello, se dice que la conexión de este derecho con la libertad y dignidad de la persona implica que la esfera de inviolabilidad de la persona frente a injerencias externas, el ámbito personal y familiar, solo en ocasiones tenga proyección hacia el exterior. [1265]

Asimismo, dentro de este derecho[1266] se encuentra el derecho a la intimidad de la información, que es aquel derecho de toda persona a que no se difunda información de carácter personal o profesional vinculada con su vida privada. Tal derecho pierde su vigencia en el momento en que el titular del mismo otorga su consentimiento para que se divulgue la información.[1267]

El derecho a la intimidad impone a los poderes públicos, como a los particulares, diversas obligaciones, a saber: no difundir información de carácter personal, entre los que se encuentran los datos personales, confidenciales, el secreto bancario e industrial y en general en no entrometerse en la vida privada de las personas; asimismo, el Estado, a través de sus órganos, debe adoptar todas las medidas tendentes a hacer efectiva la protección de este derecho. [1268] El derecho a la intimidad protege así la no divulgación de datos de la vida privada de una persona, es decir, que los demás no conozcan aspectos de su vida sin su consentimiento.[1269]

De esta forma, en el ámbito judicial, se ha destacado que la vida se constituye por el ámbito privado reservado para cada persona y del que quedan excluidos los demás, mientras que la intimidad se integra con los extremos más personales de la vida y del entorno familiar, cuyo conocimiento se reserva para los integrantes de la unidad familiar.[1270] En esta tesitura, la Primera Sala de la Suprema Corte de Justicia de la Nación (SCJN) ha destacado que "la intimidad se integra con los extremos más personales de la vida y del entorno familiar, cuyo conocimiento se reserva para los integrantes de la unidad familiar".[1271]

1263 Rebollo, L. y Gómez Y. (2008). *Biomedicina y Protección de Datos*. Dykinson S.L. Madrid, p. 33.

1264 Cfr. Méjan, L. (1994). *El Derecho a la Intimidad y la Informática*. Porrúa. México, p.1.

1265 Tribunal Constitucional Español, Sentencia 142/1993, de 22 de abril de 1993.

1266 Existe una serie de derechos destinados a la protección de la vida privada, entre ellos el del honor, que es un bien objetivo que permite que alguien sea merecedor de estimación y confianza en el medio social donde se desenvuelve y, por ello, cuando se vulnera dicho bien, también se afectan la consideración y estima que los demás le profesan, tanto en el ámbito social como en el privado. En esa tesitura, se concluye que cuando se lesiona el honor de alguien con una manifestación o expresión maliciosa, se afecta su vida privada. *Vid*, Tesis: 1a. CXLVIII/2007. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVI, julio de 2007, p. 272.

1267 Tesis: I.3o.C.696 C. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVIII, septiembre de 2008, p. 1253.

1268 Tesis: I.3o.C.695 C. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVIII, septiembre de 2008, p. 1253.

1269 Tesis: 1a. XLIV/2010. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXXI, marzo de 2010, p. 922.

1270 Tesis: 2a. LXIV/2008. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVII, mayo de 2008, p. 234.

1271 Tesis: 1a. CXLIX/2007. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVI, julio de 2007, p. 272.

La Primera Sala de la SCJN ha destacado que el concepto de vida privada comprende a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, esto es, la vida privada es lo genéricamente reservado y la intimidad —como parte de aquélla— lo radicalmente vedado, lo más personal; de ahí que, si bien son derechos distintos, al formar parte uno del otro, cuando se afecta la intimidad, se agravia a la vida privada".[1272]

Respecto de su diferencia con el derecho a la no intervención de comunicaciones, la jurisprudencia nacional ha destacado que este derecho, "a pesar de ser una manifestación más de aquellos derechos que preservan al individuo de un ámbito de actuación libre de injerencias de terceros —como sucede con el derecho a la intimidad, a la inviolabilidad del domicilio o la protección de datos personales—, el derecho a la inviolabilidad de las comunicaciones privadas posee una autonomía propia reconocida por la Constitución Política de los Estados Unidos Mexicanos (CPEUM)".[1273] En cambio, la inviolabilidad del domicilio es el derecho fundamental que permite disfrutar de la vivienda sin interrupciones ilegítimas y permite desarrollar la vida privada sin ser objeto de molestias.

En el plano normativo destaca la Ley de Responsabilidad Civil para La Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal,[1274] que en su artículo 11 precisa que la intimidad forma parte del derecho a la vida privada, y que la primera comprende conductas y situaciones que, por su contexto y que por desarrollarse en un ámbito estrictamente privado, no están destinados al conocimiento de terceros o a su divulgación, cuando no son de interés público o no se han difundido por el titular del derecho.

2. Desarrollo constitucional y en tratados internacionales

El artículo 16 constitucional establece, en general, la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. En un sentido amplio, la referida garantía puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16 de la CPEUM, primer párrafo, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida.[1275]

El derecho a la intimidad, entonces, se reconoce en el primer párrafo del artículo 16 de la CPEUM que prevé lo siguiente:

> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

1272 Tesis: 1a. CXLIX/2007. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVI, julio de 2007, p. 272.

1273 Tesis: 1a. CLIII/2011. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXXIV, agosto de 2011, p. 221.

1274 Artículo 11. Como parte de la vida privada se tendrá derecho a la intimidad que comprende conductas y situaciones que, por su contexto y que por desarrollarse en un ámbito estrictamente privado, no están destinados al conocimiento de terceros o a su divulgación, cuando no son de interés público o no se han difundido por el titular del derecho.

1275 Tesis: 2a. LXIII/2008. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVII, mayo de 2008, p. 229.

Al respecto, señala Cobos Campos que de ello deriva la abstención de realizar actos de molestia por el Estado, salvo los casos de excepción que se señalan en el mismo, así como la protección de los datos personales, la inviolabilidad del domicilio y la inviolabilidad de las comunicaciones privadas.[1276]

En lo que respecta a su reconocimiento en los instrumentos convencionales y tratados internacionales, destaca su inclusión en los siguientes instrumentos:

La Declaración Universal de Derechos Humanos en su artículo 12 señala lo siguiente:

> Artículo 12.
>
> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

La Convención Americana sobre Derechos Humanos (CADH), en su artículo 11, dispone lo siguiente:

> Artículo 11. Protección a la honra y de la dignidad
>
> Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
>
> Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
>
> Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos precisa:

> Artículo 17.
>
> Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
>
> Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.
>
> El derecho a la intimidad se configura como un derecho humano sustancial[1277] protegido por la CPEUM y diversos instrumentos de carácter internacional ratificados por México.

3. El derecho a la intimidad en las resoluciones de la Corte Interamericana de Derechos Humanos

El derecho a la intimidad se encuentra íntimamente relacionado con otros derechos humanos de carácter personal como la vida privada y el honor, tanto por sus implicaciones prácticas como por su propia naturaleza de derecho humano relacionado con la libertad y dignidad personal, por ello, para el estudio de casos sobre este concepto, nos remitimos a la lectura de los casos relativos a las voces de derecho al honor y vida privada que forman parte de esta publicación, pues la Corte Interamericana de Derechos Humanos (CIDH), en el momento de interpretar los alcances de la intimidad, lo ha hecho a la par de los derechos de honor y vida privada.

1276 Cobos, A. (2013, julio-diciembre). "El contenido del derecho a la intimidad", en *Cuestiones constitucionales*. México. IIJ-UNAM, núm. 29.México. pp. 45-81. Disponible en: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932013000200003&lng=es&tlng=es Fecha de consulta: 23 de agosto de 2018.

1277 De acuerdo con la doctrina, son derechos sustantivos los que se identifican con los bienes de la vida. En ese sentido, pueden considerarse sustantivos, sin pretender asignarles un orden, entre otros, los derechos patrimoniales, los que surgen de las relaciones de familia y del estado civil de las personas, la vida misma, la libertad personal, la de conciencia, la de expresión, el derecho al honor, a la intimidad, etc. En cambio, los derechos procesales o instrumentales, también llamados adjetivos, son únicamente el medio para hacer observar o proteger el derecho sustantivo. Tales derechos procesales no tienen por objeto su propio ejercicio, ni constituyen un fin en sí mismos, sino que se trata solo de las reglas para obtener del Estado la garantía del goce de los bienes de la vida. *Vid* Tesis: I.8o.C. J/2 (10a.). Décima época. *Gaceta del Semanario Judicial de la Federación*. Libro 40. Tomo IV, marzo de 2017, p. 2416.

Inviolabilidad de las comunicaciones

José Soto Galindo

Las comunicaciones privadas en México gozan del derecho al secreto, es decir, a que solo sean conocidas por las personas que participan o participaron en la comunicación o por los terceros que éstas decidan. A esto se le llama inviolabilidad de las comunicaciones privadas y es un derecho fundamental reconocido a favor de las personas en México. Este derecho está relacionado con otros derechos fundamentales como el derecho a la vida privada y a la intimidad, a la protección de los datos personales y a la inviolabilidad del domicilio. El derecho a las comunicaciones privadas es una garantía formal, pues implica que todas las comunicaciones privadas están protegidas con independencia de su contenido: "No se necesita en modo alguno analizar el contenido de la comunicación, o de sus circunstancias, para determinar su protección por el derecho fundamental".[1278]

Su presentación en el marco jurídico se encuentra en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM):

> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Este derecho refiere al secreto que debe regir sobre las comunicaciones privadas producidas con cualquier sistema de comunicación análogo o digital, como el correo o telégrafo, el teléfono alámbrico y móvil o las comunicaciones a través de internet, así como los datos almacenados en teléfonos móviles, aparatos de cómputo, cámaras fotográficas o de video, como datos en forma de texto, audio, imagen o video. Se trata de resguardar la esfera de la vida privada donde las personas pueden expresar libremente su identidad, en sus relaciones con los demás o en lo individual.

En un sentido amplio, el derecho a la inviolabilidad de las comunicaciones privadas "puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida".[1279]

En el derecho internacional del que México es parte, está garantizado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por los países miembros de la Organización de las Naciones Unidas (ONU) en 1966, y en el artículo 11 de la Convención Interamericana sobre Derechos Humanos (CIDH), también conocida como el Pacto de San José, suscrita por los integrantes de la Organización de los Estados Americanos (OEA) en 1969.

Entre las leyes primarias y la regulación secundaria, la intervención de las comunicaciones privadas está regulada en el Código Penal Federal (artículos 173 al 177),[1280] en el Código

1278 Tesis 1a. CLIII/2011. Primera Sala de la Suprema Corte de Justicia de la Nación. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXXIV, agosto de 2011, p. 221.

1279 Tesis 2a. LXIII/2008. Segunda Sala de la Suprema Corte de Justicia de la Nación. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVII, mayo de 2008, p. 229.

1280 El capítulo II del Código Penal Federal está dedicado a la violación de correspondencia (artículos 173 a 177) y castiga la intervención de comunicaciones privadas sin mandato de autoridad judicial competente con sanciones de seis a 12 años de prisión y de 300 a 600 días multa.

Nacional de Procedimientos Penales (artículos 291 al 303),[1281] en la Ley Federal Contra la Delincuencia Organizada (artículos 15 al 28),[1282] y en la Ley Federal de Telecomunicaciones y Radiodifusión (artículos 189 y 190).[1283] Existen también los Lineamientos de Colaboración en Materia de Seguridad y Justicia emitidos por el Instituto Federal de Telecomunicaciones para normar la colaboración de los proveedores de servicios de telecomunicaciones con las autoridades de seguridad y procuración de justicia en México.[1284]

1. Antecedentes

Su origen en el régimen jurídico mexicano se encuentra en la Constitución de 1857, que consagró en su artículo 16 la defensa del ciudadano frente a intromisiones o molestias arbitrarias de parte del Estado:

> Todos los habitantes de la República, así en su persona y familias, como en su domicilio, papeles y posesiones, están a cubierto de todo atropellamiento, examen o cateo, embargo o secuestro de cualquier persona o cosa, excepto en los casos prefijados por las leyes y con las indispensables condiciones de que se procederá racionalmente y de que la autoridad competente exprese en su mandato escrito la causa probable del procedimiento, sostenida por la afirmación al menos de un testigo, y señale y describa el lugar que debe ser registrado o la cosa o persona que debe ser secuestrada.

La autoría del artículo 16 en la Constitución del 57 es de Ponciano Arriaga Leija, quien justificó su redacción con un criterio liberal e ilustrado que oponía el uso de la razón al uso de la fuerza para defender al ciudadano de actos arbitrarios. Arriaga defendió su propuesta como una salvaguardia contra "la manera bárbara y salvaje con que en México se hacen las prisiones, esa especie de furor canino con que toda clase de autoridades maltratan y atropellan a los ciudadanos. Desde los guardias diurnos hasta los gobernadores del distrito, todos se creen con derecho para vejar y golpear al que reconvienen o aprehenden".[1285]

Esta salvaguardia contra la intromisión arbitraria a la vida privada personal y familiar fue refrendada en la Constitución de 1917 y reformada en 1996 para sumarle dos párrafos para regular la intervención de las comunicaciones privadas ante los avances tecnológicos y sus posibles repercusiones en la vida privada de los ciudadanos. Su construcción como derecho de rango máximo trata de proteger el espacio privado donde las personas ejercen su libertad a plenitud, sin injerencias ni molestias.

2. La esfera de protección y sus límites

El secreto de las comunicaciones privadas, como parte del conjunto de derechos relacionados con el espacio privado personal, se encuentra bajo el paraguas de protección a la vida privada:

1281 El artículo 291 del Código Nacional de Procedimientos Penales es el dispositivo jurídico que mejor describe la intervención de las comunicaciones privadas en el régimen jurídico mexicano: "La intervención de comunicaciones privadas abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real".

1282 Esta ley es explícita al considerar que la intervención de comunicaciones privadas como una herramienta de investigación judicial. Su capítulo sexto (artículos 15 a 28) está dedicado a la intervención de comunicaciones privadas.

1283 El título octavo de esta ley, promulgada en 2014, obliga a los concesionarios y autorizados de telecomunicaciones a colaborar con las autoridades de seguridad, procuración y administración de justicia en materia de intervención de las comunicaciones privadas.

1284 Los Lineamientos fueron publicados en el *Diario Oficial de la Federación* el 2 de diciembre de 2015.

1285 Ovalle, J. (2013). "Artículo 16. Intervención de comunicaciones privadas y jueces de control", en Ferrer Mac-Gregor Poisot, Eduardo, Caballero Ochoa, José Luis, y Steiner, Christian. *Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana*. México. SCJN-UNAM y Konrad Adenauer Stiftung. pp. 1801-1814.

> El derecho fundamental a la vida privada consiste en la facultad que tienen los individuos para no ser interferidos o molestados por persona o entidad alguna, en todo aquello que desean compartir únicamente con quienes ellos eligen; así, este derecho deriva de la dignidad de la persona e implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás.[1286]

Existen circunstancias en las que la intervención de las comunicaciones privadas puede justificarse jurídicamente (véase, intervención de comunicaciones privadas). Su conocimiento por parte de terceros puede adquirir legalidad plena bajo tres circunstancias:

1) Como un acto de investigación o diligencia de investigación, avalada por una autoridad judicial federal a una solicitud ministerial por escrito, fundada y motivada. Esta injerencia debe justificarse como una intromisión necesaria, idónea y proporcional para alcanzar un fin legítimo. Existen tres tipos de intervención de comunicaciones privadas autorizadas:
   a) del contenido, que permite a la autoridad conocer lo dicho o manifestado por un sospechoso o imputado en sus comunicaciones privadas, con la intención de acreditar el delito y su responsabilidad;
   b) de datos de tráfico de las comunicaciones, que refiere a la información relacionada con el proceso comunicativo y que, en ciertas circunstancias, puede ser más reveladora que el propio contenido de las comunicaciones privadas y
   c) de la localización geográfica de un aparato de comunicación móvil vinculado a una persona determinada (véase, geolocalización).
2) Cuando una de las partes involucradas en la comunicación la revele bajo consentimiento propio. Su utilidad en un proceso judicial dependerá de la valoración del juez y nunca podrá ser admitida cuando no se viole el "deber de confidencialidad que establezca la ley".
3) Cuando, tratándose de menores de edad, la intervención de sus comunicaciones privadas resulte imprescindible para proteger los propios intereses del menor, exista riesgo fundado de que su integridad física pueda verse afectada o se presuma la comisión de un delito flagrante.[1287]

La inviolabilidad de las comunicaciones privadas es un derecho fundamental garantizado en democracia y solo debe ser vulnerado por autoridades facultadas y con autorización judicial cuando existen elementos que la ley considere graves.

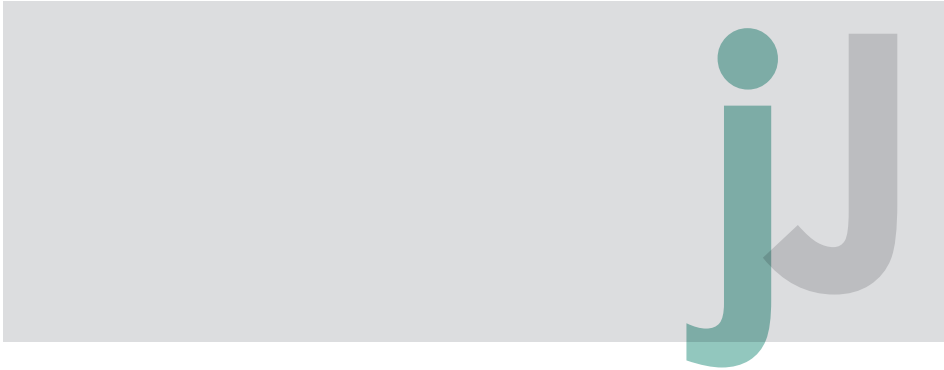
1286 Tesis 1a. CXLVIII/2007. Primera Sala de la Suprema Corte de Justicia de la Nación. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVI, julio de 2007, p. 272.

1287 Tesis 1a. CLXI/2011. Primera Sala de la Suprema Corte de Justicia de la Nación. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXXIV, agosto de 2011, p. 176.

NOTAS

NOTAS

NOTAS



Juicio contencioso administrativo (juicio de nulidad)

Gabriel López López

La voz "juicio contencioso administrativo" se trata de un procedimiento jurisdiccional general que reviste una importancia fundamental para la materia de protección de datos personales, pues se trata de uno de los medios de defensa que la normatividad del sector privado reconoce a favor de las personas (físicas o morales) afectadas por una resolución recaída a un procedimiento sustanciado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Dato Personales (INAI), Procedimiento de Protección de Datos (PPD), Procedimiento de Verificación (PV) o Procedimiento de Imposición de Sanciones (Pisan) dándoles la oportunidad de lograr una efectiva tutela de sus derechos.

Comúnmente es conocido como juicio de nulidad, es un medio de defensa que se sustancia ante el Tribunal Federal de Justicia Administrativa (TFJA) y cuyo procedimiento se contiene en la Ley Federal de Procedimiento Contencioso Administrativo (LFPCA).

Las autoridades de la administración pública federal tendrán acción para controvertir una resolución administrativa favorable a un particular cuando estime que es contraria a la ley. A este procedimiento se le conoce generalmente como juicio de lesividad.

1) Antecedentes

El TFJA[1288] tiene su origen en la Ley de Justicia Fiscal de 1936, ubicándolo dentro de la estructura del Poder Ejecutivo Federal aunque materialmente su actuación fuese jurisdiccional. Esta ley previno inicialmente todas las formas y mecanismos por los cuales los particulares podían defender sus derechos en caso de que se suscitara una controversia en contra de alguna autoridad o del Estado en materia fiscal.

Es un tribunal similar a uno judicial, con plena autonomía e independencia, sus resoluciones son revisadas por el Poder Judicial de la Federación (PJF) y la jurisprudencia de la Suprema Corte de Justicia de la Nación (SCJN) es obligatoria, así como la de los tribunales colegiados que funcionan dentro de su jurisdicción territorial.[1289]

1288 Anteriormente denominado Tribunal Federal de Justicia Fiscal y Administrativa. Con la implementación del Sistema Nacional Anticorrupción y con la entrada en vigor de la nueva Ley Orgánica del Tribunal Federal de Justicia Administrativa publicada el 18 de julio de 2016 cambió su denominación a Tribunal Federal de Justicia Administrativa (TFJA).

1289 Carpizo, J. (1972). "Bases Constitucionales de los Tribunales Administrativos", en *Revista del Tribunal de lo Contencioso Administrativo del Distrito Federal*. México.

Su existencia se encuentra prevista en el artículo 73, fracción XXIX-H, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), el cual señala que el TFJA es un órgano dotado de plena autonomía para dictar sus fallos, establecer su organización, su funcionamiento y los recursos para impugnar sus resoluciones. El Tribunal tendrá a su cargo dirimir las controversias que se susciten entre la administración pública federal y los particulares.[1290]

En lo que respecta a la composición y funcionamiento del TFJA, de acuerdo con el artículo 73, fracción XXIX-H, de la CPEUM, éste se integra de la siguiente manera:

Órgano	Integrantes	Descripción
Sala superior	16 magistrados	Pleno General, Pleno Jurisdiccional y tres secciones (primera y segunda sección con competencia en materia fiscal y administrativa; y la tercera sección con competencia en responsabilidades administrativas).
Junta de gobierno	5 magistrados	Presidente del TFJA, dos magistrados de la Sala Superior y dos magistrados de salas regionales.
Salas regionales	3 magistrados	a) Salas ordinarias b) Salas auxiliares c) Salas especializadas d) Salas mixtas

2) Formas de tramitación del JCAF

Existen dos formas para tramitar un juicio contencioso administrativo federal (JCAF): por la vía tradicional o en línea. La vía tradicional es la forma más común y frecuente de presentar una demanda, la cual se realiza por escrito y se presenta ante la sala regional competente.

Por otro lado, el juicio en línea es un proceso administrativo contencioso que surge como consecuencia del creciente desarrollo de las tecnologías de la información con la finalidad de mejorar y acelerar la impartición de justicia en nuestro país; por lo que el 12 de junio de 2009, se publicó en el *Diario Oficial de la Federación* (DOF) el decreto por el que se reforman y adicionan diversas disposiciones de la LFPCA y de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa, en el que se implementó de manera oficial el sistema de juicio en línea.

1290 "Artículo 73.- El Congreso tiene facultad:
[...]
Fracción XXIX-H. Para expedir la ley que instituya el Tribunal Federal de Justicia Administrativa, dotado de plena autonomía para dictar sus fallos, y que establezca su organización, su funcionamiento y los recursos para impugnar sus resoluciones. El Tribunal tendrá a su cargo dirimir las controversias que se susciten entre la administración pública federal y los particulares. Asimismo, será el órgano competente para imponer las sanciones a los servidores públicos por las responsabilidades administrativas que la ley determine como graves y a los particulares que participen en actos vinculados con dichas responsabilidades, así como fincar a los responsables el pago de las indemnizaciones y sanciones pecuniarias que deriven de los daños y perjuicios que afecten a la hacienda pública federal o al patrimonio de los entes públicos federales. El Tribunal funcionará en Pleno o en salas regionales. La Sala Superior del Tribunal se compondrá de dieciséis magistrados y actuará en Pleno o en secciones, de las cuales a una corresponderá la resolución de los procedimientos a que se refiere el párrafo tercero de la presente fracción. Los magistrados de la Sala Superior serán designados por el presidente de la República y ratificados por el voto de las dos terceras partes de los miembros presentes del Senado de la República o, en sus recesos, por la comisión permanente. Durarán en su encargo 15 años improrrogables. Los magistrados de Sala Regional serán designados por el presidente de la República y ratificados por mayoría de los miembros presentes del Senado de la República o, en sus recesos, por la comisión permanente. Durarán en su encargo 10 años pudiendo ser considerados para nuevos nombramientos. Los magistrados solo podrán ser removidos de sus cargos por las causas graves que señale la ley".

3) Sustanciación del JCAF

A) Procedencia

De acuerdo con el artículo 2 de su ley reglamentaria, procede contra las resoluciones administrativas definitivas que establece la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa (LOTFJFA) y contra los actos administrativos, decretos y acuerdos de carácter general, diversos a los reglamentos, cuando sean autoaplicativos o cuando el interesado los controvierta en unión del primer acto de aplicación.

B) Partes

De conformidad con el artículo 3 de la LFPCA, en el JCAF son partes:

a) el demandante, también llamado actor, es aquella persona física o moral titular de un derecho que se estima vulnerado, que acude a demandar la nulidad del acto administrativo que le ocasiona un perjuicio;

b) el demandado, teniendo tal carácter la autoridad que dictó la resolución impugnada, el particular a quien favorezca la resolución cuya modificación o nulidad pida la autoridad administrativa y el jefe del Servicio de Administración Tributaria o el titular de la dependencia u organismo desconcentrado o descentralizado que sea parte en los juicios en que se controviertan resoluciones de autoridades federativas coordinadas;

c) el tercero interesado, es aquella persona que tiene intereses diversos a los del demandante y

d) la demanda.

Un juicio contencioso administrativo federal (JCAF) inicia con la presentación de la demanda, misma que deberá realizarse dentro de los plazos previstos por el artículo 13 de LFPCA.[1291]

La demanda deberá contener, de conformidad por lo establecido por el artículo 14 de la LFPCA, los siguientes requisitos:

a) el nombre del demandante, domicilio fiscal, así como domicilio para oír y recibir notificaciones dentro de la jurisdicción de la sala regional competente y su dirección de correo electrónico;

b) la resolución que se impugna. En el caso de que se controvierta un decreto, acuerdo, acto o resolución de carácter general, precisará la fecha de su publicación;

c) la autoridad o autoridades demandadas o el nombre y domicilio del particular demandado cuando el juicio sea promovido por la autoridad administrativa;

1291 "Artículo 13. [...] I. De treinta días siguientes a aquél en el que se dé alguno de los supuestos siguientes:
a) Que haya surtido efectos la notificación de la resolución impugnada, lo que se determinará conforme a la ley aplicable a ésta, inclusive cuando se controvierta simultáneamente como primer acto de aplicación una regla administrativa de carácter general.
[...] b) hayan iniciado su vigencia el decreto, acuerdo, acto o resolución administrativa de carácter general impugnada cuando sea autoaplicativa.
II. De 30 días siguientes a aquél en el que surta efectos la notificación de la resolución de la sala o sección que habiendo conocido una queja, decida que la misma es improcedente y deba tramitarse como juicio. Para ello, deberá prevenirse al promovente para que, dentro de dicho plazo, presente demanda en contra de la resolución administrativa que tenga carácter definitivo.
III. De cinco años cuando las autoridades demanden la modificación o nulidad de una resolución favorable a un particular, los que se contarán a partir del día siguiente a la fecha en que éste se haya emitido, salvo que haya producido efectos de tracto sucesivo, caso en el que se podrá demandar la modificación o nulidad en cualquier época sin exceder de los cinco años del último efecto, pero los efectos de la sentencia, en caso de ser total o parcialmente desfavorable para el particular, solo se retrotraerán a los cinco años anteriores a la presentación de la demanda."

d) los hechos que den motivo a la demanda;
e) las pruebas que ofrezca;
f) los conceptos de impugnación;
g) el nombre y domicilio del tercero interesado, cuando lo haya y
h) lo que se pida, señalando en caso de solicitar una sentencia de condena, las cantidades o actos cuyo cumplimiento se demanda.

Cuando el demandante incumpla con algún requisito contenido dentro de los incisos a, b y f (anteriormente señalados) se desechará por improcedente la demanda, en tanto que si omite cumplir con los demás requisitos, el magistrado instructor requerirá al demandante para que los señale dentro del término de cinco días, apercibiéndolo que de no hacerlo en tiempo se tendría por no presentada la demanda o por no ofrecidas las pruebas, según corresponda.

Satisfechos los requisitos anteriormente señalados, el magistrado instructor dictará el acuerdo de admisión de demanda y ordenará que se le corra traslado de la misma y sus anexos a la demandada y al tercero interesado, emplazándolos para que formulen su contestación de demanda y manifiesten lo que a su derecho convenga dentro de los 30 días siguientes a aquél en que surta efectos el emplazamiento, según corresponda.

C) Contestación de demanda

En aras del principio de equidad procesal entre las partes, tanto el demandado como el tercero interesado, cuentan con el mismo plazo que el actor para la interposición de su demanda, para formular su contestación de demanda y realizar sus manifestaciones, respectivamente.

De conformidad con lo previsto por el artículo 19 de la LFPCA, cuando no se produzca la contestación en tiempo y forma, o ésta no se refiera a todos los hechos, se tendrán como ciertos los que el actor impute de manera precisa al demandado, salvo que por las pruebas rendidas o por hechos notorios resulten desvirtuados.

D) Notificaciones

Las notificaciones a las partes en el JCAF deberán realizarse por medio del *Boletín Jurisdiccional*, y de conformidad con el procedimiento establecido en el artículo 65 de la LFPCA.[1292]

E) Suspensión y medidas cautelares

Durante la tramitación del juicio, cualquiera de las partes podrá solicitar la suspensión de la ejecución del acto impugnado, a fin de mantener la situación de hecho existente en el estado en que se encuentra, así como solicitar que se decreten todas las medidas caute-

1292 Artículo 65. Las notificaciones a los particulares y a las autoridades en el juicio deberán realizarse por medio del *Boletín Jurisdiccional*, enviándose previamente un aviso electrónico a su dirección de correo electrónico o dirección de correo electrónico institucional según sea el caso, de que se realizará la notificación, a más tardar el tercer día siguiente a aquél en que el expediente haya sido turnado al actuario para ese efecto. El aviso de notificación deberá ser enviado cuando menos con tres días de anticipación a la publicación del acuerdo, resolución o sentencia de que se trate en el *Boletín Jurisdiccional*. Las notificaciones electrónicas a las partes se entenderán realizadas con la sola publicación en el *Boletín Jurisdiccional*, y con independencia del envío, cuando así proceda, de los avisos electrónicos. Los particulares y las autoridades, mientras no se haya realizado la notificación por *Boletín Jurisdiccional*, podrán apersonarse en el Tribunal para ser notificados personalmente. Una vez realizada la notificación por *Boletín Jurisdiccional*, las partes, cuando esto proceda, deberán acudir al Tribunal a recoger sus traslados de ley, en el entendido de que con o sin la entrega de los traslados, los plazos comenzarán a computarse a partir del día siguiente al en que surta efectos la notificación correspondiente. El actuario o el secretario de acuerdos, en todos los casos, previo levantamiento de razón, entregará los traslados de ley. La notificación surtirá sus efectos al tercer día hábil siguiente a aquél en que se haya realizado la publicación en el *Boletín Jurisdiccional* o al día hábil siguiente a aquél en que las partes sean notificadas personalmente en las instalaciones designadas por el tribunal, cuando así proceda, en términos de lo establecido por el artículo 67 de esta Ley. Dicho aviso deberá incluir el archivo electrónico que contenga el acuerdo y en el caso del emplazamiento, el escrito de demanda correspondiente.

lares positivas necesarias para evitar que el litigio quede sin materia o se cause un daño irreparable al actor, mismas que se otorgarán siempre y cuando no se afecte al interés social ni se contravengan normas de orden público y se cause con la ejecución del acto un daño o perjuicio irreparable al solicitante.

F) Ampliación de demanda y contestación de la ampliación

Formulada la contestación de demanda, el actor podrá ampliar su demanda dentro del plazo de 10 días hábiles siguientes a aquél en que surta efectos la notificación del acuerdo que admita a trámite la contestación de demanda, en aquellos casos en que se actualicen las causales previstas por el artículo 17, de la LFPCA.[1293] De igual manera, la contraparte contará con un plazo de 10 días siguientes a aquél en que surta efectos la notificación del acuerdo que admita la ampliación, para formular la contestación respectiva.

G) Pruebas

Las pruebas atraviesan por tres momentos procesales diferentes: el ofrecimiento, el desahogo y la valoración. En el JCAF, las pruebas deben de ofrecerse y exhibirse junto con la presentación de la demanda y no posteriormente, salvo que se trate de una prueba superveniente, es decir, sobre un hecho que ocurrió con posterioridad a la presentación de la demanda o que al momento de presentarla, no se tenía conocimiento de la misma. Únicamente en este caso se podrá presentar alguna prueba en cualquier momento hasta en tanto no se dicte sentencia.

Dentro del periodo probatorio, cada una de las pruebas se desahoga de manera específica. La prueba pericial se ofrece desde el escrito de demanda, donde deberá señalarse el nombre del perito, la materia, su domicilio y se exhibe el cuestionario. A través de un acuerdo, el magistrado instructor le requerirá a la parte promovente para que dentro del término de 10 días, contados a partir del día siguiente en que surta efectos dicho acuerdo, el perito acepte el cargo y proteste su legal desempeño. Una vez protestado el cargo y mediante acuerdo previo, el perito contará con 15 días, contados a partir del día siguiente en que surta efectos dicho acuerdo, para rendir y ratificar su dictamen. En caso de discrepancia entre los dictámenes presentados por los peritos de las partes, se designará a un perito tercero en discordia, mismo que será designado por la Sala de entre los que tenga adscritos.

Por su parte, de conformidad con lo establecido en el artículo 44 de la LFPCA, la prueba testimonial debe ofrecerse desde el escrito de demanda, donde se deberá señalar el nombre del testigo y acompañarse el cuestionario. Para su desahogo, se requerirá a la oferente para que presente a los testigos y cuando ésta manifieste no poder presentarlos, el Magistrado Instructor los citará para que comparezcan el día y hora que al efecto señale. De los testimonios se levantará acta pormenorizada y podrán serles formuladas por el magistrado o por las partes aquellas preguntas que estén en relación directa con los hechos controvertidos o persigan la aclaración de cualquier respuesta. Las autoridades rendirán testimonio por escrito.

1293 Artículo 17. Se podrá ampliar la demanda, dentro de los 10 días siguientes a aquél en que surta efectos la notificación del acuerdo que admita su contestación, en los casos siguientes:
I. Cuando se impugne una negativa ficta.
II. Contra el acto principal del que derive la resolución impugnada en la demanda, así como su notificación, cuando se den a conocer en la contestación.
III. En los casos previstos en el artículo anterior.
IV. Cuando con motivo de la contestación, se introduzcan cuestiones que, sin violar el primer párrafo del artículo 22, no sean conocidas por el actor al presentar la demanda.
V. Cuando la autoridad demandada plantee el sobreseimiento del juicio por extemporaneidad en la presentación de la demanda.

H) Alegatos

Los alegatos constituyen la exposición oral o escrita de los argumentos de las partes o de sus defensores, que tienen por objeto demostrar la eficacia de las pruebas rendidas y llevar al ánimo del juzgador la convicción de que los hechos en que basa la demanda o la contestación han quedado probados.[1294]

I) Cierre de instrucción

El magistrado instructor, habiendo concluido la sustanciación del juicio y no exista ninguna cuestión pendiente que impida su resolución, y habiendo otorgado a las partes término para formular sus alegatos, deberá declarar el cierre de instrucción del juicio.

J) Sentencia

Finalmente y de conformidad con el artículo 49 de la LFPCA, la sala regional deberá dictar sentencia por unanimidad o mayoría de votos de los magistrados integrantes de la sala, dentro de los cuarenta y cinco días siguientes a aquél en que haya quedado cerrada la instrucción en el juicio.[1295]

La sentencia podrá reconocer la validez de la resolución impugnada, declarar su nulidad o declarar su nulidad para efectos. Si la sentencia obliga a la autoridad a realizar un determinado acto o iniciar un procedimiento, deberá cumplirse en un plazo de cuatro meses contados a partir de que la sentencia quede firme. En el caso de que se interponga recurso, se suspenderá el efecto de la sentencia hasta que se dicte la resolución que ponga fin a la controversia.

K) Medios de impugnación de la sentencia

1. Juicio de amparo

El juicio de amparo es un medio de control de constitucionalidad por el que una persona acude ante un órgano judicial para reclamar un acto de un órgano del Estado o una ley, cuando considera que el mismo vulnera sus derechos fundamentales.

En nuestro sistema jurídico existen dos tipos de juicios de amparo, el directo y el indirecto. El amparo directo procede en contra de sentencias definitivas y resoluciones respecto de las cuales no procede algún recurso ordinario por el que puedan ser modificadas o revocadas. Por su parte, el amparo indirecto procede contra leyes federales, tratados internacionales, constituciones de las entidades federativas, reglamentos, decretos o acuerdos; actos u omisiones de autoridades distintas de los tribunales judiciales, administrativas o del trabajo; actos, omisiones o resoluciones provenientes de un procedimiento adminis-

1294 SCJN. Poder Judicial de la Federación. (2003). *Manual del justiciable, materia administrativa.* 1a. ed., México, p. 59.

1295 La Ley Federal de Procedimiento Contencioso Administrativo señala que:
Artículo 49.- La sentencia se pronunciará por unanimidad o mayoría de votos de los magistrados integrantes de la sala, dentro de los cuarenta y cinco días siguientes a aquél en que haya quedado cerrada la instrucción en el juicio. Para este efecto, el magistrado instructor formulará el proyecto respectivo dentro de los treinta días siguientes al cierre de instrucción. Para dictar resolución en los casos de sobreseimiento, por alguna de las causas previstas en el artículo 9o. de esta Ley, no será necesario que se hubiese cerrado la instrucción.
[...]
Artículo 52.- Si la sentencia obliga a la autoridad a realizar un determinado acto o iniciar un procedimiento, conforme a lo dispuesto en la fracción IV, deberá cumplirse en un plazo de cuatro meses tratándose del Juicio Ordinario o un mes tratándose del juicio sumario de conformidad con lo previsto en el artículo 58-14 de la presente Ley, contados a partir de que la sentencia quede firme.
[...]
En el caso de que se interponga recurso, se suspenderá el efecto de la sentencia hasta que se dicte la resolución que ponga fin a la controversia.

trativo seguido en forma de juicio (cuando la resolución sea definitiva o los actos sean de imposible reparación); actos de tribunales realizados fuera de juicio o después de concluido; actos de imposible reparación dentro de juicio; y actos dentro o fuera de juicio que afecten a personas extrañas.

El plazo para promover el juicio de amparo es de 15 días hábiles siguientes a aquél en que surta efectos la notificación del acto o de la resolución que se reclama, o aquél en que el quejoso haya tenido conocimiento o se ostente sabedor del acto reclamado o de su ejecución. Cuando se reclame una regla general autoaplicativa (cuando las obligaciones que impone la norma surgen de forma automática por su sola entrada en vigor), el plazo es de 30 días.

El amparo directo es resuelto por los tribunales colegiados de circuito en materia administrativa. Cuando el caso lo amerita, resuelve la Suprema Corte de Justicia de la Nación, mientras que el amparo indirecto es resuelto por los juzgados de distrito.

2. Recurso de Revisión

Es un recurso de índole procesal instancial en control de legalidad de procedencia excepcional a disposición de la autoridad demandada o demandante (tratándose del juicio de lesividad), por el cual se pueden revocar o modificar las sentencias definitivas dictadas en un juicio contencioso administrativo federal.

El plazo para promover el recurso de revisión es de 15 días hábiles siguientes a aquél en que surta efectos la notificación de la resolución o sentencia que se recurre. El recurso de revisión es resuelto por los tribunales colegiados de circuito en materia administrativa.

Juicio de resolución exclusiva de fondo

Gabriel López López

La voz "juicio de resolución exclusiva de fondo" constituye una modalidad especial del juicio contencioso administrativo federal, mismo cuya procedencia se encuentra limitada a controvertir la legalidad únicamente de aquellas resoluciones que deriven del ejercicio de las facultades de comprobación de que se encuentran investidas las autoridades fiscales y, particularmente, de las comúnmente conocidas como revisiones de escritorio y/o gabinete, visitas domiciliarias y revisiones electrónicas, no resultando procedente su instauración en contra de las resoluciones que recaigan a los procedimientos de protección de derechos, verificación, e imposición de sanciones.

Es una modalidad del juicio contencioso administrativo federal que se sustancia ante el Tribunal Federal de Justicia Administrativa (TFJA), por virtud de la cual, el actor opcionalmente somete a la jurisdicción de dicho órgano colegiado, el análisis de la legalidad de las determinaciones de créditos fiscales de las autoridades fiscales, alegando únicamente aspectos de fondo de dichas determinaciones, sin que exista la posibilidad de alegar aspectos formales, con el propósito de obtener una justicia completa y abreviar los tiempos de definición de las cuestiones controvertidas en dicha instancia.

Adicionalmente, el artículo 1-A de la Ley Federal de Procedimiento Contencioso Administrativo (LFPCA) previene que se entiende para efectos de dicha Ley como juicio de resolución exclusiva de fondo "el juicio contencioso administrativo federal en aquellos casos a los que se refiere el capítulo XII del Título II de esta Ley", mientras que el tercer párrafo del artículo 58-17 de la misma Ley caracteriza a este tipo de juicio como aquél en que "el demandante solo podrá hacer valer conceptos de impugnación que tengan

por objeto resolver exclusivamente sobre el fondo de la controversia que se plantea, sin que obste para ello que la resolución que se controvierta se encuentre motivada en el incumplimiento total o parcial de requisitos exclusivamente formales o de procedimiento establecidos en las disposiciones jurídicas aplicables; siempre que el demandante acredite que no se produjo omisión en el pago de contribuciones".

1. Antecedentes

Según se expresó en la exposición de motivos de la iniciativa de decreto por el que se reforman y adicionan diversas disposiciones de la LFPCA presentada por el titular del Ejecutivo Federal al Congreso de la Unión el 8 de septiembre de 2016 se estimó necesario crear una modalidad u opción de juicio en el que, a elección del gobernado, se analicen únicamente aspectos de fondo de las determinaciones de las autoridades fiscales sin que en este procedimiento se puedan alegar aspectos formales, lo que permitirá a los interesados elegir, de acuerdo con sus razonamientos, la modalidad del juicio que mayores probabilidades de defensa representen y, en su caso, abreviar los tiempos de definición de la situación controvertida.[1296]

Conforme al principio de oralidad, se busca simplificar el procedimiento y establecer una estrecha vinculación entre los jueces, las partes y los medios de prueba. No obstante, puede tener el inconveniente de mostrar equívocos a que pueden conducir eventuales deficiencias de memoria o de concentración en los jueces que asisten a las audiencias, particularmente cuando resulten ser prolongadas.

El principio de economía procesal, como derivado del principio de economía procesal, representa en su género el establecimiento de todas aquellas previsiones que tienden a la abreviación y simplificación del proceso, evitando que su irrazonable prolongación torne inoperante la tutela de los derechos e intereses comprometidos en él, para lo cual, se fijan normas destinadas a impedir la prolongación de los plazos y a eliminar trámites procesales superfluos u onerosos.

2. Sustanciación del procedimiento

2.1 Elección de la modalidad

Para la instauración de dicha modalidad, el actor debe pedir expresamente la elección de la misma, y el trámite y sustanciación del procedimiento contencioso administrativo se regirá de conformidad con las disposiciones contenidas en el capítulo XII de la LFPCA, resultando aplicables en lo no previsto en el mismo, las demás disposiciones que regulan el juicio contencioso administrativo federal. Aunado a ello, la modalidad referida se rige especialmente por los principios de oralidad y celeridad.

2.2 Procedencia de la modalidad

La materia que rige el juicio de resolución exclusiva de fondo se limita a la impugnación de las resoluciones determinantes de créditos fiscales que deriven del ejercicio de las facultades de comprobación previstas en el artículo 42, fracciones II (revisión de escritorio o gabinete), III (visita domiciliaria) o IX (revisión electrónica) del Código Fiscal de la Federación (CFF) y cuya cuantía exceda la cantidad de doscientas veces la Unidad de Medida y Actualización (UMA) elevada al año,[1297] vigente al momento de la resolución combatida.

1296 Cámara de diputados. (2016, septiembre 8). "Iniciativa de decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Procedimiento Contencioso Administrativo", en *Gaceta Parlamentaria*. Palacio Legislativo de San Lázaro. Año XIX. Número 4614-F Disponible en: gaceta.diputados.gob.mx/PDF/63/2016/sep/20160908-F.pdf.

1297 La Unidad de Medida y Actualización fue publicada por el INEGI en el *Diario Oficial de la Federación* el 10 de enero de 2018 y entró en vigor a partir del 1 de febrero de 2018. La UMA asciende a la cantidad de $80.60 pesos mexicanos. Información disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5510380&fecha=10/01/2018.

Tales requisitos han sido confirmados por la primera sección de la Sala Superior del TFJA en la tesis aislada VIII-P-1aS-310, cuyo rubro y texto dicen:

> SALA ESPECIALIZADA EN MATERIA DEL JUICIO DE RESOLUCIÓN EXCLUSIVA DE FONDO. ES COMPETENTE CUANDO SE ACTUALIZA LA CUANTÍA DEL ASUNTO.- De conformidad con lo establecido en el artículo 58-17 de la (LFPCA), para que una sala especializada en materia del juicio de resolución exclusiva de fondo, sea competente para conocer del juicio, además de versar únicamente sobre la impugnación de resoluciones definitivas que deriven del ejercicio de las facultades de comprobación a que se refiere el artículo 42, fracciones II, III o IX del Código Fiscal de la Federación, es un requisito de procedencia que la cuantía del asunto deba ser mayor a doscientas veces la Unidad de Medida y Actualización, elevada al año, vigente al momento de la emisión de la resolución impugnada (VIII-P-1aS-310).1298.

Adicionalmente, la modalidad referida resulta improcedente en aquellos casos en que se hubiese interpuesto un recurso administrativo en contra de las resoluciones determinantes referidas y dicho recurso hubiese sido desechado, sobreseído o se hubiese tenido por no presentado.

Finalmente, la tramitación del juicio de resolución exclusiva de fondo en ningún caso podrá efectuarse a través del juicio en la vía tradicional, sumaria o en línea y, habiéndose elegido la opción referida, el demandante no podrá variar su elección.

3. Características del juicio de resolución exclusiva de fondo

Como ha quedado identificado, la particularidad que identifica a la modalidad en estudio, implica que en la demanda inicial solo se formulen conceptos de impugnación que tengan por objeto resolver exclusivamente el fondo de la controversia que se plantea, entendiendo como tales aquéllos que, referidos al sujeto, objeto, base, tasa o tarifa de las obligaciones revisadas, tienda controvertir alguno de los siguientes supuestos:

a) Los hechos u omisiones calificados en la resolución impugnada como constitutivos de incumplimiento de las obligaciones revisadas.
b) La aplicación o interpretación de las normas involucradas.
c) Los efectos que haya atribuido la autoridad al incumplimiento total o parcial de requisitos formales o de procedimiento que impacten o trasciendan al fondo de la controversia.
d) La valoración o falta de apreciación de las pruebas relacionadas con los supuestos mencionados en los numerales que anteceden.

4. Requisitos de la demanda

Por lo que se refiere a los requisitos que debe contener la demanda de nulidad, el artículo 14 de la LFPCA dispone enunciativamente los requisitos que deberá contener el escrito inicial de demanda que se formule ante el TFJA. Tratándose del juicio de resolución exclusiva de fondo, adicionalmente deberán satisfacerse los siguientes presupuestos:

1. la manifestación expresa de que se opta por el juicio de resolución exclusiva de fondo;
2. la expresión breve y concreta de la controversia de fondo que se plantea, así como el señalamiento expreso de cuál es la propuesta de litis;
3. el señalamiento respecto al origen de la controversia, especificando si ésta deriva de la forma en que se apreciaron los hechos u omisiones revisados; de la interpre-

1298 Tesis VIII-P-1aS-310. *Revista del Tribunal Federal de Justicia Administrativa*. Octava época. Año III. No. 20, marzo de 2018, p. 156.

tación o aplicación de las normas involucradas; de los efectos que se atribuyeron al incumplimiento total, parcial o extemporáneo, de los requisitos formales o de procedimiento que impactan o trasciendan al fondo de la

4. controversia, o bien, si cualesquiera de los supuestos anteriores son coincidentes, y
5. los conceptos de impugnación que se hagan valer en cuanto al fondo del asunto.

Al escrito inicial de demanda se deberán adjuntar la resolución impugnada y su constancia de notificación, así como las pruebas que se ofrezcan, relacionándolas expresamente en su escrito de demanda con lo que se pretenda acreditar, incluyendo el dictamen pericial que, en su caso, se ofrezca.

Ante la omisión de alguno de los requisitos a que se ha hecho referencia, el magistrado instructor requerirá al demandante que lo subsane dentro del término de cinco días, bajo el apercibimiento que, de no hacerlo en tiempo, se desechará la demanda.

5. Análisis de la procedencia

Independientemente de la manifestación expresa del demandante de elegir la modalidad de juicio de resolución exclusiva de fondo, es tarea del magistrado instructor determinar la procedencia del juicio, tomando en consideración los siguientes aspectos:

a) analizará si se cumplen los requisitos de procedencia exigidos por la LFPCA para el juicio de resolución exclusiva de fondo;
b) en aquellos casos que habiéndose prevenido al actor para que subsanara alguno de los requisitos de la demanda, éste los cumpla, si el magistrado instructor advierte que los conceptos de impugnación planteados en la demanda incluyen argumentos de forma o de procedimiento, éstos se tendrán por no formulados y solo se atenderán aquellos argumentos que versen sobre el fondo de la controversia y
c) cuando el magistrado instructor advierta que en la demanda solo se plantean conceptos de impugnación relativos a cuestiones de forma o procedimiento, y no a cuestiones relativas al fondo de la controversia, ordenará la remisión de la demanda a la oficialía de partes común del TFJA para que lo ingrese como juicio en la vía tradicional, tomando en consideración la fecha de presentación de la demanda.

El juicio de resolución exclusiva de fondo no procederá en aquellos casos en que en la demanda se alegue que la resolución administrativa no fue notificada o que lo fue ilegalmente, siempre que se trate de las impugnables en el juicio contencioso administrativo federal.

6. Suspensión de la ejecución

En aquellos casos en que resulte procedente la vía intentada y en el momento en que se admita a trámite la demanda, se ordenará suspender de plano la ejecución de la resolución impugnada sin necesidad de que el demandante garantice el interés fiscal, misma que surtirá efectos hasta en tanto que se dicte la resolución que ponga fin al juicio exclusivo de fondo, sin perjuicio de los requisitos que para la suspensión establezcan las leyes que rijan los medios de impugnación que procedan contra la sentencia dictada en el mismo.

7. Recurso de reclamación

En aquellos casos en que el magistrado instructor determine que la demanda no cumple con los requisitos y, en consecuencia resuelve desecharla, procederá el recurso de reclamación, mismo que deberá presentarse ante el magistrado instructor en un plazo de 10

días contados a partir de que surta efectos la notificación del acuerdo de desechamiento, respecto del cual se ordenará correr traslado a la contraparte para que en el término de cinco días exprese lo que a su derecho convenga y sin más trámite la Sala lo resolverá de plano en un plazo de cinco días.

8. Ampliación de demanda

La ampliación de demanda en el juicio de resolución exclusiva de fondo procede únicamente en aquellos casos en que, con motivo de la contestación de demanda, se introduzcan cuestiones que, sin cambiar los fundamentos de derecho de la resolución impugnada, no sean conocidas por el actor al presentarla.

Dicha etapa deberá hacerse valer dentro del plazo de 10 días siguientes a aquél en que surta efectos la notificación del auto que tenga por presentada la contestación y en el escrito relativo, el actor deberá señalar con precisión cuál es la propuesta de litis de la controversia en la ampliación.

La autoridad demandada, al contestarla y, en su caso, la ampliación de demanda, deberá señalar si coincide o no con la propuesta de litis del juicio, expresando en este último caso, cuál es su propuesta.

9. Audiencia de fijación de litis

Una vez recibida la contestación de la demanda y, en su caso, la contestación a la ampliación de la misma, el magistrado instructor citará a las partes para audiencia de fijación de litis, la que se desahogará sin excepción de manera oral dentro de los 20 días siguientes a la recepción de la contestación respectiva.

El magistrado instructor expondrá de forma breve en qué consiste la controversia planteada por las partes, quienes manifestarán lo que a su derecho convenga, ajustándose a lo manifestado en la demanda, su ampliación o su contestación.

La audiencia de fijación de litis deberá ser desahogada, sin excepción, ante la presencia del magistrado instructor quien podrá auxiliarse del secretario de acuerdos para que levante acta circunstanciada de la diligencia.

Las partes podrán acudir personalmente o por conducto de sus autorizados legales. Los demás magistrados integrantes de la Sala podrán acudir a la audiencia de fijación de litis. Cuando estando debidamente notificadas las partes, en términos de los artículos 67 y 68 de la LFPCA, alguna no acuda a la audiencia de fijación de litis, ésta se llevará a cabo con la parte que esté presente.

Quedará al prudente arbitrio del magistrado instructor la regulación del tiempo que tengan las partes para exponer los motivos por los que estiman les asiste la razón, considerando estrictamente el principio de celeridad que rige esta vía.

Cuando alguna de las partes no acuda a la audiencia de fijación de litis se entenderá que consiente los términos en que la misma quedó fijada por el magistrado instructor, precluyendo además su derecho para formular cualquier alegato posterior en el juicio, ya sea en forma verbal o escrita.

En el caso de que se haya acordado procedente la atracción del juicio por la Sala Superior, el magistrado instructor reservará la celebración de la audiencia de fijación de litis, el desahogo de las pruebas que procedan y la formulación de los alegatos, a fin de que éstas se lleven a cabo ante el magistrado ponente que corresponda.

Una vez celebrada la audiencia de fijación de litis, el magistrado instructor notificará a las partes el acuerdo por el que se les otorgue el plazo de cinco días para formular sus alegatos, salvo en el caso del ejercicio de la facultad de atracción por parte de la Sala Superior del TFJA.

10. Audiencia privada

En aquellos casos en que durante la sustanciación del juicio de resolución exclusiva de fondo, alguna de las partes solicite una audiencia privada con el magistrado instructor o con alguno de los magistrados de la Sala Especializada, la misma deberá celebrarse invariablemente con la presencia de su contraparte; y solo podrá llevarse a cabo con la parte que audiencia, cuando estando debidamente notificadas las partes, alguna de ellas no acuda a la misma.

11. Pruebas admisibles

Tratándose de la modalidad del juicio de resolución exclusiva de fondo, únicamente serán admisibles aquellas pruebas que hubiesen sido previamente ofrecidas y exhibidas en:

a) el procedimiento de fiscalización del que derive la resolución impugnada;

b) el procedimiento de acuerdos conclusivos regulado en el CFF, o

c) el recurso administrativo correspondiente.

12. Prueba pericial

A diferencia del juicio contencioso administrativo que se tramita en la vía tradicional, tratándose de la modalidad del juicio de resolución exclusiva de fondo, en el caso de las pruebas periciales, al formular su demanda o contestación o la ampliación de ambas, las partes deben exhibir el documento que contenga el dictamen correspondiente.

Al respecto, el magistrado instructor tiene la más amplia facultad para valorar no solo la idoneidad de los dictámenes exhibidos, atendiendo a la litis fijada en la audiencia correspondiente, sino, además, la idoneidad del perito que lo rinde.

En caso de que lo considere necesario, el magistrado instructor podrá citar a los peritos que rindieron los dictámenes a fin de que, en una audiencia especial, misma que se desahogará en forma oral, respondan las dudas o cuestionamientos que aquél les formule; para lo cual, las partes deberán ser notificadas en un plazo mínimo de cinco días anteriores a la fecha fijada para dicha audiencia, debiendo levantarse un acta por el secretario de acuerdos.

Las partes podrán acudir a la audiencia a que se refiere el párrafo anterior para efectos de ampliar el cuestionario respecto del cual se rindió el dictamen pericial, así como para formular repreguntas al perito.

En aquellos casos en que los dictámenes de las partes no proporcionen al magistrado instructor elementos de convicción suficientes o si los mismos resultan discrepantes o contradictorios, y una vez celebrada la audiencia referida el magistrado instructor podrá designar a un perito tercero, mismo cuyo dictamen deberá versar exclusivamente sobre los puntos de discrepancia de los dictámenes de los peritos de las partes.

13. Cierre de instrucción

Celebrada la audiencia de fijación de litis, desahogadas las pruebas que procedan y formulados los alegatos, quedará cerrada la instrucción del juicio de resolución exclusiva de fondo sin necesidad de declaratoria expresa.

A partir del día siguiente a aquél en que quede cerrada la instrucción, comenzará a computarse el plazo de 45 días para que los magistrados de la Sala dicten la sentencia.

14. La sentencia

De conformidad con lo establecido en el artículo 58-27, de la LFPCA, la declaratoria de nulidad de una resolución impugnada, procede cuando se encuentre acreditado que:

a) los hechos u omisiones que dieron origen a la controversia no se hubiesen producido;
b) los hechos u omisiones que dieron origen a la controversia hubiesen sido apreciados por la autoridad en forma indebida;
c) las normas involucradas hubiesen sido incorrectamente interpretadas o mal aplicadas en la resolución impugnada, o
d) los efectos que la autoridad demandada hubiese atribuido al incumplimiento total, parcial o extemporáneo, de requisitos formales o de procedimiento a cargo del demandante resulten excesivos o desproporcionados por no haberse producido las hipótesis de causación de las contribuciones determinadas.

Asimismo, en cuanto a los efectos de la sentencia, el artículo 58-28, de la LFPCA, previene que ésta podrá:

I. reconocer la validez de la resolución impugnada;
II. declarar la nulidad de la resolución impugnada;
III. en los casos en que la sentencia implique una modificación a la cuantía de la resolución administrativa impugnada, la Sala Regional Especializada deberá precisar el monto, el alcance y los términos de la misma para su cumplimiento. Tratándose de sanciones, cuando el TFJA aprecie que la sanción es excesiva porque no se motivó adecuadamente o no se dieron los hechos agravantes de la sanción, deberá reducir el importe de la sanción apreciando libremente las circunstancias que dieron lugar a la misma;
IV. declarar la nulidad de la resolución impugnada y además:
    a) reconocer al actor la existencia de un derecho subjetivo y condenar al cumplimiento de la obligación correlativa;
    b) otorgar o restituir al actor en el goce de los derechos afectados;
    c) declarar la nulidad del acto o resolución administrativa de carácter general, caso en que cesarán los efectos de los actos de ejecución que afectan al demandante, inclusive el primer acto de aplicación que hubiese impugnado. La declaración de nulidad no tendrá otros efectos para el demandante, salvo lo previsto por las leyes de la materia de que se trate, y
    d) reconocer la existencia de un derecho subjetivo y condenar al ente público federal al pago de una indemnización por los daños y perjuicios causados por sus servidores públicos.
V. las salas regionales especializadas en materia del juicio de resolución exclusiva de fondo podrán apartarse de los precedentes establecidos por el Pleno o las secciones, siempre que en la sentencia expresen las razones por las que se apartan de los mismos, debiendo enviar al presidente del TFJA copia de la sentencia.

15. Recurso de revisión

Finalmente, resta señalar que en aquellos casos en que la sentencia recaída a un juicio de resolución exclusiva de fondo, no favorezca a la autoridad demandada, ésta podrá inter-

poner el recurso de revisión previsto por la LFPCA, para lo cual, deberán satisfacerse los requisitos de procedencia establecidos en el artículo 63 de dicha Ley.

Juicio por la vía sumaria

Gabriel López López

La voz "juicio por la vía sumaria" es un concepto procesal particular que puede parecer poco relacionado con la materia de protección de datos. La realidad es que es un concepto elemental cuando se busca determinar la procedencia del medio de defensa idóneo para controvertir las resoluciones del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en particular aquellas que recaen en el Procedimiento de Imposición de Sanciones (Pisan), precisamente por la cuantía a la que pueden ascender las multas que dicho Instituto imponga, por lo que su consulta es importante para los practicantes y titulares de datos personales.

Se trata de un procedimiento contencioso administrativo federal que surge con la finalidad de garantizar y agilizar el alcance a la justicia administrativa, de tal manera que ésta sea más rápida y expedita. La principal característica de este juicio es la abreviación y reducción significativa de los plazos del juicio contencioso administrativo que se sustancia por la vía tradicional.

Su tramitación se encuentra regulada en el capítulo XI, denominado "Del Juicio por la Vía Sumaria", dentro de los artículos 58-1 a 58-15 de la Ley Federal de Procedimiento Contencioso Administrativo (LFPCA), derivado de una reforma efectuada a la LFPCA publicada en el DOF el 10 de diciembre de 2010, misma que inició su vigencia el 7 de agosto de 2011.

De acuerdo con lo establecido por el artículo 1-A, fracción XIV, de la LFPCA, el juicio por la vía sumaria se define como "el juicio contencioso administrativo federal en aquellos casos a los que se refiere el capítulo XI del título II de la LFPCA".[1299]

1. Características

Entre los elementos esenciales que caracterizan al juicio contencioso administrativo federal en la vía sumaria, destacan los siguientes:

a) la instrucción y resolución del juicio serán facultad exclusiva del magistrado instructor, es decir, la ley faculta y le encomienda no solo la tramitación de todo el procedimiento, sino también el dictado de la sentencia definitiva, en contraposición a la tramitación de las demás modalidades en las que predomina un principio de colegialidad y

b) la simplificación y reducción en los términos procesales. Todos los plazos del procedimiento se abrevian notablemente, con la finalidad de mejorar y acelerar la impartición de justicia en nuestro país y reducir la carga de trabajo del Tribunal Federal de Justicia Administrativa (TFJA).

1299 Artículo 1-A. Para los efectos de esta Ley se entenderá por:
[...]
XIV. Juicio en la vía sumaria: el juicio contencioso administrativo federal en aquellos casos a los que se refiere el capítulo XI del título II de esta Ley.
[...]
Artículo 58-1. El juicio contencioso administrativo federal se tramitará y resolverá en la vía sumaria, de conformidad con las disposiciones específicas que para su simplificación y abreviación se establecen en este capítulo y, en lo no previsto, se aplicarán las demás disposiciones de esta Ley.

2. Sustanciación del procedimiento

A. Procedencia y tramitación

A diferencia del juicio en línea, los supuestos para la procedencia del juicio por la vía sumaria no son de carácter optativo en relación con el tradicional, sino obligatorio para las partes. Y para ello deben de actualizarse alguna de las hipótesis normativas contenidas en el primer párrafo del artículo 58-2 de la LFPCA.

Sirve de apoyo a lo anterior la tesis jurisprudencial de la Décima época en materia administrativa, que dice:

> Juicio contencioso administrativo federal en la vía sumaria. Su tramitación no es optativa en relación con el ordinario. El juicio contencioso administrativo federal en la vía sumaria se instauró con el objeto de agilizar los procesos cuyo conocimiento corresponde al Tribunal Federal de Justicia Fiscal y Administrativa; sin embargo, su tramitación no es optativa en relación con el juicio ordinario, ya que el artículo 14 de la Ley Federal de Procedimiento Contencioso Administrativo establece que dentro de la demanda deberá indicarse que el juicio se sustanciará en la vía sumaria y, en caso de omisión, el magistrado instructor lo tramitará así en los supuestos en que proceda, de conformidad con el título II, capítulo XI, del propio ordenamiento, por lo que no queda a elección del actor determinar la vía en la cual deba tramitarse su demanda de nulidad, y como los supuestos de procedencia del juicio sumario están claramente establecidos en la mencionada ley, el magistrado instructor únicamente debe limitarse a aplicarla, concretamente, en sus artículos 14 y 58-2; sin que pueda ir más allá de lo que la ley lo faculta, al grado de ser quien decida la vía en que ha de tramitarse un juicio (II.1o.A. J/1 [10a.]).1300

De acuerdo con lo anterior, y de conformidad con el primer párrafo del artículo 58-2, el juicio por la vía sumaria procede cuando se impugnen resoluciones definitivas cuyo importe no exceda de 15 veces el salario mínimo general vigente en el Distrito Federal (hoy Ciudad de México) elevado al año al momento de su emisión, siempre que se trate de alguna de las resoluciones definitivas siguientes:

I. las dictadas por autoridades fiscales federales y organismos fiscales autónomos, por las que se fije en cantidad líquida un crédito fiscal;

II. las que únicamente impongan multas o sanciones, pecuniaria o restitutoria, por infracción a las normas administrativas federales;

III. las que exijan el pago de créditos fiscales, cuando el monto de los exigibles no exceda el importe citado;

IV. las que requieran el pago de una póliza de fianza o de una garantía que hubiere sido otorgada a favor de la Federación, de organismos fiscales autónomos o de otras entidades paraestatales de aquélla, o

V. las recaídas a un recurso administrativo, cuando la recurrida sea alguna de las consideradas en los incisos anteriores y el importe de esta última, no exceda el antes señalado.

Para la procedencia de la vía sumaria es indiscutible que debe tratarse de una resolución definitiva, sin embargo, la LFPCA no define qué debe entenderse por resolución definitiva, por lo que para suplir esa deficiencia es necesario acudir al antepenúltimo párrafo del artículo 3 de la Ley Orgánica del Tribunal Federal de Justicia Administrativa (LOTFJA).[1301]

1300 Tesis: II.1o.A. J/1 (10a.). *Semanario Judicial de la Federación y su Gaceta.* Décima época. Tomo III, octubre 2013, p. 1677.

1301 Artículo 3. El Tribunal conocerá de los juicios que se promuevan contra las resoluciones definitivas, actos administrativos y procedimientos que se indican a continuación:
I. Los decretos y acuerdos de carácter general, diversos a los reglamentos, cuando sean autoaplicativos o cuando el interesado los controvierta con motivo de su primer acto de aplicación.

Por otra parte, el artículo 58-2 de la LFPCA establece dos hipótesis para determinar la cuantía:

a) en los casos de los incisos I), II) y V) solo se considerará el crédito principal sin accesorios ni actualizaciones, y
b) cuando en un mismo acto se contenga más de una resolución de las mencionadas anteriormente, no se acumulará el monto de cada una de ellas para efectos de determinar la procedencia del juicio sumario.

De lo anterior, es importante resaltar que el monto total de una determinación fiscal emitida por la autoridad competente puede estar constituido por diversos factores accesorios al crédito fiscal, como lo son los recargos y las actualizaciones. Por lo que al momento de

---

II. Las dictadas por autoridades fiscales federales y organismos fiscales autónomos, en que se determine la existencia de una obligación fiscal, se fije en cantidad líquida o se den las bases para su liquidación.
III. Las que nieguen la devolución de un ingreso de los regulados por el Código Fiscal de la Federación, indebidamente percibido por el Estado o cuya devolución proceda de conformidad con las leyes fiscales.
IV. Las que impongan multas por infracción a las normas administrativas federales.
V. Las que causen un agravio en materia fiscal distinto al que se refieren las fracciones anteriores.
VI. Las que nieguen o reduzcan las pensiones y demás prestaciones sociales que concedan las leyes en favor de los miembros del Ejército, de la Fuerza Aérea y de la Armada nacional o de sus familiares o derechohabientes con cargo a la Dirección de Pensiones Militares o al erario federal, así como las que establezcan obligaciones a cargo de las mismas personas, de acuerdo con las leyes que otorgan dichas prestaciones.
Cuando para fundar su demanda el interesado afirme que le corresponde un mayor número de años de servicio que los reconocidos por la autoridad respectiva, que debió ser retirado con grado superior al que consigne la resolución impugnada o que su situación militar sea diversa de la que le fue reconocida por la Secretaría de la Defensa Nacional o de Marina, según el caso; o cuando se versen cuestiones de jerarquía, antigüedad en el grado o tiempo de servicios militares, las sentencias del Tribunal solo tendrán efectos en cuanto a la determinación de la cuantía de la prestación pecuniaria que a los propios militares corresponda, o a las bases para su depuración.
VII. Las que se dicten en materia de pensiones civiles, sea con cargo al erario federal o al Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado.
VIII. Las que se originen por fallos en licitaciones públicas y la interpretación y cumplimiento de contratos públicos, de obra pública, adquisiciones, arrendamientos y servicios celebrados por las dependencias y entidades de la administración pública federal centralizada y paraestatal, y las empresas productivas del Estado; así como, las que estén bajo responsabilidad de los entes públicos federales cuando las leyes señalen expresamente la competencia del tribunal.
IX. Las que nieguen la indemnización por responsabilidad patrimonial del Estado, declaren improcedente su reclamación o cuando habiéndola otorgado no satisfaga al reclamante. También, las que por repetición, impongan la obligación a los servidores públicos de resarcir al Estado el pago correspondiente a la indemnización, en los términos de la ley de la materia.
X. Las que requieran el pago de garantías a favor de la Federación, las entidades federativas o los municipios, así como de sus entidades paraestatales y las empresas productivas del Estado.
XI. Las que traten las materias señaladas en el artículo 94 de la Ley de Comercio Exterior;
XII. Las dictadas por las autoridades administrativas que pongan fin a un procedimiento administrativo, a una instancia o resuelvan un expediente, en los términos de la Ley Federal de Procedimiento Administrativo;
XIII. Las que resuelvan los recursos administrativos en contra de las resoluciones que se indican en las demás fracciones de este artículo;
XIV. Las que se funden en un tratado o acuerdo internacional para evitar la doble tributación o en materia comercial, suscritos por México, o cuando el demandante haga valer como concepto de impugnación que no se haya aplicado en su favor alguno de los referidos tratados o acuerdos;
XV. Las que se configuren por negativa ficta en las materias señaladas en este artículo, por el transcurso del plazo que señalen el Código Fiscal de la Federación, la Ley Federal de Procedimiento Administrativo o las disposiciones aplicables o, en su defecto, en el plazo de tres meses, así como las que nieguen la expedición de la constancia de haberse configurado la resolución positiva ficta, cuando ésta se encuentre prevista por la ley que rija a dichas materias.
No será aplicable lo dispuesto en el párrafo anterior en todos aquellos casos en los que se pudiere afectar el derecho de un tercero, reconocido en un registro o anotación ante autoridad administrativa;
XVI. Las resoluciones definitivas por las que se impongan sanciones administrativas a los servidores públicos en términos de la legislación aplicable, así como contra las que decidan los recursos administrativos previstos en dichos ordenamientos, además de los órganos constitucionales autónomos;
XVII. Las resoluciones de la Contraloría General del Instituto Nacional Electoral que impongan sanciones administrativas no graves, en términos de la Ley General de Instituciones y Procedimientos Electorales;
XVIII. Las sanciones y demás resoluciones emitidas por la Auditoría Superior de la Federación, en términos de la Ley de Fiscalización y Rendición de Cuentas de la Federación, y
XIX. Las señaladas en esta y otras leyes como competencia del Tribunal.
Para los efectos del primer párrafo de este artículo, las resoluciones se considerarán definitivas cuando no admitan recurso administrativo o cuando la interposición de éste sea optativa

determinar la procedencia del juicio por la vía sumaria, deberá tomarse en consideración el importe histórico, y no así la sumatoria total.

3. Causales de improcedencia

En ese mismo sentido, tiene igual importancia señalar cuáles son las causales de improcedencia de esta vía, y que se encuentran comprendidas en el primer párrafo del artículo 58-3 de la LFPCA:

I. cuando no se actualice alguno de los supuestos previstos en el artículo 58-2;

II. simultáneamente a la impugnación de una resolución de aquellas a que se refiere el artículo 58-2, se controvierta una regla administrativa de carácter general;

III. se trate de sanciones económicas en materia de responsabilidades administrativas de los servidores públicos o de sanciones por responsabilidad resarcitoria;

IV. se trate de multas por infracciones a las normas en materia de propiedad intelectual;

V. se trate de resoluciones que además de imponer una multa o sanción pecuniaria, incluyan alguna otra carga u obligación, o

VI. el oferente de una prueba testimonial no pueda presentar a las personas señaladas como testigos.

En contra de la resolución que declare improcedente el juicio por la vía sumaria, procede la interposición del recurso de reclamación, dentro de los cinco días siguientes a aquél en que surta efectos la notificación respectiva.

4. La demanda

La demanda deberá presentarse ante la sala regional competente, dentro de los 30 días siguientes a aquél en que surta efectos la notificación de la resolución impugnada.[1302] En ese mismo escrito, el promovente deberá manifestar su voluntad que el juicio se tramite en la vía sumaria, cumpliendo con los requisitos que para el juicio ordinario establece la LFPCA.

En caso de desconocer la vía para la tramitación de la demanda o interponerla de manera incorrecta, la LFPCA prevé que opere la suplencia de la queja, en el sentido de que no se generará el desechamiento, improcedencia o sobreseimiento de la demanda, sino que operará una reconducción del juicio en la vía correcta, debiendo realizar las regularizaciones correctas. Esto operará en cualquier etapa del procedimiento, siempre y cuando no haya quedado cerrada la instrucción del juicio o se haya dictado sentencia.

5. Contestación de demanda y ampliación de demanda

Admitida la demanda, se emplazará al demandado, y en su caso al tercero, para que en el plazo de 15 días hábiles el primero conteste la demanda y el segundo se apersone a juicio. En el mismo auto, se fijará la fecha para el cierre de instrucción, el cuál no deberá de exceder de los 60 días siguientes a la admisión de demanda.

En el juicio por la vía sumaria, al igual que en el juicio ordinario, se puede ampliar la demanda cuando se actualicen los supuestos a los que se refiere el artículo 17 de la LFPCA, con la salvedad que dicha ampliación deberá hacerse en un plazo de cinco días hábiles siguientes a la notificación de la contestación de demanda. La parte demandada o en su

1302 Artículo 58-2. [...]
La demanda deberá presentarse dentro de los treinta días siguientes a aquél en que surta efectos la notificación de la resolución impugnada, de conformidad con las disposiciones de esta Ley ante la sala regional competente.

caso el tercero, contarán con el mismo plazo a partir de que surta efectos la notificación de su traslado, para contestar y apersonarse, según corresponda.[1303]

6. Pruebas

En cuanto al ofrecimiento, desahogo y valoración de las pruebas, serán aplicables las reglas contenidas en el capítulo V del título II, de la LFPCA, salvo por lo que se refiere a la prueba testimonial, la cual solo podrá ser admitida cuando el oferente se comprometa a presentar a sus testigos en el día y hora señalados para la diligencia.

La prueba pericial se desahogará conforme a las mismas reglas que se prevén para el juicio en la vía tradicional u ordinaria, con la diferencia de que todos los plazos serán de tres días; con excepción del que corresponde a la rendición y ratificación del dictamen, que será de cinco días; estos actos procesales deberá realizarlos cada perito en un único acto ante el magistrado instructor. Cuando proceda la designación de un perito tercero, ésta correrá a cargo del propio magistrado. El desahogo de las pruebas deberá hacerse a más tardar 10 días antes de la fecha prevista para el cierre de instrucción.[1304]

7. Suspensión de la ejecución y medidas cautelares

En el artículo 58-9 de la LFPCA se prevé que las medidas cautelares se tramitarán conforme a las reglas generales establecidas en el capítulo III, del título II de la LFPCA, y el magistrado instructor estará facultado para resolverlas de manera provisional o definitiva. En contra de la determinación que decida adoptar dicho juzgador procederá el recurso de reclamación ante la sala regional competente en la que se encuentre radicado el juicio.

8. Alegatos

Los alegatos podrán ser presentados por las partes del juicio en cualquier momento siempre y cuando ello ocurra con anterioridad a la fecha señalada para el cierre de la instrucción.[1305]

9. Cierre de instrucción

En la fecha fijada para el cierre de instrucción, el magistrado instructor deberá verificar si el expediente se encuentra debidamente integrado, de ser así, declarará cerrada la instrucción y en caso contrario, deberá fijar una nueva fecha dentro de un plazo máximo de 10 días. Una vez que el expediente se encuentre debidamente integrado, el magistrado ins-

1303 Artículo 58-6. El actor podrá ampliar la demanda, en los casos a que se refiere el artículo 17 de esta Ley, en un plazo de cinco días siguientes a aquél en que surta efectos la notificación del auto que tenga por presentada la contestación. La parte demandada o en su caso el tercero, contestarán la ampliación a la demanda, en el plazo de cinco días siguientes a que surta efectos la notificación de su traslado.

1304 Artículo 58-5. El magistrado proveerá la correcta integración del juicio, mediante el desahogo oportuno de las pruebas, a más tardar diez días antes de la fecha prevista para el cierre de instrucción. Serán aplicables, en lo conducente, las reglas contenidas en el capítulo V de este título, salvo por lo que se refiere a la prueba testimonial, la cual solo podrá ser admitida cuando el oferente se comprometa a presentar a sus testigos en el día y hora señalados para la diligencia. Por lo que toca a la prueba pericial, ésta se desahogará en los términos que prevé el artículo 43 de esta Ley, con la salvedad de que todos los plazos serán de tres días, salvo el que corresponde a la rendición y ratificación del dictamen, el cual será de cinco días, en el entendido de que cada perito deberá hacerlo en un solo acto ante el magistrado instructor. Cuando proceda la designación de un perito tercero, ésta correrá a cargo del propio magistrado.
[...]
Artículo 58-9. Las medidas cautelares se tramitarán conforme a las reglas generales establecidas en el capítulo III de esta Ley. El magistrado instructor estará facultado para decretar la resolución provisional o definitiva que corresponda a las medidas cautelares. Contra la resolución del magistrado instructor dictada conforme al párrafo anterior procederá el recurso de reclamación ante la sala regional en la que se encuentre radicado el juicio.
[...]

1305 Artículo 58-11. Las partes podrán presentar sus alegatos antes de la fecha señalada para el cierre de la instrucción.

tructor otorgará a las partes un término de tres días para que formulen alegatos, y fenecido dicho plazo, con o sin la presentación de dichos alegatos quedará cerrada la instrucción.[1306]

10. Sentencia

Decretado el cierre de instrucción, el magistrado instructor deberá realizar una sentencia definitiva dentro de los 10 días siguientes salvo que:

I. se haya ejercido la facultad de atracción, o

II. se actualice la competencia especial de la Sala Superior

Casos en los que serán resueltos por el Pleno o la sección respectiva, con los plazos y las reglas correspondientes para tal efecto.[1307]

Como se aprecia, la diferencia esencial existente entre el juicio por la vía sumaria y el juicio en la vía tradicional es la notable reducción de los plazos dentro del procedimiento, amén de la instrucción y resolución del mismo solo por uno de los magistrados integrantes de la sala regional. A fin de tener claridad sobre los plazos anteriormente referidos, se muestra la siguiente comparativa:

	Juicio por la vía sumaria	Juicio por la vía tradicional
Presentación de la demanda	30 días	30 días
Contestación de la demanda	15 días	30 días
Ampliación de demanda	5 días	10 días
Contestación a la ampliación de demanda	5 días	10 días
Alegatos	3 días	5 días
Sentencia	10 días	45 días
Total de días	68 días	130 días

1306 Artículo 58-12. En la fecha fijada para el cierre de instrucción el magistrado instructor procederá a verificar si el expediente se encuentra debidamente integrado, supuesto en el que deberá declarar cerrada la instrucción; en caso contrario, fijará nueva fecha para el cierre de instrucción, dentro de un plazo máximo de 10 días. En el momento en que el magistrado instructor advierta que el expediente se encuentra debidamente integrado, otorgará a las partes un término de tres días para que formulen alegatos, quedando cerrada la instrucción una vez fenecido dicho plazo, con o sin la presentación de dichos alegatos.
[...]

1307 Artículo 58-13. Una vez cerrada la instrucción, el magistrado pronunciará sentencia dentro de los 10 días siguientes, salvo en los casos en que se haya ejercido facultad de atracción, o se actualice la competencia especial de la Sala Superior, supuestos en los cuales, deberá estarse a lo dispuesto por el artículo 48, fracción II, inciso d, de esta Ley, a efecto de que sea resuelto por el Pleno o la sección respectiva, con los plazos y las reglas correspondientes a ello, de conformidad con esta Ley.

Juicio de amparo

Jean Claude Tron Petit

La voz "juicio de amparo" es indiscutiblemente relevante para la materia de protección de datos, pues se trata de un concepto relacionado con los medios de impugnación admitidos por la normatividad de datos personales en los sectores público y privado y que procede frente a las resoluciones emitidas por los órganos garantes en materia de protección de datos. Es decir, al ser un medio de control de la legalidad de las actuaciones de la autoridad garante funge como un mecanismo idóneo para la defensa de los derechos humanos y su efectiva tutela administrativa y jurisdiccional.

1. Definición

Es un medio para el control de la constitucionalidad, convencionalidad y legalidad de las normas, actos u omisiones de la autoridad o de particulares que transgredan derechos humanos fundamentales y sus garantías, contemplados por el orden jurídico en favor de los gobernados.

2. Antecedentes históricos

El primer antecedente en derecho mexicano se da con la constitución de Yucatán, del 31 de marzo de 1841, ya que recogió un proyecto, en el artículo 53, elaborado por Manuel Crescencio Rejón, que expresaba textualmente: "Corresponde a este tribunal [la Corte Suprema de Justicia] reunido: 1º Amparar en el goce de sus derechos a los que pidan su protección contra las providencias del gobernador o ejecutivo reunido, cuando en ellas se hubiese infringido el Código Fundamental o las leyes, limitándose en ambos casos a reparar el agravio en la parte que procediere".

Así, se habló en el derecho legislado, del amparo decretado por órganos jurisdiccionales para combatir agravios contra derechos, en el proyecto de Rejón y en la constitución yucateca de 1841.

Tiempo después este juicio se plasmó, con la colaboración de Mariano Otero, en el congreso constituyente, en el artículo 25 del acta constitutiva y de reformas de 1847, con lo que se estableció el juicio de amparo a nivel federal, para después incluirse en la Constitución Federal de los Estados Unidos Mexicanos de 1857.

Este juicio fue reglamentado posteriormente en la Ley Orgánica Constitucional sobre el Juicio de Amparo, del 20 de enero de 1869, siendo ésta una aportación de México al mundo; y 60 años más tarde, en la Constitución Política de los Estados Unidos Mexicanos de 1917.

Actualmente se encuentra regulado a través de la nueva Ley de Amparo, publicada en el *Diario Oficial de la Federación* el 2 de abril de 2013, la cual es reglamentaria de los artículos 103 y 107 constitucionales.

3. Contexto

Esencia: es el más popular, reconocido y efectivo medio de control en México, tanto de constitucionalidad como de legalidad en tanto que protege a las personas frente a actos u omisiones de los poderes públicos o, en ciertos casos, de particulares que actúan como autoridad; cuando sus derechos o intereses son violados por normas generales, actos u omisiones de autoridad o de particulares que actúan como autoridad.

Por tanto, su tutela se extiende a todo el orden jurídico nacional, incluyendo, desde la protección de los derechos fundamentales de fuente nacional e internacional, hasta otros

derechos de menor entidad. Sus bases están en la Constitución, artículos 103 y 107 primordialmente, en la Ley de Amparo y la abundante jurisprudencia de tribunales.

Utilidad en México: hay poca confianza en decisiones de los poderes judiciales de los estados y falta de incentivos para que los actos de autoridad, en general, se ajusten a principios jurídicos; todo ello conlleva a que el juicio de amparo sea visto como una instancia ordinaria para enmendar tales ilegalidades y deficiencias.

Jerarquía: con el fin de entender la posición normativa del juicio de amparo, es preciso establecer que existen órganos de gobierno pertenecientes a los siguientes niveles:

a) constitucional

   Constituyente permanente y Poder Judicial Federal en cuanto ejerce actos de control constitucional

b) federal

c) estatal

d) municipal

De esta relación, es fácil advertir que el juez de amparo ocupa un lugar de predominio frente a la mayoría de las autoridades constituidas, en tanto que deben circunscribir su conducta a los mandatos constitucionales y es el encargado de verificar el control de sus actuaciones.

4. Breve explicación del concepto

El antecedente del juicio de amparo son los principios de 1) supremacía constitucional, 2) Estado de derecho o legalidad, 3) división de poderes y 4) prevalencia de los derechos humanos y sus garantías; los cuales, al poder ser violados requieren se restaure el orden constitucional que pueda haber sido quebrantado, enmienda que se logra a través de la tramitación del juicio de amparo.

Es importante destacar que la parte dogmática de la Constitución ahora se conforma con el parámetro de control de regularidad constitucional o parámetro de control de regularidad constitucional, previsto expresamente en su artículo 1, lo que incluye derechos fundamentales expresamente estipulados en la Carta, así como los derechos humanos consignados en tratados de los que el Estado mexicano sea parte y sus garantías.

Conviene precisar que los derechos humanos son la versión internacional de los derechos fundamentales, lo que claramente explica Diez Picazo:

> En los usos lingüísticos establecidos, la expresión «derechos humanos» designa normalmente aquellos derechos que, refiriéndose a valores básicos, están declarados por tratados internacionales. La diferencia entre derechos fundamentales y derechos humanos estribaría, así, en el ordenamiento que los reconoce y protege: interno, en el caso de los derechos fundamentales; internacional, en el caso de los derechos humanos.

Otra explicación de la expresión constitucional es dejar en evidencia que ahora la Carta Magna asume como referente crucial de tutela y eficacia, los valores morales que inspiran a los derechos humanos previstos en tratados ratificados, atribuibles también a los derechos fundamentales previstos en la Constitución.

Merced a la adopción de valores esenciales, la Constitución reconoce la existencia de los derechos humanos previstos en tratados y de los fundamentales, lo que, en conjunto, constituye el denominado parámetro de control de regularidad constitucional.[1308]

1308 La técnica del bloque de constitucionalidad parte de concebir la Constitución como un texto abierto, caracterizado por la presencia de diversas cláusulas mediante las cuales se operan reenvíos que permiten ampliar el espectro de normas jurídicas que deben ser respetadas por el legislador. Corte Constitucional de Colombia, Sentencia c-355/06 de 10 de mayo de 2006.

La expresión "garantías" alude a muy variadas instituciones cuyo objetivo es tutelar y dar efectividad a los derechos fundamentales. El mismo Diez Picazo, dice:

La expresión "garantías de los derechos fundamentales" carece de un significado técnico-jurídico preciso. Hace referencia al conjunto de medios que el ordenamiento prevé para la protección, tutela o salvaguardia de los derechos fundamentales. Se trata de un conjunto heterogéneo, pues abarca tanto procedimientos de distinta índole como requisitos sustantivos, cuyo rasgo común es precisamente estar dirigidos a asegurar la observancia y la efectividad de los derechos fundamentales. Sin embargo, la citada expresión puede inducir a confusión, dada su proximidad lingüística con los términos "garantía institucional" y "garantía del contenido esencial"; términos que, en cambio, sí poseen un significado técnico-jurídico preciso.

Por otro lado, dentro de la categoría de garantías de los derechos fundamentales suelen incluirse previsiones normativas de muy distinta naturaleza y en particular, es frecuente mezclar normas sustantivas y normas procesales. De aquí que, a la hora de hacer un catálogo de las garantías de los derechos fundamentales sea conveniente distinguir ambos planos: sustantivo y procesal.

Como un instrumento de efectividad, la Constitución otorga para ese fin una serie de garantías.

El juicio de amparo se ha revelado como una de las ramas del derecho procesal constitucional que, a la par de las controversias constitucionales, las acciones de inconstitucionalidad y la materia electoral, es un medio jurídico de protección, tutela y preservación de la constitucionalidad y al mismo tiempo es:

a) el medio de defensa del gobernado, y

b) el remedio frente a los actos inconstitucionales del gobernante.

Recientemente, la jurisprudencia ha configurado la institución del control de convencionalidad, en virtud del cual, cualquier juez estatal deberá interpretar toda norma conforme al parámetro de control de regularidad constitucional o no aplicar disposiciones contrarias a los objetos y fines constitucionales. Esto equivale al control difuso que desde tiempo atrás se utiliza en otros países, implicando un control de constitucionalidad en la decisión de problemas concretos y contingentes. Una conclusión trascendente es que ahora todos los jueces en cualquiera de sus actuaciones son garantes de la Constitución. Desaparece así la distinción entre jueces de legalidad y de constitucionalidad.

La complejidad actual del juicio de amparo se da a partir de que implica una trilogía estructural en tanto que satisface las funciones de:

1) un recurso o proceso de legitimidad constitucional y convencional de las normas generales. Amparo contra normas y amparo soberanía;

2) amparar y tutelar genéricamente los derechos humanos y las garantías constitucionales. Amparo contra actos administrativos, y

3) un recurso de casación. Amparo jurisdiccional

5. Medio de control constitucional y convencional

La Constitución es la fuente del juicio de amparo (porque es creado por ella) y al mismo tiempo su meta, porque la finalidad es lograr el imperio y vigencia de sus mandatos. Ahora se adicionan como objeto de tutela las normas previstas en tratados que prevean derechos humanos.

Los derechos humanos fundamentales[1309] y sus garantías tienen una secuela y concatenación peculiar. Siguiendo algunas ideas de Ferrajoli[1310] pueden construirse los siguientes conceptos:

- Derechos subjetivos fundamentales —individuales, colectivos o *erga omnes*— entendidos como expectativas positivas[1311] o negativas[1312] de la titularidad de los gobernados atribuidas por la norma.
- Los deberes correspondientes o garantías primarias, consistentes en obligaciones[1313] o prohibiciones[1314] a cargo del Estado o una clase.
- Garantías secundarias, entendidas como obligaciones de aplicar la sanción o declarar la nulidad de las violaciones a los deberes aludidos y restituir en el disfrute de los derechos.

Es así que la doctrina constitucional ha diseñado varios medios para salvaguardar la supremacía constitucional. En México prevalece como medio fundamental el juicio de amparo, dicho en otras palabras, es el código procesal para conseguir la vigencia de los derechos fundamentales. Sin embargo, coadyuvan algunas otras instituciones como las controversias constitucionales y las acciones de inconstitucionalidad, previstas en el artículo 105, fracciones I y II de la Carta Magna, el ombudsman (Comisión Nacional y Estatales de Derechos Humanos), el juicio político, la desaparición de poderes, los procesos electorales, etcétera.

Se ha dicho que el juicio de amparo es el guardián del derecho y la Constitución, lo que no es totalmente exacto; en tanto no tiene como objeto la defensa y protección de todo el orden constitucional ni el control integral de todos los actos, omisiones o causas que lo contravengan.[1315] En efecto, su alcance protector o de tutela se concreta, básica, preferente y esencialmente, en la constitucionalidad[1316] de los actos de autoridad que violen derechos humanos, fundamentales y las garantías concedidas en favor y relación con tales derechos. Por tanto, más que un medio de defensa y protección de la Constitución, es apenas el medio —más efectivo— para el control de la constitucionalidad y convencionalidad de los actos que transgredan derechos humanos, fundamentales y sus garantías que el orden jurídico contemple en favor de los gobernados.

Es en este contexto que se inscribe el juicio de amparo como instrumento procesal de protección jurídica para declarar, en su caso, la inconstitucionalidad de los actos que por esa vía se reclamen y obtener la restitución en el disfrute de los derechos. Como tal, en un aspecto estático, permite constatar y confrontar un acto de autoridad frente a la Constitución y convenciones sobre derechos humanos, atendiendo a sus valores, principios y reglas para decidir así su conformidad u oposición.

1309 En lo subsecuente, la referencia a derechos fundamentales, se entiende referida a los previstos en la Constitución, no obstante, el texto expreso.

1310 Ferrajoli, L. (1999). *Derechos y Garantías*. Madrid. Editorial Trotta, p. 59.

1311 Significa que el Estado o un particular vinculado debe desplegar una conducta de hacer o acciones positivas de protección u otorgar alguna prestación al titular, *v. gr.* impartir justicia.

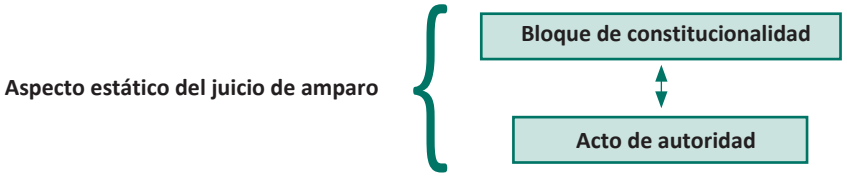
1312 Implica que el obligado no debe causar lesiones o afectaciones al bien tutelado, evitando o prohibiendo ciertas acciones que transgredan derechos, *v. gr.* libertad de expresión.

1313 Acciones positivas o prestaciones.

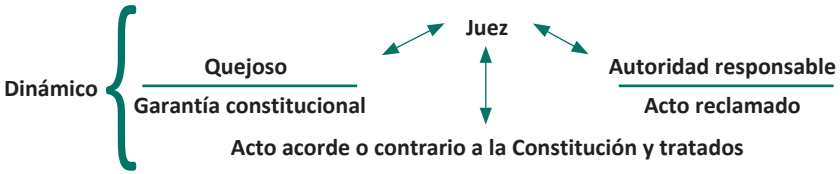
1314 Acciones negativas o abstenciones.

1315 Un ejemplo pueden ser las políticas públicas indebida o incorrectamente atendidas, aspecto que solo podrá ser cuestionado cuando afecte el mínimo vital de los derechos económicos, sociales y culturales, por poner una referencia. Además, la violación a un derecho subjetivo o interés legítimo debe trascender en un agravio para que proceda el juicio.

1316 Debe agregarse la legalidad en tanto es un bien constitucionalmente protegido, además de la convencionalidad.



Pero al juicio de amparo, como proceso que es, le caracteriza ser dialéctico y de naturaleza contradictorio, basado en el debido proceso legal, atento lo cual, se desarrolla en una dinámica donde el quejoso plantea una pretensión de inconstitucionalidad de un acto ante un juez, responsabilizando de ello a una autoridad por un acto u omisión, quien debe responder a tal imputación, todo lo cual se da en un contexto dinámico.



Y es precisamente dentro de este aspecto que se desarrolla el juicio de amparo y los incidentes que le son propios.

El nuevo artículo primero constitucional

La reforma constitucional al artículo 1 constituye un cambio de paradigma en el orden jurídico nacional,[1317] pues ahora estipula que todas las personas gozarán de los derechos humanos reconocidos en la propia norma fundamental y en los tratados internacionales de los que México sea parte. Esto implicó la constitucionalización del contenido —esencialmente moral— de los tratados, lo que conforma un parámetro de control de regularidad constitucional en la medida que los convenios internacionales, en cuanto disponen derechos humanos, pasan a formar parte del contenido de la Constitución, integrando una unidad exigible o imponible a todos los actos u omisiones que puedan ser lesivos de derechos fundamentales.[1318]

De este modo, todas las autoridades del país, dentro del ámbito de sus competencias, se encuentran obligadas a velar, no sólo por los derechos humanos contenidos en los instrumentos internacionales firmados por el Estado mexicano, sino también por los derechos fundamentales contenidos en la Constitución Federal.

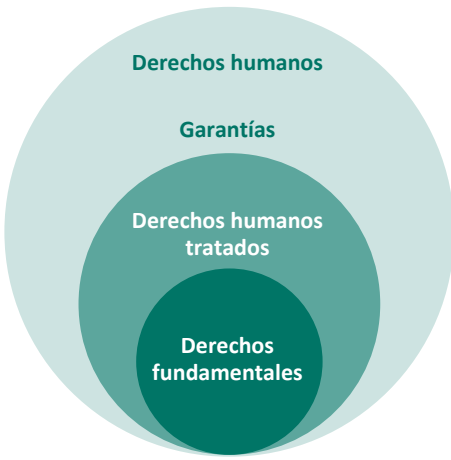
1317 Artículo 1. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.
Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.

1318 No debe perderse de vista la distinción entre el concepto de "derecho humano" y el de "derecho fundamental" que realiza Pérez Luño, considerando que los derechos humanos son la fuente de los derechos fundamentales en los siguientes términos: "Los derechos humanos suelen venir entendidos como un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas, las cuales deben ser reconocidas positivamente por los ordenamientos jurídicos a nivel nacional e internacional. En tanto que con la noción de los derechos fundamentales se tiende a aludir a aquellos derechos humanos garantizados por el ordenamiento jurídico positivo, en la mayor parte de los casos en su normativa constitucional, y que suelen gozar de una tutela reforzada". Citado por Carbonell,

Sin embargo, para sostener esa tesis es menester argumentarla. En efecto, una lectura aislada y fuera de contexto del primer párrafo del artículo 1 constitucional, pudiera llevar a un caos connotativo y a cuestionar la idea propuesta. El texto de la norma es el siguiente:

> Artículo 1. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.[1319]

Lo que sucede es que el legislador privilegió la alusión a "derechos humanos" para dejar en claro que ahora se contempla en el ordenamiento positivo, un parámetro o bloque, que reconoce la dimensión moral de los derechos, aunque solo en lo concerniente a los que aparecen previstos en los tratados que México haya suscrito. Es así que podemos hablar de derechos humanos en un sentido lato e ilimitado,[1320] concepto que no estaría expresamente tutelado, sin embargo dentro de ese universo hallamos un sector que si está protegido al grado de estar dotado de garantías; estos son, los derechos humanos recogidos en los tratados y cuando éstos o algunos otros, diversos pero análogos, aparecen estipulados expresamente en el texto constitucional, hablaríamos de derechos fundamentales. Estas ideas se reflejan en el grafico siguiente:



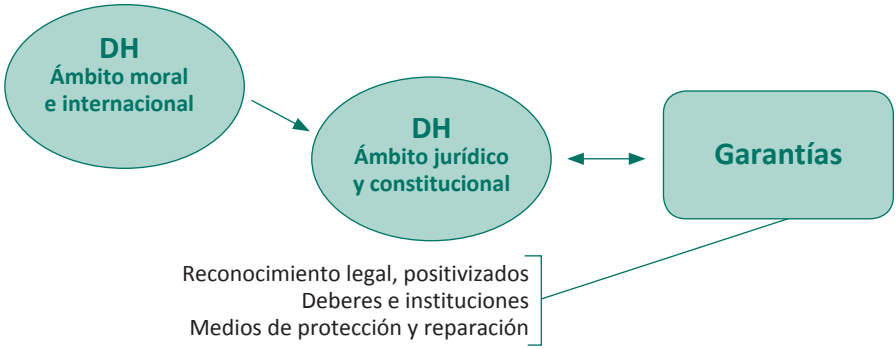
Paralelamente, Diez Picazo, sostiene que la esencia en ambos tipos de derechos, son los valores básicos, declarados en tratados, convenios o constitución. A su vez, son la base y condiciones mínimas de todo orden jurídico.

"En los usos lingüísticos establecidos, la expresión 'derechos humanos' designa normalmente aquellos derechos que, refiriéndose a valores básicos, están declarados por tratados internacionales. La diferencia entre derechos fundamentales y derechos humanos estribaría, así, en el ordenamiento que los reconoce y protege: interno, en el caso de los derechos fundamentales; internacional, en el caso de los derechos humanos. Dicho esto, el problema es si entre los derechos fundamentales y los derechos humanos hay separación o comunicación. A favor de la idea de que no se trata de compartimentos estancos militan dos factores ya conocidos: la tendencial identidad de valores protegidos, y la creciente internacionalización de la protección de los derechos. Ello es particularmente claro en el ámbito regional europeo, donde hay una aplicación capilar, cada día más intensa, del Convenio Europeo de Derechos Humanos. De aquí que, al menos en Europa, lo más correcto sea afirmar que unos mismos derechos son protegidos por distintos ordenamientos (internacional, comunitario, interno); ordenamientos que, por perseguir unos mismos fines en un mismo espacio, están llamados a colaborar. Esta conclusión, por lo demás, es inevitable en España, donde el artículo 10.2 de la constitución española CE obliga a interpretar las normas constitucionales sobre derechos fundamentales «de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España" (2003:34)

1319 CPEUM.

1320 Donde prima la naturaleza, finalidad y justificación moral.

Esta secuela puede ser vista tal como lo denota el esquema siguiente:



Complementariamente, en un segundo párrafo incorpora la obligación de interpretar esos derechos a modo de obtener el máximo beneficio y privilegia el principio pro persona, al momento de definir o establecer la tutela de los derechos humanos o fundamentales. El objetivo es adoptar el alcance y la interpretación más amplia y favorable a las normas que proclaman derechos y la más reducida a las que prevén límites y restricciones.

Lo anterior denota la intención del constituyente permanente de ampliar el rango de cobertura del sistema jurídico nacional al derecho internacional de los derechos humanos[1321] y a la perspectiva moral de los derechos fundamentales, lo cual implica necesariamente la renuncia a las ideologías positivistas duras, caracterizadas por formalismos rígidos; en cambio, se adopta una visión incluyente en la que se persiga como fin último enaltecer la libertad, dignidad e igualdad del hombre en cualesquiera de sus actividades.

El resultado formal es que la actual procedencia del juicio de amparo puede ser mucho más amplia que la tutela del orden constitucional, abarcando e incluyendo al convencional.

> Artículo 1º. El juicio de amparo tiene por objeto resolver toda controversia que se suscite:
>
> I. por normas generales, actos u omisiones de autoridad que violen los derechos humanos reconocidos y las garantías otorgadas para su protección por la Constitución Política de los Estados Unidos Mexicanos, así como por los tratados internacionales de los que el Estado mexicano sea parte,
>
> II. por normas generales, actos u omisiones de la autoridad federal que vulneren o restrinjan la soberanía de los Estados o la esfera de competencias del Distrito Federal, siempre y cuando se violen los derechos humanos reconocidos y las garantías otorgadas para su protección por la Constitución Política de los Estados Unidos Mexicanos, y
>
> III. por normas generales, actos u omisiones de las autoridades de los estados o del Distrito Federal, que invadan la esfera de competencia de la autoridad federal, siempre y cuando se violen los derechos humanos reconocidos y las garantías otorgadas por la Constitución Política de los Estados Unidos Mexicanos.

6. Control de legalidad

Los artículos 14, 16 y 31 constitucionales han erigido a la categoría de un derecho humano y garantía al principio de legalidad, incorporando a la teleología del juicio de amparo el control de ésta, a través de incluir como materia del contencioso constitucional a los conceptos de:

1321 En lo subsecuente DIDH.

a) exacta aplicación de la ley penal
b) correcta aplicación de la ley en las sentencias
c) legalidad *in genere*, *lato sensu*
d) legalidad tributaria

El amparo es en la actualidad:

a) un juicio constitucional respecto de normas generales y actos genéricos de autoridad.
b) un juicio o recurso extraordinario de legalidad (especialmente el directo) que preserva incluso la debida o exacta aplicación de leyes secundarias. Algunos consideran que hace las veces del recurso de casación.

Integra así, en un solo procedimiento, todos los medios de que puede disponer el gobernador para defenderse de cualquier acto de autoridad (sean leyes, actos de autoridad administrativa o sentencias judiciales) susceptibles de violar la Constitución.

El amparo a diferencia de:

a) el *habeas corpus* anglosajón;
b) el recurso de "exceso de poder" francés, los *writs* norteamericanos y
c) la casación, es superior a todos ellos ya que los engloba, por lo que son medios parciales que solo en su conjunto equivalen al amparo mexicano.

Sin embargo, el juicio constitucional no tuvo esta cobertura desde un principio.

En efecto, Vallarta en 1869 proscribió el amparo en negocios judiciales porque:

a) vulnera la soberanía judicial de los estados y
b) sobrecarga las funciones de la Suprema Corte.

Sin embargo, Carranza, en 1916,[1322] señaló que:

> El pueblo mexicano está ya tan acostumbrado al amparo en los juicios civiles, para librarse de las arbitrariedades de los jueces, que [...] sería no solo injusto sino impolítico, privarlo ahora de tal recurso, estimando que bastará limitarlo únicamente a los casos de verdadera y positiva necesidad, dándole un procedimiento fácil y expedito para que sea efectivo [...].

La diversidad de finalidades o amplitud de espectro que el juicio de garantías persigue es lo que determina su naturaleza y condiciones o modalidades multívocas y *sui generis*.

En efecto, el juicio de garantías puede perseguir variadas finalidades, lo cual resulta determinante de su naturaleza y, en concreto, de las condiciones o modalidades que le imprimen. Fix Zamudio[1323] comenta sobre el particular lo siguiente:

> El juicio de amparo mexicano ha llegado a adquirir en la actualidad una estructura jurídica sumamente compleja, que bajo su aparente unidad comprende varios instrumentos procesales, que, si bien poseen ciertos principios generales comunes, cada uno de ellos tiene aspectos peculiares de carácter autónomo, ... En consecuencia, el juicio de amparo mexicano debemos considerarlo como una federación de instrumentos procesales, cada uno de los cuales posee una función tutelar específica, que a su vez determina una serie de aspectos peculiares que no pueden comprenderse sino por conducto de su análisis autónomo.

En efecto, en el amparo mexicano podemos descubrir cinco funciones diversas, ya que puede utilizarse para la tutela de la libertad personal; para combatir las leyes inconstitucio-

1322 Rabasa, E. (1978). *El artículo 14 y el juicio constitucional*. México. Editorial Porrúa, p. XVII.

1323 Fix, H. (1993). *Ensayos sobre el derecho de amparo*. México. UNAM- IIJ., primera edición, p.30.

nales; como medio de impugnación de las sentencias; para reclamar los actos y resoluciones de la administración activa, y finalmente para proteger los derechos sociales de los campesinos sometidos al régimen de la reforma agraria.

Por lo tanto, es posible afirmar que los objetivos teleológicos actuales del juicio de amparo son:

a) el control de la Constitución y
b) la protección del gobernado frente al poder público en cuanto tutela la legalidad en sentido amplio y absoluto.

El sistema jurisdiccional de control constitucional que actualmente recoge y prescribe la Constitución de 1917 se caracteriza porque:

a) la preservación de la Constitución se encomienda a un órgano judicial con facultades expresas para otorgarla;
b) la petición de una sentencia de inconstitucionalidad incumbe a cualquier gobernado que haya sufrido un agravio;
c) ante el órgano de control se sustancia un procedimiento contencioso, y
d) las declaraciones de inconstitucionalidad solo tienen efectos en relación con el peticionario, no son *erga omnes*. (Ahora ya matizado por el interés legítimo colectivo, según lo ha determinado la Primera Sala de la Suprema Corte de Justicia de la Nación).

A partir de 1995 el artículo 105 constitucional establece en favor de ciertos órganos estatales y partidos políticos una novedosa acción de inconstitucionalidad en contra de leyes y con efectos generales.

Esta amplitud y versatilidad del juicio de garantías y otros análogos, lo ha hecho complejo en el ámbito procesal, lo que se traduce en una abundancia de formalidades que trascienden en múltiples incidentes y un intrincado sistema, a veces no muy uniforme ni sistemático.

7. Principios comunes a juicios y actuaciones

Tanto la doctrina —a partir del iusnaturalismo racionalista—, como la jurisprudencia y las leyes, han definido —algunas veces con una ideología política y otras por razones de método y técnicas— ciertos principios que, además, son características propias y esenciales del proceso judicial, entre los que destacan:

• ***Imparcialidad:*** La paz jurídica requiere que todos renuncien a la autodefensa y busquen su derecho (real o supuesto) ante los tribunales, en atinada expresión de Larenz:

Es un elemento fundamental y *sine qua non* de todo juicio, consiste en que la posición del juez debe ser independiente de los intereses contradictorios de las partes y órganos.

Pero tal independencia debe incluir factores de la persona que puedan implicar prejuicios "subliminales" que hasta el propio juez desconoce, en tanto que su propia formación y personalidad constituyen un determinismo que incide sobre la independencia de pensamiento de quien juzga. Comenta el autor citado que: "Para juzgar jurídicamente los asuntos hay que contemplarlos desde ángulos diferentes y sin emoción, las respuestas se demuestran después de pensarlas despacio y que lo mejor es seguir cuestionándose las cosas".

En este sentido conviene citar a Perelman cuando afirma que el juez debe ser imparcial pero subjetivo pues en ningún momento deja de ser persona incidida y condicionada por los intereses sociales, porque detrás de la fachada de la argumentación jurídica subyace la personalidad del juez.

La imparcialidad es un concepto indefinido y subjetivo que no puede concebirse ni operar de manera absoluta. En ocasiones la propia ley lo conmina a suplir deficiencias de los conceptos de violación o allegar oficiosamente pruebas del quejoso, además que la personalidad, esquemas y formación de cualquier juez pueden inclinarlo a tomar partido por una de las partes, sobre todo cuando resulta evidente una injusticia. Además, al momento de tomar una decisión, el juez toma partido y, tan lo hace, que después debe cuidar el cabal cumplimiento de la sentencia en perjuicio del perdedor. En ese sentido podría ser más propio hablar de una neutralidad durante la instrucción, de manera que permita, con equilibrio, que las partes propongan su acción y defensas con igualdad de oportunidades.

De suyo, hay factores de objetivación como la formación jurídica y el papel jurídico y social que desempeña, lo que obliga al juez a oír diferentes puntos de vista ya fundamentar la decisión.[1324]

El juez Barak, presidente de la Suprema Corte de Justicia de Israel,[1325] dice que un juez "debe ser capaz de examinarse así mismo desde afuera. Debe ser capaz de analizarse, criticarse y ejercer autocontrol". Beverly McLachlin[1326] considera se requiere una buena dosis tanto de modestia para aceptarla disciplina del caso, determinante de lo que debe decidirse específicamente y ser sensible a las consecuencias, como de introspección para reconocer y confrontar la propia subjetividad para impedir que interfiera con la voluntad decisoria; es reconocer los prejuicios y neutralizar su efecto, y es de esa manera que la conciencia tiene un efecto antiséptico sobre los aludidos prejuicios.

Por tanto, es indispensable invertir en la formación intelectual y ética de los jueces que deben estar dotados de una vocación de servicio, sentido común y hasta pasión por resolver las controversias de una manera adecuada, equitativa e integral. Esta cualidad y peculiaridad de los procesos está plasmada y ordenada en el artículo 17 constitucional, el reto es conseguirlo. En este sentido la tesis siguiente:

> IMPARCIALIDAD. CONTENIDO DEL PRINCIPIO PREVISTO EN EL ARTÍCULO 17 CONSTITUCIONAL. El principio de imparcialidad que consagra el artículo 17 constitucional, es una condición esencial que debe revestir a los juzgadores que tienen a su cargo el ejercicio de la función jurisdiccional, la cual consiste en el deber que tienen de ser ajenos o extraños a los intereses de las partes en controversia y de dirigir y resolver el juicio sin favorecer indebidamente a ninguna de ellas. Así, el referido principio debe entenderse en dos dimensiones: a) la subjetiva, que es la relativa a las condiciones personales del juzgador, misma que en buena medida se traduce en los impedimentos que pudieran existir en los negocios de que conozca y b) la objetiva, que se refiere a las condiciones normativas respecto de las cuales debe resolver el juzgador, es decir, los presupuestos de ley que deben ser aplicados por el juez al analizar un caso y resolverlo en un determinado sentido. Por lo tanto, si por un lado, la norma reclamada no prevé ningún supuesto que imponga al juzgador una condición personal que le obligue a fallar en un determinado sentido, y por el otro, tampoco se le impone ninguna obligación para que el juzgador actúe en un determinado sentido a partir de lo resuelto en una diversa resolución, es claro que no se atenta contra el contenido de las dos dimensiones que integran el principio de imparcialidad garantizado en la Constitución Federal. 160309. 1a./J. 1/2012 (9a.). Primera Sala. Décima época. Semanario Judicial de la Federación y su Gaceta. Libro V, febrero de 2012, Pág. 460.

• ***Igualdad de las partes:*** las partes deben tener los mismos derechos, posibilidades y cargas de manera que no haya privilegios, debe regir la igualdad de los ciudadanos ante la ley. Sin

1324 Brusiin, Otto, citado por Kart Larenz, *op. cit*., p. 184.

1325 Citado por McLachlin, B. (2002). *Ser juez en una democracia constitucional*. México. Colección Discursos, número 28. Suprema Corte de Justicia de la Nación, p.28.

1326 Citado por McLachlin, B. (2002). *Ser juez en una democracia constitucional*. México. Colección Discursos, número 28. Suprema Corte de Justicia de la Nación, pp. 23 y 26.

embargo, las partes no son siempre iguales o, bien, como en el caso del juicio de garantías, existen valores que se deben tutelar en vinculación con lo que establece la Constitución. Es así que encontramos, cada día, más principios legales y jurisprudenciales atinentes a esta finalidad de equilibrar lo que no está en condiciones de paridad, creando tareas al juez para lograr el predominio de las garantías; una igualdad legal y genérica, asociada de una práctica específica al caso concreto que sea pauta de una decisión justa, es la gran finalidad.

Ejemplos de las medidas legales o tutelas privilegiadas son la suplencia de los conceptos de violación o agravios en los supuestos donde está tasada su aplicación (materias laboral o penal); y de las jurisprudenciales, como son las facultades del juez para subsanar o corregir defectos en que hayan incurrido las partes e incluso que les instruya en temas y aspectos necesarios para encauzar debidamente el proceso. En la etapa de ejecución de las sentencias, es cada día más típico y usual este enfoque.

• ***Expeditez:*** la solución de conflictos debe ser sencilla, accesible y rápida. Por tanto, el acceso a los órganos jurisdiccionales y la supresión de obstáculos y limitaciones que no encaucen razonablemente el derecho de acción son principios que se deducen del artículo 17 constitucional.

Los laberintos y trampas procesales, formalidades irracionales y supuestos análogos deben desterrarse. Así lo proclamaba, desde tiempo atrás, el entonces magistrado Guillermo Guzmán Orozco en célebres tesis jurisprudenciales.

Montero Aroca[1327] propone: el fomento de la ejecución material de las medidas cautelares, la oralidad, suprimir formalismos inútiles, evitar recursos meramente dilatorios, criticando las medidas genéricas de aceleración basadas en suprimir trámites y abreviar plazos porque suponen, en muchos casos, la minoración de garantías fundamentales. En la etapa cautelar, el adelanto provisional del derecho cuestionado está resultando significativamente importante en el derecho europeo, fundado en la apariencia del buen derecho.

La racionalización y simplificación del sistema procesal debe provenir del legislador, sin embargo, dado el divorcio entre la *praxis* legislativa y la jurisdiccional, los jueces, en todo el mundo, han debido concebir principios y reglas conducentes a falta de disposiciones oportunas para dar congruencia, sentido práctico y eficacia a los grandes valores y principios que el orden legal establece con el fin de hacerlos operativos en el caso concreto.

• ***Eficacia:*** La facultad jurisdiccional, esencialmente, es componer un diferendo o controversia mediante el *ius dicere* diciendo el derecho. Consecuencia de ello y colofón necesario es la plena ejecución de las resoluciones, para lo cual, las leyes procesales deben proveer lo conducente y necesario y, de no hacerlo, deberán disponerlo los principios jurisprudenciales, así se entiende el mandato el mandato del artículo 17, párrafo segundo, constitucional. Por tanto, es importante la implementación práctica de medidas y soluciones conducentes a hacer realidad este anhelo del constituyente y del pueblo, y no que los juicios o sentencias favorables sean meras quimeras o sentencias de papel. En este tema es importante aplicar la inteligencia judicial para sortear y hacer realidad una verdadera ejecución de justicia que el desarrollo y avance democrático requieren.

No hay que olvidar, independientemente de lo previsto en los códigos procesales, que el orden jurídico nacional se compone también con lo previsto en tratados y, en ese sentido, la Convención Americana sobre Derechos Humanos, adoptada en la ciudad de San José de Costa Rica, en su artículo 25, punto 1, inciso c establece lo siguiente:

1327 Montero, J. et al. (1994). *Derecho Jurisdiccional, I parte general*. Barcelona. José María Bosch, editor, pp. 320 y 321.

1. Toda persona tiene derecho a un recurso sencillo y rápido o a cualquier otro recurso efectivo ante los jueces o tribunales competentes, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución, la ley o la presente convención, aun cuando tal violación sea cometida por personas que actúen en ejercicio de sus funciones oficiales.

[...]

c) a garantizar el cumplimiento, por las autoridades competentes, de toda decisión en que se haya estimado procedente el recurso.

• ***Contradicción o audiencia:*** la solución del juicio implica, para una de las partes, un acto de privación, atento lo cual, nadie puede ser condenado sin ser oído y vencido en juicio, destacando como valor fundamental el de defensa real o material. Lo anterior implica ser citado, informado del contenido de los elementos o materiales de hecho y de derecho que puedan influir en la resolución judicial, brindando así transparencia de lo debatido y aportado al proceso, con la oportunidad de probar y alegar a fin de concluir con el dictado de una resolución que ponga fin al debate. En este sentido resulta ilustrativo citar el criterio jurisprudencial siguiente:

AUDIENCIA. CÓMO SE INTEGRA ESTA GARANTÍA. De entre las diversas garantías de seguridad jurídica que contiene el segundo párrafo del artículo 14 constitucional destaca, por su primordial importancia, la de audiencia previa. Este mandamiento superior, cuya esencia se traduce en una garantía de seguridad jurídica para los gobernados, impone la ineludible obligación a cargo de las autoridades para que, de manera previa al dictado de un acto de privación, cumplan con una serie de formalidades esenciales, necesarias para oír en defensa a los afectados. Dichas formalidades y su observancia, a las que se unen, además, las relativas a la garantía de legalidad contenida en el texto del primer párrafo del artículo 16 constitucional, se constituyen como elementos fundamentales útiles para demostrar a los afectados por un acto de autoridad, que la resolución que los agravia no se dicta de un modo arbitrario y anárquico sino, por el contrario, en estricta observancia del marco jurídico que la rige. Así, con arreglo a tales imperativos, todo procedimiento o juicio ha de estar supeditado a que en su desarrollo se observen, ineludiblemente, distintas etapas que configuran la garantía formal de audiencia a favor de los gobernados, a saber, que el afectado tenga conocimiento de la iniciación del procedimiento, así como de la cuestión que habrá de ser objeto de debate y de las consecuencias que se producirán con el resultado de dicho trámite; que se le otorgue la posibilidad de presentar sus defensas a través de la organización de un sistema de comprobación tal, que quien sostenga una cosa tenga oportunidad de demostrarla, y quien estime lo contrario, cuente a su vez con el derecho de acreditar sus excepciones; que cuando se agote dicha etapa probatoria se dé oportunidad de formular las alegaciones correspondientes y, finalmente, que el procedimiento iniciado concluya con una resolución que decida sobre las cuestiones debatidas, fijando con claridad el tiempo y forma de ser cumplidas. 1012296. 1009. Tribunales Colegiados de Circuito. Novena época. Apéndice 1917-septiembre 2011. Tomo I. Constitucional 3. Derechos Fundamentales Segunda Parte - TCC Octava Sección - Garantías del inculpado y del reo, Pág. 2359.

Conviene añadir que la decisión puede apoyarse en fundamentos que aporte el tribunal de amparo, *motu proprio*, en casos de suplencia en razón de los principios *iura novit curia* y *da mihi factum, babo tibi jus*.

• ***Seguridad jurídica y formalidades esenciales (debido proceso legal):*** es consecuencia y complemento del derecho de audiencia, es necesaria la erradicación de la discrecionalidad del juez y el justiciable debe estar en condiciones de predecir y saber exactamente los actos que debe realizar y las cargas que comporta el ser parte. Ello implica sujetar y subordinar el proceso a una serie de formas que son el precio de la seguridad, como lo planteó Montesquieu, al grado de que el juez no es más que la boca de la ley y tiene proscrita la discrecionalidad. Sin embargo, una postura irrazonable provoca un derecho formulario en

que la "aparente seguridad" derivada del culto a las formas, conduce a injusticias y provoca el entorpecimiento, dilación y rezago en el quehacer judicial. Por tanto, los formalismos no deben ser llevados a extremos en los que no se subordinen y hasta se disocien de los principios que los han creado, ya que formalismos y dogmatismos irrazonables son antitéticos con la rapidez y eficacia que debe caracterizar siempre al juicio de amparo.

• ***Dinámico y dialéctico:*** la esencia de todo proceso es el debate de (cuando menos dos) sujetos parciales en posiciones contrapuestas ante un juez imparcial. Es así que, en lo general, se da una demanda (tesis) seguida de una contestación o informe justificado (antítesis) determinantes de un conflicto o controversia, que será resuelto a través de una decisión o sentencia (síntesis). Este acontecer ocurre dentro de un procedimiento dinámico y complejo donde las partes interactúan accionando y reaccionando recíprocamente de manera continua en cada una de las etapas procesales. La contradicción es, así, un eficaz instrumento técnico y dispositivo psicológico para garantizar la aplicación exacta de la ley y la imparcialidad del juez, incluyendo la mejor defensa de las partes y del interés público en la justicia.

• ***Dispositivo:*** es un principio del juicio de amparo conocido también como de instancia de parte agraviada, lo que proscribe la oficialidad del ejercicio de la acción y subsecuentes actuaciones, dicho en otras palabras, es la disposición del objeto del proceso.[1328] Sin embargo, poco a poco se va matizando este principio, especialmente en el caso del señalamiento complementario de actos reclamados y autoridades responsables, instancias para obtener el cumplimiento de sentencias; supuestos, entre otros, orientados a una impartición de justicia e integración procesal despojada de formalismos y requisitos draconianos. Otro caso donde puede llegar a sustituirse la voluntad específica de las partes en aras de privilegiar el interés social es la facultad de la Suprema Corte de Justicia para disponer el cumplimiento sustituto de una sentencia o declararla cumplida por razones supervenientes que lo aconsejen, artículo 107, fracción XVI, párrafo segundo, constitucional y tesis respectivas.

Complementario y derivado de este principio, tenemos el de aportación de elementos justiciables —sean de hecho o medios de prueba de aspectos jurídicos, científicos o tecnológicos— que adscribe a las partes, preferentemente, la dirección y conducción del proceso; sin embargo, en ciertos casos, la instrucción o integración procesal es un papel que puede también corresponder al juez a través de allegar ciertas pruebas.

En el juicio de garantías ha sido tradicional la oficialidad del impulso procesal, artículo 157 Ley de Amparo, que matiza a la voluntad de las partes; pero, además, se contemplan ahora excepciones, tales como que el juez puede aportar elementos para la decisión, debe proveer el desahogo de las pruebas que obren ante la responsable y considere necesarias para resolver en el período de ejecución de fallos disponer la aportación de pruebas e incluso ordenar la práctica de incidentes para determinar el cumplimiento de la liquidación de prestaciones.

8. Suspensión

Suspender el acto reclamado significa interrumpir transitoriamente o detener temporalmente la aplicación de una orden, una acción o sus efectos (hasta en tanto se dicte sentencia ejecutoria), paralizando así algo que está rigiendo o en actividad en forma positiva o impidiendo que inicie su ejecución cuando está en potencia. Excepcionalmente puede tener efectos restitutorios cuando haya peligro de que el juicio quede sin materia.

1328 Montero, J. et al. (1994). *Derecho Jurisdiccional, I parte general*. Barcelona. José María Bosch, editor, p. 325.

Por tanto, poder detener la ejecución de actos de autoridad, sea administrativa o jurisdiccional, en tanto se argumenta y decide la validez de la legalidad de fondo, ha servido para rescatar y mantener el valor, utilidad y eficacia del juicio de garantías.

Cabe destacar que, la suspensión también procede contra omisiones, en determinadas circunstancias, como cuando éstas implican una afectación a la esfera jurídica del gobernado con efectos que no se agotan en un solo momento, tales como no proporcionar medicamentos que son parte del tratamiento a un paciente con una enfermedad grave como lo es el VIH, en este caso, el tratamiento es de por vida.

De ahí que, la suspensión en contra de una omisión debe ponderarse por el juzgador al examinar un caso particular, pues, tal como se mencionó, no en todos los asuntos la concesión de la suspensión por omisiones implica dejar el juicio sin materia.

Tal como se evidencia el incidente de suspensión es para el juicio de amparo un aditamento o accesorio que, en lo sustancial, lo complementa, le da vida, inyecta oxígeno, rejuvenece, le aporta funcionalidad y, puede llegar a ser, la ratio del juicio.

9. Jurisprudencia

Tomando en consideración los precedentes sentados por las sentencias que dan solución a diversas situaciones específicas, es posible ir proponiendo directrices para resolver casos similares.

Una definición de jurisprudencia es el conjunto de criterios derivados de la interpretación de la ley, realizada en fallos judiciales y sentencias, por la Suprema Corte de Justicia de la Nación (SCJN), en Pleno o sus Salas, los plenos de circuito o tribunales colegiados, que conforman una de las fuentes del derecho, al constituir una serie de directrices para la solución de casos en el futuro.

Acorde con lo dispuesto en la Ley de Amparo, la jurisprudencia se establece por reiteración de criterios, por contradicción de tesis y por sustitución.

Reiteración: la jurisprudencia por reiteración se establece cuando se sustenta un mismo criterio en cinco sentencias no interrumpidas por otra en contrario, resueltas en diferentes sesiones.

En el caso de la SCJN en Pleno, las sentencias deberán ser resueltas por una mayoría de cuando menos ocho votos.

Cuando la jurisprudencia sea de las salas del máximo tribunal, las sentencias deberán ser resueltas por una mayoría de cuando menos cuatro votos.

Tratándose de jurisprudencia de tribunales colegiados, las sentencias deberán ser votadas por unanimidad.

Contradicción: la jurisprudencia por contradicción se establece al dilucidar los criterios discrepantes sostenidos entre las salas de la SCJN, entre los plenos de circuito o entre los tribunales colegiados de circuito, en los asuntos de su competencia.

Las contradicciones de tesis serán resueltas por:

I. el Pleno de la SCJN cuando deban dilucidarse las tesis contradictorias sostenidas entre sus salas;

II. el Pleno o las salas de la SCJN, según la materia, cuando deban dilucidarse las tesis contradictorias sostenidas entre los plenos de circuito de distintos circuitos, entre los plenos de circuito en materia especializada de un mismo circuito, o sus tribunales de diversa especialidad, así como entre los tribunales colegiados de diferente circuito y

III. los plenos de circuito cuando deban dilucidarse las tesis contradictorias sostenidas entre los tribunales colegiados del circuito correspondiente.

Sustitución: la jurisprudencia que por reiteración o contradicción establezca el Pleno o las salas de la SCJN, así como los plenos de circuito, podrá ser sustituida conforme a las siguientes reglas:

I. Cualquier tribunal colegiado de circuito (TCC), previa petición de alguno de sus magistrados, con motivo de un caso concreto una vez resuelto, podrán solicitar al Pleno de circuito al que pertenezcan que sustituya la jurisprudencia que por contradicción haya establecido, para lo cual expresarán las razones por las cuales se estima debe hacerse.

   Para que los plenos de circuito sustituyan la jurisprudencia se requerirá de las dos terceras partes de los magistrados que lo integran.

II. Cualquiera de los plenos de circuito, previa petición de alguno de los magistrados de los tribunales colegiados de su circuito y con motivo de un caso concreto una vez resuelto, podrán solicitar al Pleno de la SCJN, o a la sala correspondiente, que sustituya la jurisprudencia que hayan establecido, para lo cual expresarán las razones por las cuales se estima debe hacerse. La solicitud que, en su caso, enviarían los plenos de circuito al Pleno de la SCJN, o a la sala correspondiente, debe ser aprobada por la mayoría de sus integrantes.

III. Cualquiera de las salas de la SCJN, previa petición de alguno de los ministros que las integran, y solo con motivo de un caso concreto una vez resuelto, podrán solicitar al Pleno de la SCJN que sustituya la jurisprudencia que haya establecido, para lo cual expresarán las razones por las cuales se estima debe hacerse. La solicitud que, en su caso, enviaría la sala correspondiente al pleno de la SCJN, deberá ser aprobada por la mayoría de sus integrantes.

Jerarquía: La jurisprudencia sigue una jerarquía que se regula de la manera siguiente:

I. La que establezca la SCJN, funcionando en Pleno o en salas es obligatoria para éstas tratándose de la que decrete el Pleno, y además para los plenos de circuito, los tribunales colegiados y unitarios de circuito, los juzgados de distrito, tribunales militares y judiciales del orden común de los estados y del Distrito Federal, y tribunales administrativos y del trabajo, locales o federales.

II. La jurisprudencia que establezcan los plenos de circuito es obligatoria para los tribunales colegiados y unitarios de circuito, los juzgados de distrito, tribunales militares y judiciales del orden común de las entidades federativas y tribunales administrativos y del trabajo, locales o federales que se ubiquen dentro del circuito correspondiente.

III. La jurisprudencia que establezcan los tribunales colegiados de circuito es obligatoria para los órganos mencionados en el párrafo anterior, con excepción de los plenos de circuito y de los demás tribunales colegiados de circuito.

La jurisprudencia en ningún caso tendrá efecto retroactivo en perjuicio de persona alguna.

10. Declaratoria general de inconstitucionalidad

Cuando las salas o el Pleno de la SCJN, en los juicios de amparo indirecto en revisión, resuelvan la inconstitucionalidad de una norma general por segunda ocasión consecutiva (con excepción de normas tributarias), en una o en distintas sesiones, el presidente de la sala respectiva o de la SCJN lo informará a la autoridad emisora de la norma.

Una vez que se hubiere notificado al órgano emisor de la norma y transcurrido el plazo de 90 días naturales sin que se modifique o derogue la norma declarada inconstitucional, el pleno de la SCJN emitirá la declaratoria general de inconstitucionalidad correspondiente, siempre que hubiera sido aprobada por mayoría de cuando menos ocho votos.

Cuando el órgano emisor de la norma sea el órgano legislativo federal o local, el plazo referido en el párrafo anterior se computará dentro de los días útiles de los periodos ordinarios de sesiones determinados en la Constitución Federal, en el estatuto de gobierno del Distrito Federal o en la constitución local, según corresponda.

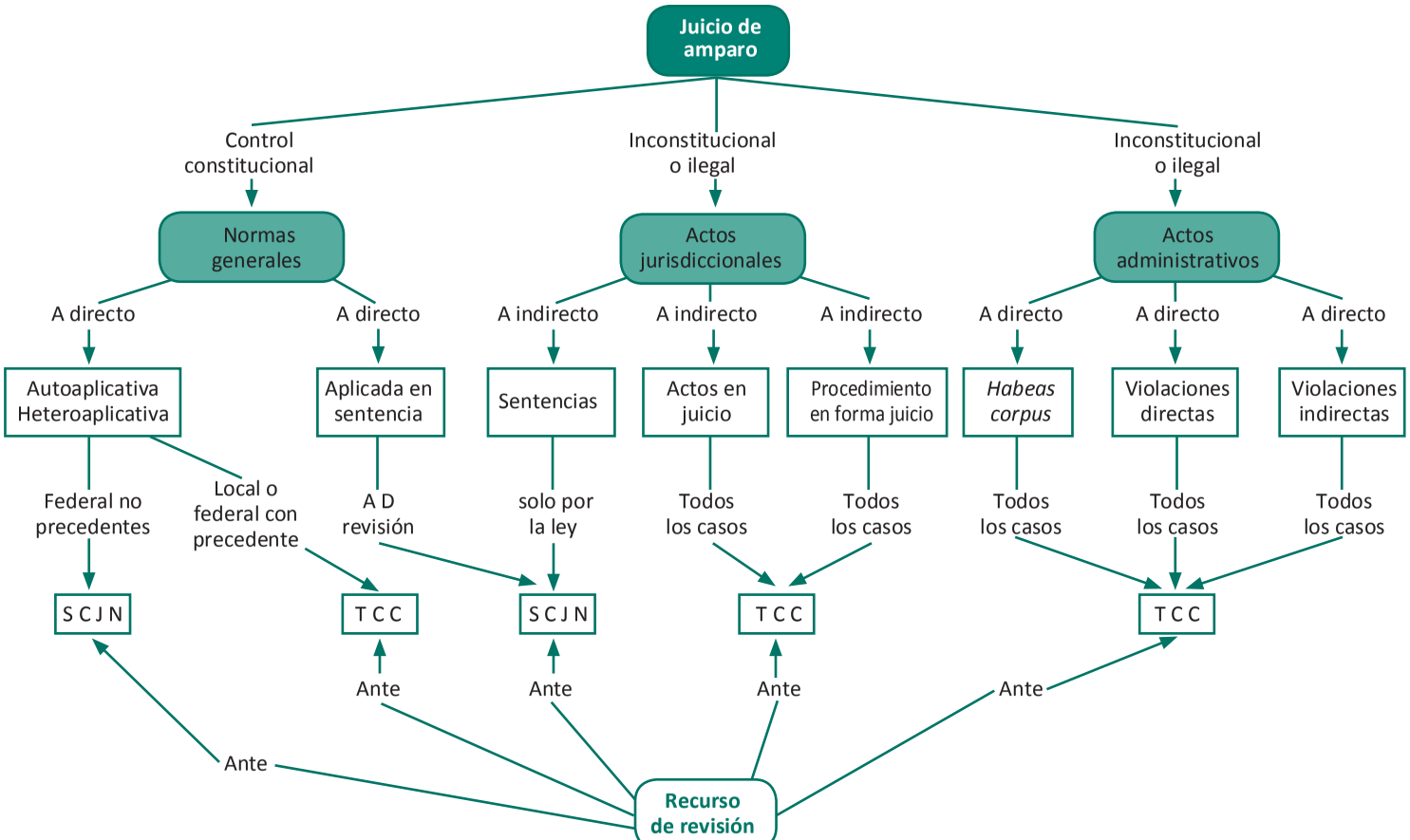
Los plenos de circuito, conforme a los acuerdos generales que emita la Suprema Corte de Justicia de la Nación, podrán solicitar a ésta, por mayoría de sus integrantes, que inicie el procedimiento de declaratoria general de inconstitucionalidad, cuando dentro de su circuito se haya emitido jurisprudencia derivada de amparos indirectos en revisión en la que se declare la inconstitucionalidad de una norma general.

La declaratoria general de inconstitucionalidad se remitirá al *Diario Oficial de la Federación* y al órgano oficial en el que se hubiera publicado la norma declarada inconstitucional para su publicación dentro del plazo de siete días hábiles.

Cabe destacar que la declaratoria en ningún caso podrá modificar el sentido de la jurisprudencia que le da origen, será obligatoria, tendrá efectos generales y establecerá la fecha a partir de la cual surtirá sus efectos, los alcances y las condiciones de la declaratoria de inconstitucionalidad.

Los efectos de estas declaratorias no serán retroactivos salvo en materia penal, en términos del párrafo primero del artículo 14 de la Constitución Política de los Estados Unidos Mexicanos.

11. Mapa conceptual



12. Modalidades del juicio de amparo

De acuerdo con lo dispuesto en el artículo 2 de la Ley en la materia, el juicio de amparo se tramitará en vía directa o indirecta.

13. Legitimación

La SCJN ha señalado que es un concepto mediante el cual se faculta a todas aquellas personas que, sin ser titulares de un derecho lesionado por un acto de autoridad, es decir, sin ser titulares de un derecho subjetivo u objetivo, les asista un interés en que una actuación u omisión de la autoridad sea acorde a la ley por derivar de ello un beneficio diferenciado o evitar un perjuicio en sus intereses, lo que exige demostrar tener una situación cualificada de afectación a efecto de conseguir que esa conducta sea enmendada.

En otras palabras, implica el reconocimiento de la legitimación del gobernado para ejercer un poder de exigencia respecto a la legitimidad de actos u omisiones de las autoridades cuyo sustento no se encuentra en un derecho subjetivo otorgado por la normatividad, sino en una posición cualificada que de hecho pueda tener respecto de la conveniencia o interés por la legalidad de determinados actos de autoridad que proviene de la afectación a la esfera jurídica del individuo, ya sea directa o derivada de su situación particular respecto del orden jurídico.

Para que un pretendido interés no sea reputado como simple, deben concurrir los siguientes requisitos:

I. especial posición cualificada de la persona o colectivo recurrente;

II. círculo de intereses individual o colectivo afectado, distinto o diferente de uno general o universal;

III. un interés propio y cualificado, distinto del común o convencional de cualquier otra persona;

IV. un agravio diferenciado respecto al resto de la comunidad;

V. conveniencia o provecho específicos para el caso de ser acogida la pretensión o exigencia de legalidad respecto de actuaciones de la autoridad, esto implica un beneficio o efecto positivo y cierto en la esfera jurídica del quejoso, actual o futura, si eventualmente se concediera el amparo y

VI. el interés legítimo existe, siempre que pueda presumirse que la pretendida actuación legítima de las autoridades, habría de colocar al accionante en condiciones de conseguir un determinado beneficio o evitar un perjuicio, sin que sea necesario que quede asegurado de antemano, que forzosamente haya de obtenerlo ni que deba tener apoyo en un precepto legal expreso y declarativo de derechos. Así, la afectación al interés legítimo se acredita cuando la situación de hecho creada o que pudiera crear el acto impugnado pueda ocasionar un perjuicio o privar de un beneficio, tanto a la colectividad como al interesado, pero de manera diferenciada y con distinta intensidad.

Al respecto, resultan ilustrativa la tesis 1a. XLIII/2013 (10a.), emitida por la Primera Sala de la Suprema Corte de Justicia de la Nación y la jurisprudencia P./J. 50/2014, del Pleno de la SCJN, de los rubros y textos siguientes.

> INTERÉS LEGÍTIMO EN EL AMPARO. SU DIFERENCIA CON EL INTERÉS SIMPLE.
>
> La reforma al artículo 107 constitucional, publicada en el *Diario Oficial de la Federación* el 6 de junio de 2011, además de que sustituyó el concepto de interés jurídico por el de interés legítimo, abrió las posibilidades para acudir al juicio de amparo. No obstante lo anterior, dicha reforma

no puede traducirse en una apertura absoluta para que por cualquier motivo se acuda al juicio de amparo, ya que el Constituyente Permanente introdujo un concepto jurídico mediante el cual se exige al quejoso que demuestre algo más que un interés simple o jurídicamente irrelevante, entendido éste como el que puede tener cualquier persona por alguna acción u omisión del Estado pero que, en caso de satisfacerse, no se traducirá en un beneficio personal para el interesado, pues no supone afectación a su esfera jurídica en algún sentido. En cambio, el interés legítimo se define como aquel interés personal, individual o colectivo, cualificado, actual, real y jurídicamente relevante, que puede traducirse, en caso de concederse el amparo, en un beneficio jurídico en favor del quejoso derivado de una afectación a su esfera jurídica en sentido amplio, que puede ser de índole económica, profesional, de salud pública, o de cualquier otra. Consecuentemente, cuando el quejoso acredita únicamente el interés simple, mas no el legítimo, se actualiza la causal de improcedencia prevista en el artículo 73, fracción XVIII, de la Ley de Amparo, en relación con el numeral 107, fracción I, de la Constitución Política de los Estados Unidos Mexicanos.

INTERÉS LEGÍTIMO. CONTENIDO Y ALCANCE PARA EFECTOS DE LA PROCEDENCIA DEL JUICIO DE AMPARO (INTERPRETACIÓN DEL ARTÍCULO 107, FRACCIÓN I, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS).

A consideración de este Tribunal Pleno de la Suprema Corte de Justicia de la Nación, el párrafo primero de la fracción I del artículo 107 de la Constitución Política de los Estados Unidos Mexicanos, establece que tratándose de la procedencia del amparo indirecto —en los supuestos en que no se combatan actos o resoluciones de tribunales—, quien comparezca a un juicio deberá ubicarse en alguno de los siguientes dos supuestos: (I) ser titular de un derecho subjetivo, es decir, alegar una afectación inmediata y directa en la esfera jurídica, producida en virtud de tal titularidad; o (II) en caso de que no se cuente con tal interés, la Constitución ahora establece la posibilidad de solamente aducir un interés legítimo, que será suficiente para comparecer en el juicio. Dicho interés legítimo se refiere a la existencia de un vínculo entre ciertos derechos fundamentales y una persona que comparece en el proceso, sin que dicha persona requiera de una facultad otorgada expresamente por el orden jurídico, esto es, la persona que cuenta con ese interés se encuentra en aptitud de expresar un agravio diferenciado al resto de los demás integrantes de la sociedad, al tratarse de un interés cualificado, actual, real y jurídicamente relevante, de tal forma que la anulación del acto que se reclama produce un beneficio o efecto positivo en su esfera jurídica, ya sea actual o futuro pero cierto. En consecuencia, para que exista un interés legítimo, se requiere de la existencia de una afectación en cierta esfera jurídica —no exclusivamente en una cuestión patrimonial— apreciada bajo un parámetro de razonabilidad, y no solo como una simple posibilidad, esto es, una lógica que debe guardar el vínculo entre la persona y la afectación aducida, ante lo cual, una eventual sentencia de protección constitucional implicaría la obtención de un beneficio determinado, el que no puede ser lejanamente derivado, sino resultado inmediato de la resolución que en su caso llegue a dictarse. Como puede advertirse, el interés legítimo consiste en una categoría diferenciada y más amplia que el interés jurídico, pero tampoco se trata del interés genérico de la sociedad como ocurre con el interés simple, esto es, no se trata de la generalización de una acción popular, sino del acceso a los tribunales competentes ante posibles lesiones jurídicas a intereses jurídicamente relevantes y, por ende, protegidos. En esta lógica, mediante el interés legítimo, el demandante se encuentra en una situación jurídica identificable, surgida por una relación específica con el objeto de la pretensión que aduce, ya sea por una circunstancia personal o por una regulación sectorial o grupal, por lo que si bien en una situación jurídica concreta pueden concurrir el interés colectivo o difuso y el interés legítimo, lo cierto es que tal asociación no es absoluta e indefectible; pues es factible que un juzgador se encuentre con un caso en el cual exista un interés legítimo individual en virtud de que, la afectación o posición especial frente al ordenamiento jurídico, sea una situación no solo compartida por un grupo formalmente identificable, sino que redunde también en una persona determinada que no pertenezca a dicho grupo. Incluso, podría darse el supuesto de que la afectación redunde de forma exclusiva en la esfera jurídica de una persona

determinada, en razón de sus circunstancias específicas. En suma, debido a su configuración normativa, la categorización de todas las posibles situaciones y supuestos del interés legítimo, deberá ser producto de la labor cotidiana de los diversos juzgadores de amparo al aplicar dicha figura jurídica, ello a la luz de los lineamientos emitidos por esta Suprema Corte, debiendo interpretarse acorde a la naturaleza y funciones del juicio de amparo, esto es, buscando la mayor protección de los derechos fundamentales de las personas.

Consecuentemente, cuando el quejoso aduzca ser titular de un interés legítimo derivado de su especial situación frente al orden jurídico y, con base en ello, promueva el juicio, debe acreditar, de manera plena, que la norma impugnada o el acto de autoridad produce una afectación cualificada, diferenciada, real y actual a su esfera jurídica. Esto es, no basta aducir la titularidad de un interés legítimo y alegar que los actos reclamados violan los derechos reconocidos en la Constitución, puesto que también debe acreditarse una afectación a la esfera jurídica de manera directa o en virtud de la especial situación que se tenga frente al orden jurídico. Solo así, quien acude al juicio es realmente la parte agraviada.

Juicio de amparo directo

Jean Claude Tron Petit

La voz "juicio de amparo directo" es indiscutiblemente relevante para la materia de protección de datos, pues se trata de un concepto relacionado con los medios de impugnación admitidos por la normatividad de datos personales en los sectores público y privado y que procede frente a las resoluciones emitidas por los órganos garantes en materia de protección de datos. Es decir, al ser un medio de control de la legalidad de las actuaciones de la autoridad garante funge como un mecanismo idóneo para la defensa de los derechos humanos y su efectiva tutela administrativa y jurisdiccional.

1. Concepto

El juicio de amparo, en sentido amplio, es un medio de control constitucional, una garantía procesal prevista en la propia Constitución para la defensa de sus postulados cuando éstos han sido desconocidos o violados. Constituye la garantía constitucional por antonomasia y es la institución procesal más importante del ordenamiento mexicano para la defensa de los derechos fundamentales.[1329]

El juicio de amparo, dependiendo la naturaleza del acto de la autoridad que se reclame, puede sustanciarse en vía indirecta o directa. Este último, amparo directo, se conoce como amparo de una instancia, pues en principio, la decisión que se emita en él es de carácter terminal; sin embargo, de manera excepcional, procede la revisión en amparo directo, con supuestos de procedencia reforzados. Su procedencia está dirigida a combatir sentencias definitivas, laudos y resoluciones que pongan fin al juicio, dictadas por tribunales judiciales, administrativos, agrarios o del trabajo, ya sea que la violación se cometa en ellas o durante la sustanciación del procedimiento.

El escrito inicial de demanda debe presentarse por conducto de la autoridad responsable en términos del artículo 176 de la Ley de Amparo y su conocimiento corresponde, por regla general, a los tribunales colegiados de circuito, en términos del artículo 37, fracción I, de la Ley Orgánica del Poder Judicial de la Federación (LOPJF) y 107, fracción V, constitucional y, excepcionalmente, a la Suprema Corte de Justicia de la Nación, que ejerce su facultad de atracción en aquellos casos que por su interés y trascendencia así lo ameriten.

1329 Fix-Zamudio, H. (2005). *Estudio de la defensa de la Constitución en el ordenamiento mexicano*. Porrúa. México, p.257.

2. Marco Normativo

El juicio de amparo directo se encuentra previsto, sustancialmente, en los artículos 107, fracción III, inciso a, fracción V de la Constitución Política de los Estados Unidos Mexicanos (CEPUM) y 170 de la Ley de Amparo, que disponen lo siguiente:

Constitución:

> Art. 107. Las controversias de que habla el artículo 103 de esta Constitución, con excepción de aquellas en materia electoral, se sujetarán a los procedimientos que determine la ley reglamentaria, de acuerdo con las bases siguientes:
>
> III. Cuando se reclamen actos de tribunales judiciales, administrativos o del trabajo, el amparo solo procederá en los casos siguientes:
>
> a) Contra sentencias definitivas, laudos y resoluciones que pongan fin al juicio, ya sea que la violación se cometa en ellos o que, cometida durante el procedimiento, afecte las defensas del quejoso trascendiendo al resultado del fallo. En relación con el amparo al que se refiere este inciso y la fracción V de este artículo, el tribunal colegiado de circuito deberá decidir respecto de todas las violaciones procesales que se hicieron valer y aquéllas que, cuando proceda, advierta en suplencia de la queja, y fijará los términos precisos en que deberá pronunciarse la nueva resolución. Si las violaciones procesales no se invocaron en un primer amparo, ni el tribunal colegiado correspondiente las hizo valer de oficio en los casos en que proceda la suplencia de la queja, no podrán ser materia de concepto de violación, ni de estudio oficioso en juicio de amparo posterior.

Ley de Amparo:

> Artículo 170. El juicio de amparo directo procede:
>
> I. Contra sentencias definitivas, laudos y resoluciones que pongan fin al juicio, dictadas por tribunales judiciales, administrativos, agrarios o del trabajo, ya sea que la violación se cometa en ellos, o que, cometida durante el procedimiento, afecte las defensas del quejoso trascendiendo al resultado del fallo.
>
> Se entenderá por sentencias definitivas o laudos, los que decidan el juicio en lo principal; por resoluciones que pongan fin al juicio, las que sin decidirlo en lo principal lo den por concluido. En materia penal, las sentencias condenatorias, absolutorias y de sobreseimiento podrán ser impugnadas por la víctima u ofendido del delito.
>
> Para la procedencia del juicio deberán agotarse previamente los recursos ordinarios que se establezcan en la ley de la materia, por virtud de los cuales aquellas sentencias definitivas o laudos y resoluciones puedan ser modificados o revocados, salvo el caso en que la ley permita la renuncia de los recursos.
>
> Cuando dentro del juicio surjan cuestiones sobre constitucionalidad de normas generales que sean de reparación posible por no afectar derechos sustantivos ni constituir violaciones procesales relevantes, solo podrán hacerse valer en el amparo directo que proceda contra la resolución definitiva.
>
> Para efectos de esta Ley, el juicio se inicia con la presentación de la demanda. En materia penal el proceso comienza con la audiencia inicial ante el juez de control.
>
> II. Contra sentencias definitivas y resoluciones que pongan fin al juicio dictadas por tribunales de lo contencioso administrativo cuando éstas sean favorables al quejoso, para el único efecto de hacer valer conceptos de violación en contra de las normas generales aplicadas.
>
> En estos casos, el juicio se tramitará únicamente si la autoridad interpone y se admite el recurso de revisión en materia contencioso administrativa previsto por el artículo 104 de la CPEUM. El tribunal colegiado de circuito resolverá primero lo relativo al recurso de revisión contencioso administrativa, y únicamente en el caso de que éste sea considerado procedente y fundado, se avocará al estudio de las cuestiones de constitucionalidad planteadas en el juicio de amparo.

De los artículos reproducidos se advierte que el amparo directo procede contra sentencias definitivas, laudos y resoluciones que pongan fin al juicio, ya sea que la violación se cometa en ellos o que, cometida durante el procedimiento, afecte las defensas del quejoso trascendiendo al resultado del fallo.

Por sentencias definitivas y laudos se debe entender aquellas que decidan el juicio en lo principal, y por resoluciones que pongan fin al juicio, las que, sin decidirlo en lo principal, lo den por concluido (por ejemplo, el sobreseimiento).

Al conocer del amparo directo, el tribunal colegiado de circuito deberá decidir entre todas las violaciones procesales que se hicieron valer y aquéllas que, cuando proceda, advierta en suplencia de la queja, y fijará los términos precisos en que deberá pronunciarse la nueva resolución. Si las violaciones procesales no se invocaron en un primer amparo, ni el tribunal colegiado correspondiente las hizo valer de oficio en los casos en que proceda la suplencia de la queja, no podrán ser materia de concepto de violación, ni de estudio oficioso en juicio de amparo posterior.

Así, en el escrito inicial de demanda de amparo se pueden plantear violaciones procesales de fondo (*in iudicando* y sobre hechos), así como reclamar la inconstitucionalidad de normas generales aplicadas en el procedimiento o en el propio fallo.

Para la procedencia del juicio deberán agotarse previamente los recursos ordinarios que se establezcan en la ley de la materia, por virtud de los cuales aquellas sentencias definitivas, laudos y resoluciones puedan ser modificados o revocados, salvo el caso en que la ley permita la renuncia de los recursos.

Además, la Ley de Amparo vigente incorporó la figura del amparo adhesivo que consiste en que la parte que haya obtenido sentencia favorable y que tenga interés jurídico en que subsista el acto reclamado podrá presentar un amparo en forma adhesiva al que promueva cualquiera de las partes que intervinieron en el juicio del que emana el acto reclamado. En cuanto a la presentación del amparo adhesivo, si bien el amparo principal se promueve por conducto de la autoridad responsable, el amparo adhesivo debe presentarse ante el tribunal colegiado de circuito que conozca del amparo principal, ello en términos de la jurisprudencia P./J. 15/2017 (10a.), del Pleno de la Suprema Corte de Justicia de la Nación.

> AMPARO DIRECTO ADHESIVO. LA DEMANDA RELATIVA DEBE PRESENTARSE ANTE EL TRIBUNAL COLEGIADO DE CIRCUITO QUE CONOCE DEL PRINCIPAL Y NO ANTE LA AUTORIDAD RESPONSABLE. Conforme a los artículos 107, fracción III, inciso a), párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos y 182 de la Ley de Amparo, la circunstancia de que el ejercicio del amparo adhesivo dependa del principal, cuyas reglas le son aplicables en lo conducente, no significa que, en términos del artículo 176, párrafo segundo, de la ley citada, la demanda relativa deba presentarse ante la autoridad responsable, ya que en el juicio de amparo directo ésta solo tiene la calidad de auxiliar de la justicia federal, entre cuyas atribuciones explícitamente conferidas, no se encuentra la recepción de la demanda de amparo adhesivo, como deriva de los artículos 176, 177, 178 y 190 de la propia legislación, ni existe sanción para el supuesto en que no la remitiese al tribunal de amparo, según se advierte del artículo 260 de la Ley de Amparo; por tanto, la demanda de amparo adhesivo debe presentarse ante el tribunal colegiado de circuito que conozca del principal, en el entendido de que su presentación ante autoridad distinta no interrumpe los plazos legales para su promoción, en el caso, el de 15 días previsto en el diverso 181 del propio ordenamiento legal.

El artículo 172 de la Ley de Amparo prevé, de manera enunciativa, aquellos supuestos en que se considerarán violadas las leyes del procedimiento y que afectan las defensas del quejoso, trascendiendo al resultado del fallo, en las materias administrativa, civil, agraria o del trabajo. El diverso artículo 173 enuncia los mismos casos, pero en materia penal.

Por su parte, el diverso artículo 175 de la Ley de Amparo prevé los requisitos que debe contener el escrito inicial de demanda, entre los cuales se destaca el contenido en la fracción IV que consiste en el señalamiento del acto reclamado. El acto reclamado en materia de amparo directo es la sentencia definitiva, laudo o resolución que ponga fin al juicio, no obstante, la ley autoriza reclamar la inconstitucionalidad de normas generales aplicadas en la propia sentencia, laudo o resolución, o en la secuela del procedimiento que dio origen a la resolución; sin embargo, el reclamo de normas generales en la vía indirecta y directa es diferente.

Sobre este tema, el Pleno de la Suprema Corte de Justicia de la Nación, en la jurisprudencia P. VIII/2005, sostuvo el criterio siguiente:

> AMPARO CONTRA LEYES. SUS DIFERENCIAS CUANDO SE TRAMITA EN LAS VÍAS INDIRECTA Y DIRECTA. Las características que distinguen a esas vías tratándose del amparo contra leyes radican, esencialmente, en lo siguiente: a) en el amparo indirecto la ley es uno de los actos reclamados y las autoridades legisladoras participan en el juicio como autoridades responsables, mientras que en el amparo directo la ley no puede constituir un acto reclamado ni se emplaza como autoridades responsables a sus autores; b) en la vía indirecta el amparo concedido contra la ley produce la consecuencia práctica de invalidarla por cuanto hace al quejoso, por ende, no se le aplicará mientras esté vigente; en tanto que en la vía directa el amparo se concede única y exclusivamente en contra de la sentencia, laudo o resolución reclamada y no contra la ley, por tanto, la concesión solamente vincula a desaplicar la ley en ese caso concreto, pero no impide que se le vuelva a aplicar al quejoso; c) en el amparo indirecto pueden rendirse pruebas para demostrar la inconstitucionalidad de la ley, mientras que en la vía directa no existe tal posibilidad, aun cuando el quejoso pueda apoyarse en las pruebas ofrecidas ante la responsable para demostrar tal inconstitucionalidad; d) en el amparo indirecto promovido sin agotar antes algún medio de defensa ordinario, el juez de Distrito tiene amplias facultades para determinar la improcedencia del juicio; en cambio, en el amparo directo (y en aquellos amparos indirectos promovidos después de haberse agotado un medio ordinario de defensa) deben respetarse los presupuestos procesales que ya estén determinados por la autoridad responsable, tales como el interés jurídico, la legitimación, la personalidad, etcétera; e) en el amparo indirecto los tribunales colegiados de circuito, a partir de las reformas constitucionales de 1994 y 1999, así como de la expedición de diversos acuerdos generales emitidos por el Pleno de la Suprema Corte de Justicia de la Nación, como el 5/2001, participan como órganos de segunda instancia en virtud de la delegación de competencia que les hace este alto tribunal, conforme a la cual, en determinadas condiciones, resolverán sobre el fondo del asunto y sus decisiones serán terminales; por su parte, en el amparo directo esos órganos son de primera instancia y sus sentencias también son revisables por la Suprema Corte, solamente en la materia de constitucionalidad de leyes o interpretación directa de la Carta Magna; f) en el amparo indirecto solo pueden interponer revisión, en defensa de la constitucionalidad de la ley, los titulares de los órganos de Estado a quienes se encomiende su promulgación, o quienes la representen, en tanto que en el amparo directo, como ya se dijo, no participan los órganos legiferantes y, por ende, no son ellos quienes pueden interponer la revisión; en cambio, en muchos casos, la autoridad que aplicó la ley figura como tercero perjudicado y puede, con ese carácter, hacer valer dicho recurso; y g) en el amparo indirecto el juez de distrito resuelve sobre la suspensión de los actos reclamados, mientras que en el directo esa decisión le corresponde a la autoridad responsable.

En cuanto a la presentación de la demanda de amparo directo, como se sostuvo, el escrito se presenta ante la autoridad responsable, esto es, aquella que emitió la sentencia definitiva, laudo o resolución, y sobre este aspecto debe destacarse que la Segunda Sala de la Suprema Corte de Justicia de la Nación, en la jurisprudencia 2a./J. 36/2018 (10a.), sostuvo que para determinar la oportunidad en la presentación de la demanda de amparo contra una sentencia definitiva, laudo o resolución que ponga fin al juicio, dictada por tribunales judiciales, administrativos o del trabajo, no deben excluirse del cómputo del

plazo respectivo los días en los que el tribunal colegiado de circuito al que corresponda conocer de dicha demanda haya suspendido sus labores, pues por disposición del artículo 176 de la Ley de Amparo, es ante la autoridad responsable del acto reclamado y no ante el tribunal colegiado de circuito, que inicia el trámite del juicio de amparo directo con la presentación de la demanda respectiva, y por ello, para el cómputo del plazo relativo deben excluirse los días inhábiles de la responsable, sin que deban excluirse los días en los que el tribunal colegiado de circuito haya dejado de laborar, pues esa circunstancia no incide para el cómputo del plazo, ni ocasiona inseguridad o falta de certeza al particular.

Por último, como se dijo al inicio, por regla general, las sentencias dictadas por los tribunales colegiados de circuito en amparo directo son definitivas y solo de manera extraordinaria pueden impugnarse mediante el recurso de revisión previsto en los artículos 107, fracción IX, de la CPEUM y 81, fracción II, de la Ley de Amparo conforme a los cuales, una vez actualizados los presupuestos procesales (competencia, legitimación, oportunidad del recurso —en su caso— entre otros) procede el mencionado medio de defensa siempre que: 1) en la sentencia de amparo directo combatida se decida sobre la constitucionalidad o inconstitucionalidad de una norma general o se establezca la interpretación directa de un precepto constitucional o de los derechos humanos reconocidos en los tratados internacionales de los que el Estado mexicano sea parte, o bien, si en dichas sentencias se omite el estudio de las cuestiones referidas, cuando se hubieren planteado en la demanda de amparo y 2) el problema de constitucionalidad entrañe la fijación de un criterio de importancia y trascendencia.

En cuanto a la fijación de un criterio de importancia y trascendencia, se actualiza cuando: (i) pueda dar lugar a un pronunciamiento novedoso o de relevancia para el orden jurídico nacional o (ii) lo decidido en la sentencia recurrida pueda implicar el desconocimiento de un criterio sostenido por la Suprema Corte de Justicia de la Nación relacionado con alguna cuestión propiamente constitucional, por haberse resuelto contra ese criterio o se hubiere omitido aplicarlo.

Juicio de amparo indirecto

Jean Claude Tron Petit

La voz "juicio de amparo indirecto" es de notaria importancia para la materia de protección de datos, pues la defensa procesal en este rubro reviste particularidades importantes que es necesario delimitar y conocer, siendo las características del amparo indirecto una de ellas, pues en aquellos casos en los que no es posible impugnar un acto procesal mediante el juicio de amparo directo, el amparo indirecto se perfila como una opción viable para la defensa de los derechos de los gobernados.

1. ¿Qué es y para qué sirve el juicio de amparo indirecto?

El juicio de amparo es el medio de impugnación, control y decisión sobre la mayoría de actos de autoridades respecto a la constitucionalidad, convencionalidad o legalidad de sus méritos.

Sin embargo, conviene puntualizar que el juicio de amparo indirecto se distingue del directo por los actos que pueden ser reclamados o enjuiciados.

En efecto, mediante el amparo directo (AD), en términos muy generales, pueden reclamarse las sentencias definitivas y resoluciones que pongan fin al juicio, provenientes de cualquier categoría de tribunales. En cambio, el juicio de amparo indirecto (AI) es el medio de impugnación y control de todos los demás actos, por exclusión, salvo los casos de proscripción e improcedencia del juicio.

En consecuencia, el espectro impugnativo consiste en actos, normas y omisiones que provengan de quienes actúan o se comportan como autoridades. Esto incluye actos que i) no provengan de tribunales judiciales administrativos o del trabajo, ii) actos de dichos tribunales ejecutados fuera de juicio o después de concluido éste, iii) actos en el juicio que tengan sobre las personas o las cosas una ejecución de imposible reparación y iv) actos ejecutados dentro o fuera de juicio que afecten a personas extrañas.

El propósito del juicio no se reduce a anular o declarar la ilegitimidad de los actos reclamados, sino en restituir o reparar a los afectados en el goce de los derechos fundamentales violados; de ahí la estructura y complejidad de la institución.

Es así que las fracciones III, incisos b) y c), IV y VII, del artículo 107 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) no definen con exactitud la procedencia del juicio de amparo indirecto, pero de ellas se concluye como actos impugnables mediante el sumario constitucional en comento, los siguientes:

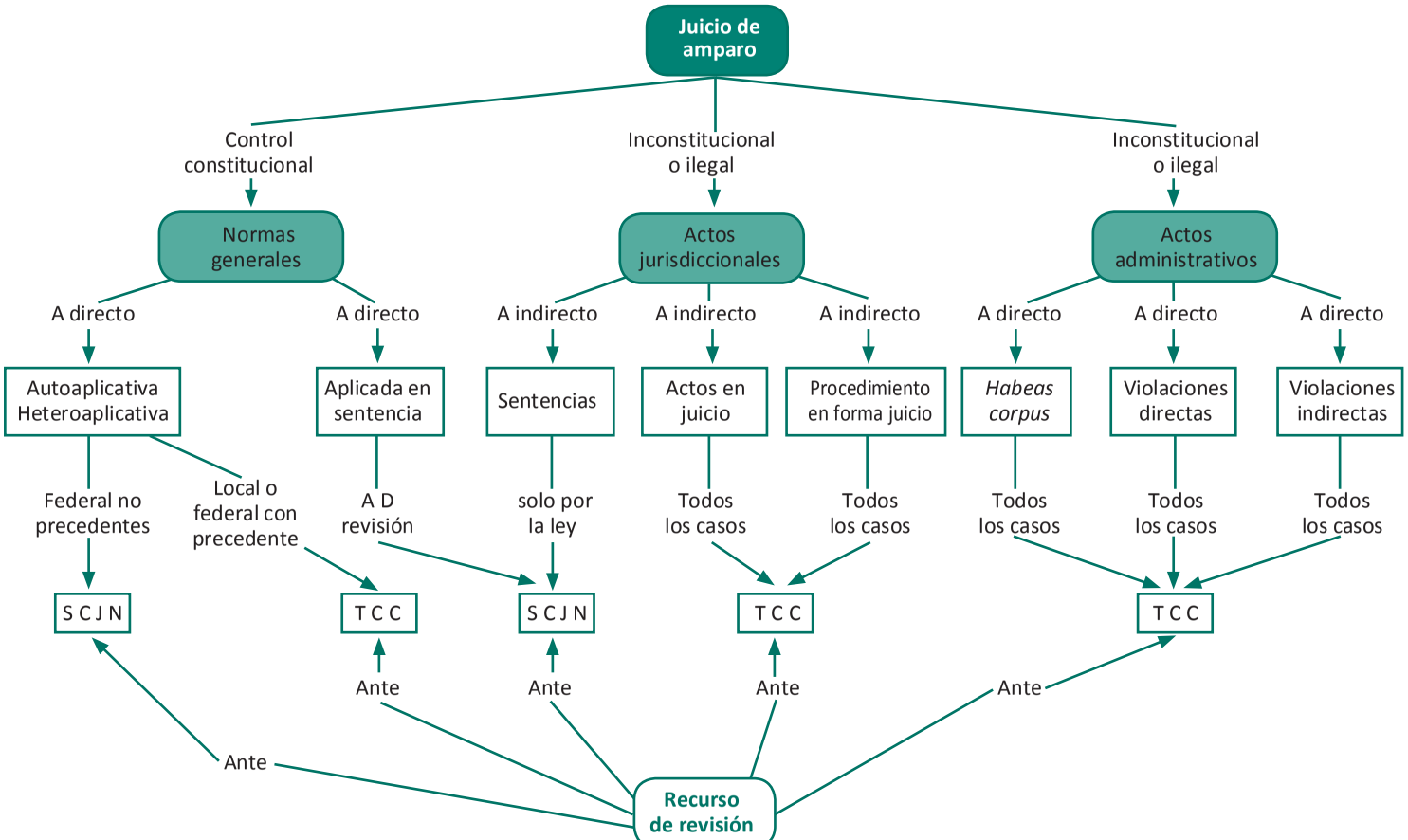
a) actos en juicio cuya ejecución sea de imposible reparación;
b) actos fuera de juicio;
c) actos después de concluido el juicio;
d) actos que afecten a personas extrañas al juicio;
e) normas generales y
f) actos u omisiones de autoridad, distinta de los tribunales.

El artículo 107 de la Ley de Amparo desarrolla a detalle cada uno de ellos, estableciendo condiciones, lineamientos y previsiones sobre los mismos. Además, la ley especifica otros supuestos de procedencia que no se comprenden expresamente en este precepto constitucional, como son ciertos actos u omisiones del ministerio público y de la Comisión Federal de Competencia Económica y del Instituto Federal de Telecomunicaciones, así como los que determinen inhibir o declinar la competencia o el conocimiento de un asunto.

Conviene resaltar que en ambas modalidades del juicio de amparo pueden coincidir como autoridades responsables los tribunales. Sin embargo, dependerá el acto que se reclame para definir si procede la vía directa o la indirecta. De tal forma que, si se trata de una resolución que pone fin al juicio, como la sentencia que resuelve el fondo de la controversia o la resolución que, sin decidirlo, lo da por concluido, entonces procede el amparo directo. Pero si la resolución combatida del tribunal es un acto dentro del juicio que tiene una ejecución de imposible reparación, un acto fuera de juicio, después de concluido, o que afecta a personas extrañas, procederá el amparo indirecto.

Retomando el esquema de procedencia del juicio de amparo, conviene tenerlo a la vista para considerar la amplitud de espectro del juicio indirecto (ver mapa conceptual), que procede contra cualquier acto u omisión, con tal que no sea la sentencia definitiva que es el propósito del juicio directo.

Mapa conceptual



Nuevas perspectivas

Merced al interés legítimo (especialmente el colectivo) el juicio de amparo permite cuestionar indirectamente políticas públicas cuando se afecte el núcleo esencial de los derechos fundamentales, superando criterios tradicionales sobre la clasificación de leyes auto aplicativas y el principio de relatividad, pues la restitución o reparación ordenada en una sentencia desborda como límite personal a una sola persona que actúe como quejoso y se extiende a todo el colectivo.

En efecto, un concepto de agravio más flexible —como el de interés legítimo— genera una reducción del espacio de las leyes heteroaplicativas y es directamente proporcional en la ampliación del espacio de las leyes autoaplicativas ya que existen mayores posibilidades lógicas de que una ley genere afectación por su sola entrada en vigor, dado que solo se requiere constatar una afectación individual o colectiva, calificada, actual, real y jurídicamente relevante, siempre que esté tutelada por el derecho objetivo y, en caso de obtener el amparo, pueda traducirse en un beneficio para el quejoso, como lo sostuvo la Primera Sala de la Suprema Corte de Justicia de la Nación (SCJN) en la tesis aislada 1a. CCLXXXI/2014 (10a.) de rubro: "INTERÉS LEGÍTIMO Y JURÍDICO. CRITERIO DE IDENTIFICACIÓN DE LAS LEYES HETEROAPLICATIVAS Y AUTOAPLICATIVAS EN UNO U OTRO CASO".

Asimismo, el juicio de amparo que originalmente fue concebido para proteger derechos estrictamente individuales y exclusivos, ahora también puede utilizarse para proteger derechos con una naturaleza más compleja, como los económicos, sociales y culturales, cuya afectación y consecuente reparación trasciende a la esfera jurídica subjetiva o individual de quien promovió el medio de control constitucional en comento, siendo inadmisible suponer que por esa cuestión se niegue la procedencia del mismo, pretextándose la violación al principio de relatividad de las sentencias. Así lo resolvieron la Primera y Segunda Salas de la SCJN, en las tesis aisladas 1a. XXI/2018 (10a.) y 2a. LXXXIV/2018 (10a.) de rubros: "PRINCIPIO DE RELATIVIDAD. SU REINTERPRETACIÓN A PARTIR DE LA REFORMA CONSTITUCIONAL DE 10 DE JUNIO DE 2011." y "SENTENCIAS DE AMPARO. EL PRINCIPIO DE RELATIVIDAD ADMITE MODULACIONES CUANDO SE ACUDE AL JUICIO CON UN INTERÉS LEGÍTIMO DE NATURALEZA COLECTIVA".

2. ¿Quiénes son los protagonistas en el juicio de amparo indirecto?

A continuación se dará una breve explicación de cada protagonista en el juicio de amparo indirecto.

a) La parte quejosa es quien promueve la demanda, puede ser una persona física o una persona moral, privada, pública o social, nacional o extranjera, individual o colectiva, o sucesión testamentaria o legal, con la posibilidad de hacerlo a través de quien los represente.
b) La autoridad responsable será cualquier órgano del Estado que dicte, ordene, ejecute, o trate de ejecutar, un acto o norma y al hacerlo, crea, modifique o extinga una situación jurídica en forma unilateral y obligatoria, u omita un acto que de realizarse crearía, modificaría o extinguiría dicha situación.
c) Los particulares son autoridad cuando realizan actos equivalentes a los de autoridad conforme a las funciones determinadas por una norma general, debiendo precisar que no lo son cuando actúan como auxiliares de la administración pública.
d) El tercero interesado es la persona física o moral, nacional o extranjera, pública o privada, que siendo titular de un interés jurídico comparece al juicio en defensa de tal interés, incompatible o contrario al de la parte quejosa, es decir, quien está interesado en preservar el acto, omisión o norma reclamada.
e) El ministerio público es un órgano del Estado que actúa como parte en todos los juicios en representación del interés general, estando en posibilidad de expresar su parecer sobre el juicio ante el tribunal y solicitar alguna providencia o el dictado de una resolución en determinado sentido, mediante la formulación de oficios llamados "pedimentos".

3. ¿Qué límites tiene el juicio de amparo indirecto?

Improcedencia y proscripción del juicio

A la par de los supuestos de procedencia, el legislador estableció en el artículo 61 de la legislación de la materia, diversos motivos de improcedencia, sin ser las únicas causas que impidan el inicio del juicio o provoquen su conclusión anticipada o sobreseimiento en sentencia, pues de la Constitución Federal derivan directamente otras.

Debe precisarse que la previsión de supuestos de improcedencia no es contraria al derecho de tutela judicial efectiva, siempre que los requisitos para el acceso a la justicia no se contrapongan a la racionalidad, proporcionalidad o resulten discriminatorios, como lo estableció la Primera Sala de la SCJN en la jurisprudencia 1a./J. 90/2017 (10a.), de rubro: "DERECHO FUNDAMENTAL DE ACCESO A LA JURISDICCIÓN. SU CONTENIDO ESPECÍFICO COMO PARTE DEL DERECHO A LA TUTELA JURISDICCIONAL EFECTIVA Y SU COMPATIBILIDAD CON LA EXISTENCIA DE REQUISITOS DE PROCEDENCIA DE UNA ACCIÓN".

Las causas de improcedencia, pueden agruparse en los criterios explicados a continuación:

a) Actos inatacables

Aquellos que por disposición constitucional o legal no pueden impugnarse por esta vía, como es el caso de las resoluciones dictadas por el Tribunal Electoral del Poder Judicial de la Federación o de los tribunales colegiados de circuito, adiciones o reformas a la Constitución Federal y actos de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal, entre otros.

b) Seguridad jurídica

Por un lado, las causales que se refieren a la litispendencia consisten en que el acto u omisión reclamada sea materia de otro juicio de amparo ya admitido y pendiente de re-

solución, existiendo identidad entre las partes, aunque los conceptos de violación sean distintos, pues se entiende que la parte quejosa debe plantear todas las violaciones en una sola demanda. Al respecto, la jurisprudencia P./J. 24/2014 (10a.) emitida por el Pleno de la SCJN, de rubro: "LITISPENDENCIA. PARA QUE SE ACTUALICE ESTA CAUSAL DE IMPROCEDENCIA, PREVISTA EN EL ARTÍCULO 73, FRACCIÓN III, DE LA LEY DE AMPARO, VIGENTE HASTA EL 2 DE ABRIL DE 2013, ES NECESARIO QUE SE HAYAN ADMITIDO LAS DEMANDAS RESPECTIVAS".

Por otro lado, existen supuestos de improcedencia derivados de la actualización de la figura jurídica de cosa juzgada, configurada cuando hay identidad de acto omisión o norma reclamada y partes en dos o más juicios y ya se dictó sentencia firme en uno de éstos. Sobre el tema, las jurisprudencias P./J. 86/2008 y 1a./J. 161/2007, emitidas por el Pleno y la Primera Sala de la SCJN, de rubros: "COSA JUZGADA. SUS LÍMITES OBJETIVOS Y SUBJETIVOS." y "COSA JUZGADA. PRESUPUESTOS PARA SU EXISTENCIA".

Además, existe la cosa juzgada refleja, en la cual no existe identidad entre partes u objeto, pero hay tal vinculación entre la materia de un juicio y otro, que lo resuelto en una afecta necesariamente lo que debe resolverse en el otro, sin llegar a configurar una causa de improcedencia, pero sí la ineficacia de conceptos de violación.

c) Consentimiento tácito o expreso

Deriva de la expresión de la parte quejosa de estar conforme con el acto, omisión o norma reclamados o no los impugna dentro de los plazos legales para promover el juicio en su contra. El conocimiento tácito o expreso requiere el conocimiento completo del acto reclamado por parte del promovente del juicio.

d) Definitividad

Consiste en el deber de agotar todos los medios ordinarios de defensa procedentes contra el acto u omisión antes de promover el juicio de amparo, dado su carácter extraordinario.

Como consecuencia de lo anterior también se actualiza la improcedencia del juicio por promover un medio ordinario de defensa en contra del mismo acto que se reclama en el juicio de amparo, cuando aquel se haya admitido, tal como lo refiere la Primera Sala de la SCJN, en la jurisprudencia 1a./J. 68/2011, de rubro: "EMPLAZAMIENTO. CUANDO SE PROMUEVE AMPARO POR SU FALTA O INDEBIDA REALIZACIÓN A UN JUICIO Y AL MISMO TIEMPO SE EJERCE LA ACCIÓN DE NULIDAD DE JUICIO CONCLUIDO RESPECTO DE AQUEL CUYO EMPLAZAMIENTO SE RECLAMA, SE ACTUALIZA LA CAUSA DE IMPROCEDENCIA ESTABLECIDA EN EL ARTÍCULO 73, FRACCIÓN XIV DE LA LEY DE AMPARO".

Existen numerosas excepciones a este principio, como cuando se aleguen violaciones directas a la Constitución, excluyendo cualquier tema de legalidad o tratándose de actos administrativos, cuando conforme a las leyes que los rijan, la interposición del recurso, juicio o medio de defensa, no prevea la suspensión de los efectos del acto reclamado o sí la prevé, exija mayores requisitos o un plazo mayor del previsto en la Ley de Amparo para dictar la suspensión definitiva, por mencionar solo algunas.

e) Actos intraprocesales que no son de imposible reparación

A diferencia del anterior principio, el de irreparabilidad consiste en la imposibilidad de reclamar en amparo los actos intraprocesales dictados dentro de un procedimiento judicial o administrativo en forma de juicio y que será impugnable hasta que se dicte la resolución que ponga fin al procedimiento.

La excepción a tal regla es la relativa a actos intermedios que tienen ejecución de imposible reparación, es decir, que afectan derechos sustantivos, pues después de agotar los

recursos ordinarios en su contra pueden ser reclamados en amparo indirecto sin esperar la resolución final como lo refiere la jurisprudencia1a./J. 113/2013 (10a.), emitida por la Primera Sala de la SCJN, de rubro: "DEFINITIVIDAD EN EL JUICIO DE AMPARO INDIRECTO. LA IRREPARABILIDAD DEL ACTO NO CONSTITUYE, POR SÍ MISMA, UNA EXCEPCIÓN A ESTE PRINCIPIO, AUN CUANDO EN LA CONTIENDA JURÍDICA ESTÉ INVOLUCRADO UN MENOR DE EDAD".

f) Interés legítimo o jurídico

La persona que acuda al juicio de amparo debe ser titular de un derecho subjetivo o de un interés legítimo, individual o colectivo que es afectado por el acto, siendo carga procesal de la quejosa acreditar esa calidad.

Sobre el tema, los órganos del Poder Judicial de la Federación han emitido diversos criterios aislados y jurisprudenciales, como lo son los identificadas bajo los números P./J. 50/2014, 1a. XLIII/2013 (10a.) y 1a. XCVII/2014 (10a.), de rubros: "INTERÉS LEGÍTIMO. CONTENIDO Y ALCANCE PARA EFECTOS DE LA PROCEDENCIA DEL JUICIO DE AMPARO (INTERPRETACIÓN DEL ARTÍCULO 107, FRACCIÓN I, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS)"; "INTERÉS LEGÍTIMO EN EL AMPARO. SU DIFERENCIA CON EL INTERÉS SIMPLE."; y "INTERÉS JURÍDICO EN EL AMPARO. PARA LA PROCEDENCIA DE LA DEMANDA RELATIVA, ADEMÁS DE ADVERTIRSE LA PRESENCIA DE UN DERECHO SUBJETIVO, DEBE VERIFICARSE SI EXISTE UN OBJETIVO CONFERIDO POR EL MARCO CONSTITUCIONAL (LEGISLACIÓN VIGENTE HASTA EL 2 DE ABRIL DE 2013)".

g) Cambio de situación jurídica

Este supuesto se surte cuando algunos actos del procedimiento son separables, es decir, pueden sobrevivir aun cuando los actos que le preceden puedan resultar ilegales o nulos. Derivado de ello, se sobresee en el juicio promovido en contra de un acto del procedimiento, si el procedimiento continúa y se dicta otro acto que podría subsistir, aunque el reclamado fuera ilegal, pues entonces la concesión del amparo no podría liberar a la parte quejosa de la situación creada por el nuevo acto. Para mayor claridad es conveniente observar el contenido de la jurisprudencia 1a./J. 17/2008, emitida por la Primera Sala de la SCJN, cuyo rubro es: "SOBRESEIMIENTO POR CAMBIO DE SITUACIÓN JURÍDICA. PROCEDE DECRETARLO RESPECTO DE LA ORDEN DE APREHENSIÓN RECLAMADA SI DEL INFORME JUSTIFICADO APARECE QUE SE SUSTITUYÓ AL HABERSE DICTADO AUTO DE FORMAL PRISIÓN".

h) Cesación de efectos

El motivo de improcedencia se actualiza cuando el acto reclamado ha quedado insubsistente y han desaparecido del mundo jurídico y material todos sus efectos. La Suprema Corte de Justicia de la Nación ha señalado como requisitos de configuración: i) la existencia del acto reclamado; ii) que un acto de autoridad sobrevenga y deje insubsistente, en forma permanente, el acto reclamado; iii) una situación de hecho o de derecho que destruya de en forma definitiva el acto reclamado, de modo que se vuelva al estado anterior a la violación y iv) una situación de hecho que sobrevenga durante la tramitación del juicio y haga imposible el cumplimiento de la sentencia protectora. Destaca la jurisprudencia 2a./J. 59/99, emitida por la Segunda Sala de la SCJN, de rubro: "CESACIÓN DE EFECTOS EN AMPARO. ESTA CAUSA DE IMPROCEDENCIA SE ACTUALIZA CUANDO TODOS LOS EFECTOS DEL ACTO RECLAMADO SON DESTRUIDOS EN FORMA TOTAL E INCONDICIONAL".

i) Desaparición del objeto o materia

El objetivo esencial que persigue la acción de amparo es destruir los efectos perjudiciales del acto, omisión o norma reclamados, lo cual significa que si desaparece el objeto o la materia sobre la cual recae el acto reclamado; si el acto se ha consumado de manera irre-

parable; si subsiste, pero no puede surtir efecto alguno o si han cesado los efectos de lo reclamado sin dejar huella en la esfera jurídica de la parte quejosa, debe sobreseerse en el juicio por no haber objeto sobre el cual puedan recaer los efectos de la sentencia. Al respecto, la jurisprudencia 2a./J. 181/2006, emitida por la Segunda Sala de la SCJN, de rubro: "ACTO RECLAMADO QUE FORMALMENTE SUBSISTE, PERO CUYO OBJETO O MATERIA DEJÓ DE EXISTIR. LA CAUSA DE IMPROCEDENCIA ESTABLECIDA EN LA FRACCIÓN XVII DEL ARTÍCULO 73 DE LA LEY DE AMPARO SE ACTUALIZA CUANDO LOS EFECTOS DE AQUÉL NO HAN AFECTADO LA ESFERA JURÍDICA DEL QUEJOSO Y SE MODIFICA EL ENTORNO EN EL CUAL FUE EMITIDO, DE MODO QUE LA PROTECCIÓN QUE EN SU CASO SE CONCEDIERA CARECERÍA DE EFECTOS".

j) Ineficacia reparadora de la sentencia

El objeto esencial que persigue la acción de amparo es destruir los efectos perjudiciales del acto u omisión o norma reclamadas y restituir a la parte quejosa en el goce del derecho violado, pero cuando no pueden lograrse tales efectos reparatorios por cualquier motivo, se estima improcedente el juicio.

Este supuesto también se ha utilizado para sobreseer en el juicio en que el efecto restitutorio solo podría alcanzarse dándole efectos generales a la sentencia o cuando existe otro obstáculo análogo.

Sin embargo, se ha admitido como excepción, la posibilidad de que la sentencia pueda producir en algunos casos efectos reparadores más allá de las partes, lo que acontece cuando se reclaman omisiones por parte de quienes son titulares de intereses legítimos, como lo sostiene la tesis aislada 1a. CLXXIII/2015 (10a.), emitida por la Primera Sala de la SCJN, cuyo rubro es: "IMPROCEDENCIA DEL JUICIO DE AMPARO. NO SE ACTUALIZA LA CAUSAL RELATIVA A LA IMPOSIBILIDAD DE REPARAR LA VIOLACIÓN ALEGADA, SI SE DETERMINA LA EXISTENCIA DE UN INTERÉS LEGÍTIMO A UNA ASOCIACIÓN CIVIL EN DEFENSA DEL DERECHO A LA EDUCACIÓN".

k) Otras

La última fracción del artículo 61 de la Ley de Amparo permite que la improcedencia derive de otra disposición de la ley o de la propia Constitución General, como son los actos derivados de otros consentidos o las omisiones legislativas.

Otra forma de clasificar las causas de improcedencia es la siguiente:*

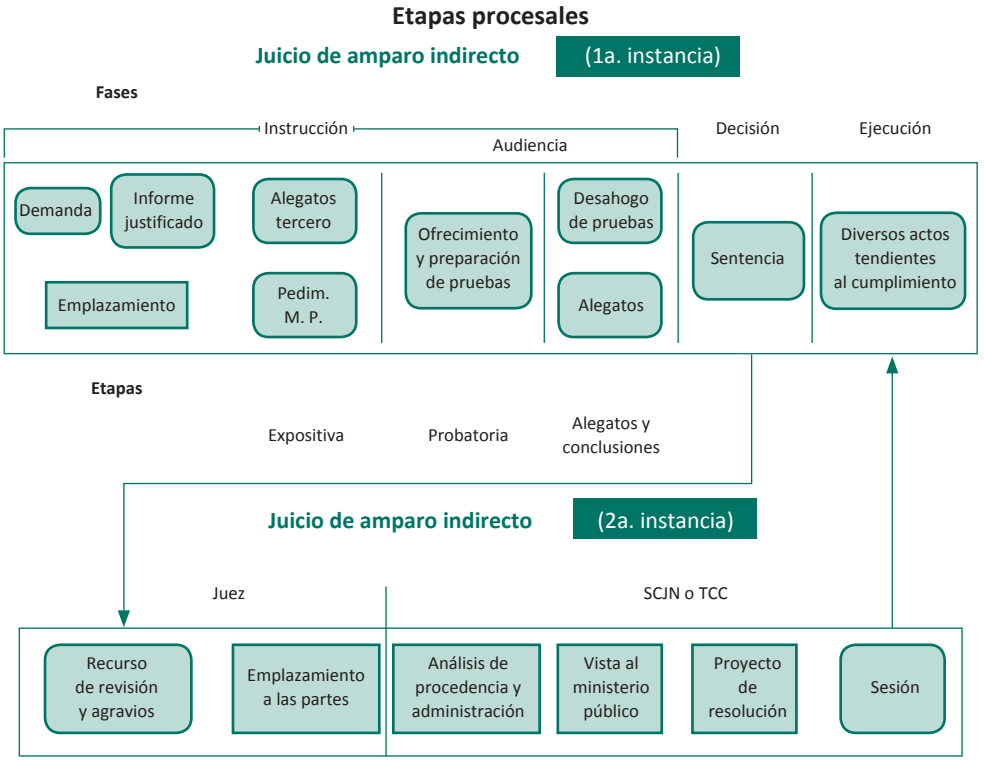
Referentes al acto	IX. Consumados irreparablemente X. Cambio situación jurídica XVI. Cesado efectos XVII. Extinción del objeto o materia
De definitividad	XV. Proceda medio, no tribunales administrativos XII. Proceda medio, 1 acto de aplicación XIV. Cuando se esté tramitando XIII. Proceda medio, tribunales administrativos
De litispendencia y cosa juzgada	III. Litispendencia IV. Cosa juzgada
De interés jurídico	V. Interés jurídico VI. Aplicación de leyes
De consentimiento	XI. Consentimiento expreso o manifestaciones XII. Consentimiento tácito
De la autoridad que emite el acto	I. SCJN o CJF II. Por orden de un tribunal colegiado, juzgados de amparo u otra autoridad VII. Organismo u autoridades en materia electoral
Relacionadas con otra disposición	VIII. Órganos legislativos XVIII. Resultados de una disposición de la ley

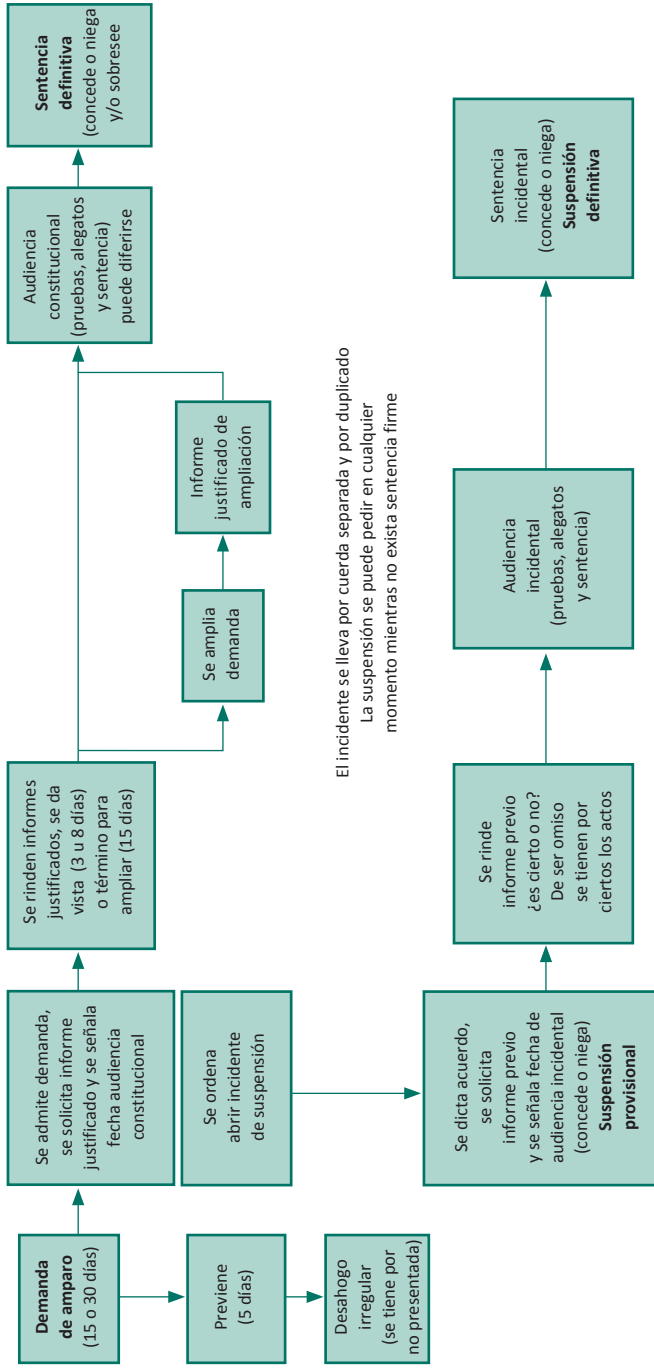
*La numeración corresponde a las fracciones del artículo 61 de la Ley de Amparo.

Asimismo, debe tenerse presente que el numeral 117, párrafo final, de la Ley de Amparo señala que tratándose de actos materialmente administrativos a los que se atribuya la ausencia o insuficiencia de fundamentación y motivación, por excepción, la autoridad debe complementar dichos aspectos en el informe justificado que rinda, así como el deber por parte del juzgador consistente en dar a conocer a la parte quejosa dicho documento, concederle un plazo razonable para que formule la ampliación de la demanda, correr traslado a las demás partes y dictar sentencia tomando en consideración todo ello, en la inteligencia que, conforme al último párrafo del artículo 124 del ordenamiento citado, ante la falta o insuficiencia de fundamentación y motivación, en la sentencia en conceso estimará que el acto reclamado presenta un vicio de fondo que impide a la autoridad su reiteración.

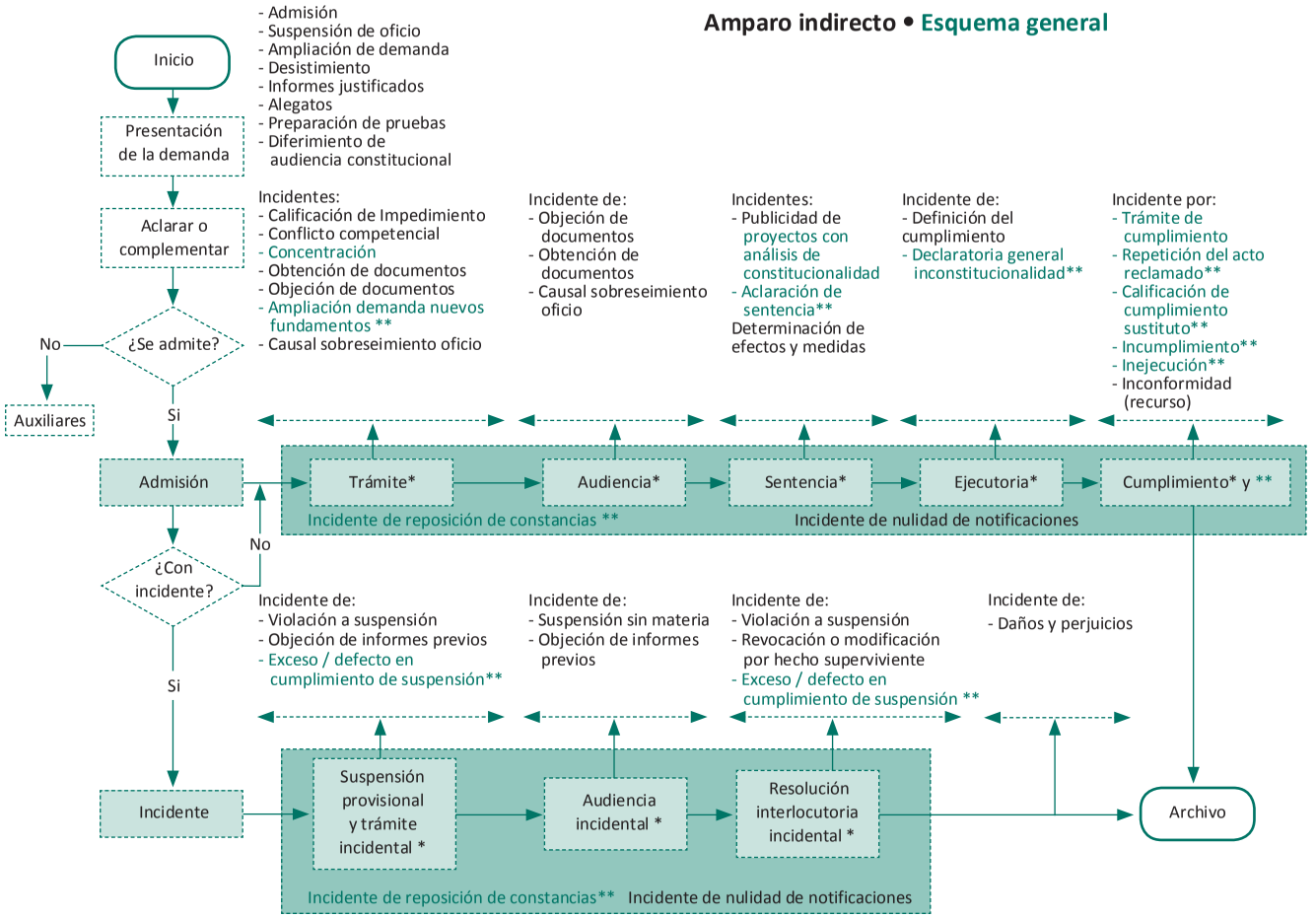
4. ¿Cómo es el trámite?

El trámite en el juicio de amparo indirecto, tanto en su primera instancia como en la segunda, puede representarse con los siguientes esquemas:




Demanda de amparo (15 o 30 días)
Previene (5 días)
Desahogo irregular (se tiene por no presentada)
Se admite demanda, se solicita informe justificado y se señala fecha audiencia constitucional
Se ordena abrir incidente de suspensión
Se rinden informes justificados, se da vista (3 u 8 días) o término para ampliar (15 días)
Se amplia demanda
Informe justificado de ampliación
Audiencia constitucional (pruebas, alegatos y sentencia) puede diferirse
Sentencia definitiva (concede o niega y/o sobresee
Se dicta acuerdo, se solicita informe previo y se señala fecha de audiencia incidental (concede o niega) Suspensión provisional
Se rinde informe previo ¿es cierto o no? De ser omiso se tienen por ciertos los actos
Audiencia incidental (pruebas, alegatos y sentencia)
Sentencia incidental (concede o niega) Suspensión definitiva
El incidente se lleva por cuerda separada y por duplicado
La suspensión se puede pedir en cualquier momento mientras no exista sentencia firme

Amparo indirecto • Esquema general



* En cualquier etapa debe adicionarse cualquier otro incidente innominado que requiera sustanciación especial **Régimen especial para la tramitación del incidente

5. ¿Qué incidentes pueden plantearse en el juicio de amparo indirecto?

En el juicio de amparo pueden resultar procedentes varios incidentes para resolver problemas específicos o superar circunstancias que impidan, dificulten o incidan en aspectos pragmáticos del juicio en cuanto a sus objetivos.

Especial mención debe hacerse respecto al incidente de suspensión que permite detener la ejecución de los actos reclamados y sus consecuencias, en tanto se decide sobre la constitucionalidad o legalidad de los actos reclamados. En ciertos casos, donde sea evidente la apariencia de un buen derecho, la medida cautelar puede tener efectos restitutorios para impedir afectaciones desproporcionadas y evidentes.

El esquema anterior (Amparo indirecto • Esquema general) ilustra este panorama.

6. ¿Qué es y para qué sirve el incidente de suspensión?

La suspensión es la medida cautelar que se prevé para el juicio de amparo y que impide que el acto o norma reclamada se ejecuten, se continúen ejecutando o afecten a la parte quejosa durante el tiempo que dure el juicio de amparo. Comprende medidas conservativas que impiden que el acto reclamado se materialice o continúe haciéndolo y medidas de tutela anticipada que permitan provisionalmente restablecer al quejoso en el goce del derecho violado.

Existen diversos tipos de suspensión: i) de oficio y de plano, ii) de oficio y en vía incidental y iii) a petición de parte, siendo las últimas dos los casos en que se sustancia en vía incidental. La parte quejosa puede solicitar la suspensión en cualquier momento, desde la demanda y hasta antes que concluya el juicio con sentencia definitiva.

La legislación impone proveer provisionalmente sobre la suspensión desde el momento en que se solicita para después ser sustituida por una decisión definitiva tomada en una audiencia en la que se desahogan pruebas y se formulan alegatos.

Los requisitos a satisfacer para obtener la suspensión definitiva son:

a) que lo solicite la parte quejosa;
b) que haya certidumbre sobre la existencia de los actos;
c) que la naturaleza del acto lo permita;
d) que el caso no esté en aquellos supuestos donde se presuma que se sigue perjuicio al interés social y se contravengan disposiciones de orden público y, si lo está, que la negativa de la suspensión cause un daño mayor a la colectividad;
e) que la ponderación entre la apariencia del buen derecho y el interés social resulte favorable a la parte quejosa y
f) en caso de aducir interés legítimo, acreditar el daño cualificado, inminente e irreparable a su pretensión en caso de que se niegue, y el interés social que motive su otorgamiento.

La suspensión, generalmente, tiene efectos conservativos, es decir, paraliza el estado en que se encuentra el acto reclamado (no se ejecute o no se siga ejecutando), pero también puede tener efectos de tutela anticipada, adicionales o restitutorios provisionalmente.

Juicio en línea

Faustino Gerardo Hidalgo Ezquerra

La voz "juicio en línea" se trata de un concepto procesal específico que reviste una importancia fundamental para la materia de protección de datos personales, pues se trata de uno de los medios de impugnación que la legislación federal reconoce a favor de las personas (físicas o morales) afectadas por una resolución recaída de un procedimiento instaurado ante el INAI como el Procedimiento de Protección de Derechos (PPD), el Procedimiento de Verificación (PV) o el Procedimiento de Imposición de Sanciones (Pisan) para hacerse valer mediante el uso de los medios electrónicos, dándoles la oportunidad de lograr una efectiva tutela de sus derechos.

1. Definición

El juicio en línea es una modalidad del juicio contencioso administrativo federal ordinario o sumario y de los procedimientos accesorios como recursos e incidentes, por virtud de la cual se presentan las promociones; se exhiben pruebas; se emiten acuerdos, oficios, resoluciones interlocutorias y sentencias definitivas; se formalizan actuaciones jurisdiccionales y se realizan las notificaciones a las partes por vía remota utilizando internet y las plataformas tecnológicas del Tribunal Federal de Justicia Administrativa (TFJA), prescindiendo absolutamente del papel e integrando la totalidad de las constancias procesales en expedientes electrónicos que pueden ser consultados por las partes, autorizados y personal jurisdiccional desde cualquier computadora con acceso a internet, las 24 horas del día de los 365 días del año.

Independientemente de lo anterior, hay que considerar que en la fracción XIII del artículo 1A de la Ley Federal de Procedimiento Contencioso Administrativo (LFPCA), que se ubica en el título I que habla sobre el juicio contencioso administrativo federal, capítulo I, de las disposiciones generales, se define el juicio en línea.[1330]

2. Delimitación conceptual y conceptos correlacionados

En el artículo 2 de la LFPCA se prevén los actos de la autoridad administrativa federal que pueden se impugnados mediante el juicio contencioso administrativo federal y particularmente en su párrafo segundo se indica que dicho medio de defensa procede en contra de las resoluciones definitivas que se consignan en Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa (LOTFJA), ahora denominado TFJA,[1331] mientras que en la fracción XIX del artículo 3 de la LOTFJA,[1332] publicada en el *Diario Oficial de la Federación,* el 18 de julio de 2016, se establece que ese órgano jurisdiccional conocerá de los juicios que se promuevan en contra de las resoluciones definitivas señaladas en otras leyes

1330 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 1A. Para los efectos de esta Ley se entenderá por:
XIII. Juicio en línea: substanciación y resolución del juicio contencioso administrativo federal en todas sus etapas, así como de los procedimientos previstos en el artículo 58 de esta Ley, a través del Sistema de Justicia en Línea, incluso en los casos en que sea procedente la vía sumaria.

1331 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 2. El juicio contencioso administrativo federal procede contra las resoluciones administrativas definitivas que establece la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa.

1332 Ley Orgánica del Tribunal Federal de Justicia Administrativa.
Artículo 3. El Tribunal conocerá de los juicios que se promuevan contra las resoluciones definitivas, actos administrativos y procedimientos que se indican a continuación:
XIX. Las señaladas en esta y otras leyes como competencia del Tribunal.

Por su parte, el artículo 126 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) dispone que procede el juicio contencioso administrativo federal, en contra de la resolución al procedimiento de protección de derechos,[1333] lo que es confirmado por el artículo 48 del acuerdo ACT-PUB/25/11/2015.06 por el cual se aprueban los lineamientos de los procedimientos de protección de derechos, de investigación y verificación, y de imposición de sanciones[1334] emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado en el *Diario Oficial de la Federación* el 9 de diciembre de 2015.

En el artículo 138 del Reglamento se determina que se puede hacer valer el medio de defensa que nos ocupa para controvertir el procedimiento de verificación[1335] y en el mismo sentido se emitió el artículo 67 del acuerdo ACT-PUB/25/11/2015.06 antes referido.[1336]

Finalmente, en el artículo 144 del RLFPDPPP se indica que para combatir las resoluciones de imposición de sanciones se puede promover el juicio ante el TFJA,[1337] lo cual se reitera en el artículo 74 del acuerdo ACT-PUB/25/11/2015.06.[1338]

Por virtud de lo anterior, debemos concluir que en contra de las resoluciones definitivas en materia de datos personales a que se refieren los preceptos antes analizados, es procedente el juicio contencioso administrativo federal, también conocido cono juicio de nulidad.

Al respecto, debemos precisar que conforme a LFPCA, existen dos modalidades para promover, sustanciar y resolver ese medio de defensa, a saber: el juicio tradicional y el juicio en línea.

El juicio tradicional —definido en la fracción XII[1339] del artículo 1A del artículo de LFPCA— se caracteriza por la presentación de promociones y emisión de acuerdos y resoluciones del Tribunal en papel y su integración en expedientes físicos. El juicio tradicional es una modalidad del juicio contencioso administrativo federal que ha operado hasta la fecha desde el primero de enero de 1937 con la entrada en vigor de la Ley de Justicia Fiscal publicada en el *Diario Oficial de la Federación* el 31 de agosto de 1936, por virtud de la cual se creó ese

1333 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Artículo 126. Contra la resolución al procedimiento de protección de derechos procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

1334 Acuerdo ACT-PUB/25/11/2015.06
Artículo 48. Contra la resolución al procedimiento de protección de derechos podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa, de conformidad con lo previsto por los artículos 56 de la Ley y 126 de su Reglamento.

1335 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Artículo 138. En contra de la resolución al procedimiento de verificación, se podrá interponer el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

1336 Acuerdo ACT-PUB/25/11/2015.06
Artículo 67. En contra de la resolución al procedimiento de verificación, se podrá interponer el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa, conforme al artículo 138 del Reglamento.

1337 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Artículo 144. En contra de la resolución al procedimiento de imposición de sanciones procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

1338 Acuerdo ACT-PUB/25/11/2015.06
Artículo 74. En contra de la resolución del procedimiento de imposición de sanciones, el infractor podrá promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa, de conformidad con el artículo 144 del Reglamento.

1339 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 1A. Para los efectos de esta Ley se entenderá por:
XII. Juicio en la vía tradicional: el juicio contencioso administrativo federal que se substancia recibiendo las promociones y demás documentales en manuscrito o impresos en papel, y formando un expediente también en papel, donde se agregan las actuaciones procesales, incluso en los casos en que sea procedente la vía sumaria o el juicio de resolución exclusiva de fondo.

medio de impugnación, como un medio de control de legalidad. El Tribunal Fiscal de la Federación, ahora denominado Tribunal Federal de Justicia Administrativa, es la instancia competente para resolverlo.

La otra modalidad de juicio contencioso administrativo es el juicio en línea, el cual está funcionado y se encuentra disponible para los particulares y autoridades administrativas desde el 7 de junio de 2011, por virtud del decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Procedimiento Contencioso Administrativo y de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa, publicado en el *Diario Oficial de la Federación* el 12 de junio de 2009 y del decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Federal de Procedimiento Contencioso Administrativo y de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa, publicado en el DOF el 10 de diciembre de 2010, y en particular por su artículo transitorio tercero, que ordenó que el juicio en línea iniciará su operación a los 18 meses contados a partir de la entrada en vigor de dicho decreto (7 de junio de 2011).

Conforme al contenido de los artículos 13 y 58C de la LFPCA, los particulares tienen la opción de promover el juicio en la modalidad tradicional o en línea, pero una vez ejercida no podrán cambiarla, mientras que si la demanda la presenta una autoridad, por ejemplo en el caso de impugnación de resoluciones favorables a los particulares, lo que se conoce en la doctrina como juicios de lesividad, deberá hacerlo en línea, en cuyo caso, el particular emplazado de la forma tradicional también podrá decidir si se tramitará de una forma o de la otra.[1340]

Es muy importante dejar en claro que, no obstante la existencia de las modalidades mencionadas, estamos en presencia de un procedimiento contencioso federal único en lo sustancial, y que si bien existen algunas disposiciones especiales para la sustanciación del juicio en línea, contenidas en el capítulo X, del juicio en línea, del título I, del juicio contencioso administrativo federal, de la LFPCA, en lo no previsto en ellas se aplicarán las demás disposiciones que resulten aplicables de ese ordenamiento, según dispone su artículo 58-A.[1341]

Sobre la regulación especial para el juicio en línea, debemos hacer hincapié que en el artículo 1A de de la Ley Federal de Procedimiento Contencioso Administrativo se establece el sistema de justicia en línea, lo que se verá más adelante, así como algunos otros conceptos relacionados con él, los cuales son importantes para su promoción, sustancia-

1340 Ley Federal de Procedimiento Contencioso Administrativo.
[...]
Artículo 13.- El demandante podrá presentar su demanda, mediante Juicio en la vía tradicional, por escrito ante la sala regional competente o, en línea, a través del Sistema de Justicia en Línea, para este último caso, el demandante deberá manifestar su opción al momento de presentar la demanda. Una vez que el demandante haya elegido su opción no podrá variarla. Cuando la autoridad tenga este carácter la demanda se presentará en todos los casos en línea a través del sistema de justicia en línea.
Para el caso de que el demandante no manifieste su opción al momento de presentar su demanda se entenderá que eligió tramitar el Juicio en la vía tradicional.
[...]
Artículo 58-C.- Cuando la demandante sea una autoridad, el particular demandado, al contestar la demanda, tendrá derecho a ejercer su opción para que el juicio se tramite y resuelva en línea conforme a las disposiciones de este capítulo, señalando para ello su domicilio y Dirección de Correo Electrónico.
A fin de emplazar al particular demandado, el secretario de acuerdos que corresponda, imprimirá y certificará la demanda y sus anexos que se notificarán de manera personal.
Si el particular rechaza tramitar el juicio en línea contestará la demanda mediante el juicio en la vía tradicional.

1341 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 58-A. El juicio contencioso administrativo federal se promoverá, substanciará y resolverá en línea, a través del sistema de justicia en línea que deberá establecer y desarrollar el Tribunal, en términos de lo dispuesto por el presente capítulo y las demás disposiciones específicas que resulten aplicables de esta Ley. En todo lo no previsto, se aplicarán las demás disposiciones que resulten aplicables de este ordenamiento.

ción, resolución, notificaciones y consulta, así como para entender su especial naturaleza y forma de operación. Dichos elementos son los siguientes: acuse de recibo electrónico, archivo electrónico, boletín jurisdiccional, aviso electrónico, clave de acceso, contraseña, dirección de correo electrónico, dirección de correo electrónico institucional, documento electrónico o digital, expediente electrónico y firma electrónica avanzada.

Es oportuno indicar que para la debida operación técnica y administrativa, y la correcta tramitación del juicio en línea, la junta de gobierno y administración del entonces Tribunal Federal de Justicia Fiscal y Administrativa, ahora de Justicia Administrativa, emitió el acuerdo e/jga/16/2011, que establece los lineamientos técnicos y formales para la sustanciación del juicio en línea, publicado en el *Diario Oficial de la Federación* el 4 de mayo de 2011, el cual define algunos conceptos como: centro de atención a usuarios, código de barras, huella digital, internet, módulo de registro, virus e intranet, y regula aspectos tales como la existencia de usuarios internos y externos, la clave de acceso y contraseña, el registro de autoridades, los requerimientos para firmar resoluciones y actuaciones, el portal del sistema de justicia en línea, así como su integridad, seguridad, y respaldo de información, la firma electrónica avanzada, el registro de envío de promociones electrónicas, la digitalización, impresión y resguardo de documentos, el boletín electrónico y las sanciones.

Una de las características más importantes del juicio en línea, según se desprende del contenido del artículo 58D[1342] de la LFPCA, es la existencia de expedientes electrónicos, y la integración a ellos de todas las promociones y pruebas de las partes, así como de los acuerdos, actas y resoluciones que dicta el Tribunal y que respecto a dichos expediente el Tribunal debe garantizar su autenticidad, integridad y durabilidad.

Sin embargo, como veremos en el párrafo siguiente, existen algunos supuestos previstos en para que los juicios en línea puedan ser tramitados —total o parcialmente— de manera simultánea en la modalidad tradicional y en línea y en ese sentido es factible que los documentos se generen digitalmente y sean impresos y certificados para integrar expedientes físicos o que surjan en papel, se digitalicen, certifiquen e integren expedientes electrónicos y en ambos casos subsisten los dos expedientes.

Los supuestos previstos en la LFPCA son:

a) De acuerdo con lo dispuesto en el artículo 58-M[1343] de la LFPCA, cuando un particular promueve un juicio en línea contra una autoridad administrativa y existe un tercero que tenga un interés incompatible con la pretensión del demandante en términos del

1342 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 58-D. En el sistema de justicia en línea del Tribunal se integrará el expediente electrónico, mismo que incluirá todas las promociones, pruebas y otros anexos que presenten las partes, oficios, acuerdos, y resoluciones tanto interlocutorias como definitivas, así como las demás actuaciones que deriven de la substanciación del juicio en línea, garantizando su seguridad, inalterabilidad, autenticidad, integridad y durabilidad, conforme a los lineamientos que expida el Tribunal.
En los juicios en línea, la autoridad requerida, desahogará las pruebas testimoniales utilizando el método de videoconferencia, cuando ello sea posible.

1343 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 58-M. Para los juicios que se substancien en términos de este capítulo no será necesario que las partes exhiban copias para correr los traslados que la ley establece, salvo que hubiese tercero interesado, en cuyo caso, a fin de correrle traslado, el demandante deberá presentar la copia de traslado con sus respectivos anexos.
En el escrito a través del cual el tercero interesado se apersone en juicio, deberá precisar si desea que el juicio se continúe substanciando en línea y señalar en tal caso, su dirección de correo electrónico. En caso de que manifieste su oposición, la Sala dispondrá lo conducente para que se digitalicen los documentos que dicho tercero presente, a fin de que se prosiga con la instrucción del juicio en línea con relación a las demás partes, y a su vez, se impriman y certifiquen las constancias de las actuaciones y documentación electrónica, a fin de que se integre el expediente del tercero en un juicio en la vía tradicional.

artículo 3 fracción III del mismo ordenamiento,[1344] además de presentar la demanda y pruebas por vía remota a través de Internet, la parte actora deberá exhibir un tanto impreso de la misma y sus anexos en la oficialía de partes de la sala del tribunal de conocimiento, para emplazar a dicho tercero, el cual podrá apersonarse al juicio en papel o hacerlo en línea, previa obtención de su clave de acceso y contraseña para poder ingresar en la plataforma tecnológica del tribunal diseñada para ese efecto.

b) En aquellos casos en que se promueva un juicio en línea por una autoridad administrativa en contra de un particular, tendrá la opción de acudir en línea o de forma tradicional. Ello se desprende del artículo 58-C[1345] de la LFPCA.

c) Cuando se ofrezcan pruebas que por su naturaleza no se puedan integrar a los expedientes electrónicos, se presentarán en la oficialía de partes del tribunal y las constancias respectivas se integraran al expediente electrónico, previa certificación de un secretario de acuerdos de la sala del conocimiento y el debido resguardo de las mismas en el archivo de la sala. Lo mismo sucede cuando se desahogan, con la comparecencia de la las partes o peritos, diligencias y se implementan actas o constancias escritas. Lo anterior lo podemos desprender del artículo 58-L de la LFPCA.[1346]

d) Si las partes en el juicio promueven un juicio de amparo directo o interponen un recurso de revisión, según corresponda, en contra de las sentencias del Tribunal, los escritos deben ser presentados de forma física en la oficialía de partes de la sala del conocimiento para su remisión en términos de ley al Poder Judicial de la Federación, junto con una copia certificada del expediente electrónico en el que se dictó la sentencia impugnada. Al mismo tiempo se digitalizarán dichas promociones y se integrarán al expediente electrónico, previa certificación del secretario de acuerdos, para consultas posteriores de las partes por vía remota, y lo mismo se hará con las ejecutorias que se emitan en esos medios de defensa. El referido mecanismo tiene su soporte en el artículo 58-Q de la LFPCA.[1347]

1344 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 3o.- Son partes en el juicio contencioso administrativo:
III. El tercero que tenga un derecho incompatible con la pretensión del demandante.

1345 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 58-C.- Cuando la demandante sea una autoridad, el particular demandado, al contestar la demanda, tendrá derecho a ejercer su opción para que el juicio se tramite y resuelva en línea conforme a las disposiciones de este capítulo, señalando para ello su domicilio y dirección de correo electrónico.
A fin de emplazar al particular demandado, el secretario de acuerdos que corresponda, imprimirá y certificará la demanda y sus anexos que se notificarán de manera personal.
Si el particular rechaza tramitar el juicio en línea contestará la demanda mediante el juicio en la vía tradicional.

1346 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 58-L. Para el caso de pruebas diversas a las documentales, los instrumentos en los que se haga constar la existencia de dichas pruebas se integrarán al expediente electrónico. El secretario de acuerdos, a cuya mesa corresponda el asunto, deberá digitalizar las constancias relativas y procederá a la certificación de su cotejo con los originales físicos, así como a garantizar el resguardo de los originales y de los bienes materiales que en su caso hubieren sido objeto de prueba.
Para el caso de pruebas diversas a las documentales, éstas deberán ofrecerse en la demanda y ser presentadas a la sala que esté en conocimiento del asunto, en la misma fecha en la que se registre en el sistema de justicia en línea del Tribunal la promoción correspondiente a su ofrecimiento, haciendo constar su recepción por vía electrónica.

1347 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 58-Q. Para la presentación y trámite de los recursos de revisión y juicios de amparo que se promuevan contra las actuaciones y resoluciones derivadas del juicio en línea, no será aplicable lo dispuesto en el presente capítulo.
El secretario general de acuerdos del Tribunal, los secretarios adjuntos de sección y los secretarios de acuerdos de sala superior y de salas regionales según corresponda, deberán imprimir el archivo del expediente electrónico y certificar las constancias del juicio que deban ser remitidos a los juzgados de distrito y tribunales colegiados de circuito, cuando se impugnen resoluciones de los juicios correspondientes a su mesa.
Sin perjuicio de lo anterior, en aquellos casos en que así lo solicite el juzgado de distrito o el tribunal colegiado se podrá remitir la información a través de medios electrónicos.

e) Si una persona modifica, altera, destruye o provoca la pérdida de información contenida en el sistema de justicia en línea, el Tribunal tomará las medidas necesarias para evitar dicha conducta hasta que concluya el juicio, el cual se continuará tramitando en la vía tradicional, lo cual está previsto en el artículo 58-R de la LFPCA.[1348]

Por virtud de lo anterior, podemos concluir entonces que, de manera excepcional, los juicios en línea, además de tener expedientes electrónicos integrados con las promociones, pruebas y actuaciones jurisdiccionales, pueden generar expedientes tradicionales parcialmente, los cuales se han dado en llamar híbridos o mixtos.

Otra de las características importantes del juicio en línea es la posibilidad que tienen las partes, sus autorizados y delegados e incluso peritos con los debidos permisos de enviar promociones y consultar los expedientes electrónicos, utilizando siempre su clave de acceso y contraseña, y su certificado de firma electrónica avanzada para hacer tal remisión de promociones, lo cual pueden hacer, dada la alta disponibilidad de las plataformas tecnológicas del Tribunal, desde cualquier computadora con acceso a internet y a estas plataformas las 24 horas del día, los 365 días del año, evitándose de esa manera hacer traslados innecesarios y consumo de papel innecesario, además de que se privilegian los derechos humanos de acceso a la justicia y transparencia. Lo anterior lo podemos desprender de los artículos 58-A, 58-F, 58-H, y 58-J de la LFPCA.[1349]

Asimismo, es importante dar relevancia al sistema previsto en la LFPCA para realizar las notificaciones en el juicio en línea y que coadyuva de manera importante en la agilización de la sustanciación y resolución del mismo. Dicho procedimiento consiste básicamente en que cuando el magistrado instructor o la sala del conocimiento emiten un acuerdo o resolución que por su naturaleza debe ser hecho del conocimiento especial de las partes, se envía un aviso al correo electrónico de estas para que ingresen al expediente electrónico, dentro del término de los tres días hábiles siguientes a la fecha de recepción de dicho aviso, en cuyo caso se tendrá por hecha formalmente la notificación y se expedirá la constancia respectiva; pero si no es así, al cuarto día hábil se hará la notificación por boletín electrónico. Dicho procedimiento está previsto en el artículo 58 N de ese cuerpo de leyes.[1350] Especial relevancia tiene en el procedimiento contencioso administrativo federal

1348 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 58-R. En caso que el Tribunal advierta que alguna persona modificó, alteró, destruyó o provocó la pérdida de información contenida en el sistema de justicia en línea, se tomarán las medidas de protección necesarias, para evitar dicha conducta hasta que concluya el juicio, el cual se continuará tramitando a través de un Juicio en la vía tradicional.
Si el responsable es usuario del sistema, se cancelará su firma electrónica avanzada, clave y contraseña para poder ingresar al sistema de justicia en línea y no tendrá posibilidad de volver a promover juicios en línea.
Sin perjuicio de lo anterior, y de las responsabilidades penales respectivas, se impondrá al responsable una multa de trescientas a quinientas veces el salario mínimo general vigente en el Distrito Federal al momento de cometer la infracción.

1349 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 58-A. El juicio contencioso administrativo federal se promoverá, substanciará y resolverá en línea, a través del sistema de justicia en línea que deberá establecer y desarrollar el Tribunal, en términos de lo dispuesto por el presente capítulo y las demás disposiciones específicas que resulten aplicables de esta Ley. En todo lo no previsto, se aplicarán las demás disposiciones que resulten aplicables de este ordenamiento.
Artículo 58-F. La firma electrónica avanzada producirá los mismos efectos legales que la firma autógrafa y garantizará la integridad del documento, teniendo el mismo valor probatorio.
Artículo 58-H. Los titulares de una firma electrónica avanzada, clave de acceso y contraseña serán responsables de su uso, por lo que el acceso o recepción de las notificaciones, la consulta al expediente electrónico y el envío de información mediante la utilización de cualquiera de dichos instrumentos, les serán atribuibles y no admitirán prueba en contrario, salvo que se demuestren fallas del sistema de justicia en línea.
Artículo 58-J. Cualquier actuación en el juicio en línea se efectuará a través del sistema de justicia en línea del Tribunal en términos del presente capítulo. Dichas actuaciones serán validadas con las firmas electrónicas avanzadas de los magistrados y secretarios de acuerdos que den fe, según corresponda.

1350 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 58-N. Las notificaciones que se practiquen dentro del juicio en línea, se efectuarán conforme a lo siguiente:

en línea, el ofrecimiento y exhibición de pruebas distintas a las físicas, testimoniales, e inspecciones judiciales, así como su integración al expediente electrónico, y ulterior valoración.

En principio tenemos que conforme a lo dispuesto por los artículos 14 fracción V, 15 fracción I, 17 segundo párrafo, 20 fracción VI y 21 fracción I de la LFPCA, [1351] las pruebas deben ser enunciadas y ofrecidas por las partes en sus escrito de demanda, contestación, ampliación de demanda y ampliación de contestación, según corresponda, y si se trata de documentales, incluida la resolución impugnada y sus constancias de notificación, acompañarlas a los escritos relativos; pero en tratándose del juicio en línea, además deben atenderse las reglas previstas en el artículo 58 K del mismo ordenamiento.[1352]

Sobre el particular se exige, en primer lugar, que los documentos que las partes ofrezcan como prueba, incluido el expediente administrativo, se deben exhibir de forma legible a través del sistema de justicia en línea del Tribunal, y si se trata de documentos digitales, las partes deben manifestar cual es la naturaleza de los mismos, precisándose si la reproducción digital corresponde a una copia simple, una copia certificada o al original y tratándose de esta última, si tiene o no firma autógrafa; y en el caso de los particulares esa manifestación debe ser indefectiblemente bajo protesta de decir verdad, pues si se

---

I. Todas las actuaciones y resoluciones que conforme a las disposiciones de esta Ley deban notificarse en forma personal, mediante correo certificado con acuse de recibo, o por oficio, se deberán realizar a través del sistema de justicia en línea del Tribunal.
II. El actuario deberá elaborar la minuta electrónica en la que precise la actuación o resolución a notificar, así como los documentos que se adjunten a la misma. Dicha minuta, que contendrá la firma electrónica avanzada del actuario, será ingresada al sistema de justicia en línea del Tribunal junto con la actuación o resolución respectiva y los documentos adjuntos.
III. El actuario enviará a la dirección de correo electrónico de la o las partes a notificar, un aviso informándole que se ha dictado una actuación o resolución en el expediente electrónico, la cual está disponible en el sistema de justicia en línea del Tribunal.
IV. El sistema de justicia en línea del Tribunal registrará la fecha y hora en que se efectúe el envío señalado en la fracción anterior.
V. Se tendrá como legalmente practicada la notificación, conforme a lo señalado en las fracciones anteriores, cuando el sistema de justicia en línea del Tribunal genere el acuse de recibo electrónico donde conste la fecha y hora en que la o las partes notificadas ingresaron al expediente electrónico, lo que deberá suceder dentro del plazo de tres días hábiles siguientes a la fecha de envío del aviso a la dirección de correo electrónico de la o las partes a notificar.
VI. En caso de que en el plazo señalado en la fracción anterior, el sistema de justicia en línea del Tribunal no genere el acuse de recibo donde conste que la notificación fue realizada, la misma se efectuará mediante lista y por boletín procesal al cuarto día hábil contado a partir de la fecha de envío del correo electrónico, fecha en que se tendrá por legalmente notificado.

1351 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 14. La demanda deberá indicar:
V. Las pruebas que ofrezca
Artículo 15. El demandante deberá adjuntar a su demanda:
I. Una copia de la misma y de los documentos anexos para cada una de las partes.
Artículo 17. Se podrá ampliar la demanda, dentro de los diez días siguientes a aquél en que surta efectos la notificación del acuerdo que admita su contestación, en los casos siguientes:
En el escrito de ampliación de demanda se deberá señalar el nombre del actor y el juicio en que se actúa, debiendo adjuntar, con las copias necesarias para el traslado, las pruebas y documentos que en su caso se presenten.
Artículo 20. El demandado en su contestación y en la contestación de la ampliación de la demanda, expresará:
Artículo 21. El demandado deberá adjuntar a su contestación:
I. Copias de la misma y de los documentos que acompañe para el demandante y para el tercero señalado en la demanda.

1352 Ley Federal de Procedimiento Contencioso Administrativo
Artículo 58-K. Los documentos que las partes ofrezcan como prueba, incluido el expediente administrativo a que se refiere el artículo 14, fracción V, de esta Ley, deberán exhibirlos de forma legible a través del sistema de justicia en línea del tribunal.
Tratándose de documentos digitales, se deberá manifestar la naturaleza de los mismos, especificando si la reproducción digital corresponde a una copia simple, una copia certificada o al original y tratándose de esta última, si tiene o no firma autógrafa. Los particulares deberán hacer esta manifestación bajo protesta de decir verdad, la omisión de la manifestación presume en perjuicio solo del promovente, que el documento digitalizado corresponde a una copia simple.
Las pruebas documentales que ofrezcan y exhiban las partes tendrán el mismo valor probatorio que su constancia física, siempre y cuando se observen las disposiciones de la presente Ley y de los acuerdos normativos que emitan los órganos del Tribunal para asegurar la autenticidad de la información, así como de su transmisión, recepción, validación y notificación.

omite esa manifestación, se presumirá para todos sus efectos y solo en su perjuicio, que el documento digitalizado corresponde a una copia simple.

En el precepto citado se determina, conforme a un principio de buena fe en el proceder de las partes, que las pruebas que se ofrezcan y exhiban en las condiciones apuntadas, tendrán el mismo valor probatorio de las constancias físicas que quedan en su poder, sin perjuicio de que en cierto momento puedan ser requeridas por el instructor para verificar su autenticidad.

También debemos señalar que como en el juicio contencioso administrativo, por regla general, la parte demandada es una autoridad administrativa, para que el juicio en línea sea viable es necesario el registro previo de las unidades administrativas cuyos actos son susceptibles de ser controvertidos mediante ese medio de defensa, en los módulos que existen en las sedes de las salas regionales, lo cual se desprende del cuarto transitorio[1353] del decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Procedimiento Contencioso Administrativo y de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa, publicado en el *Diario Oficial de la Federación* el 12 de junio de 2009, y conforme al diverso transitorio quinto[1354] de dicho decreto, esas autoridades tienen que instrumentar y mantener permanentemente actualizados los mecanismos tecnológicos, materiales y humanos necesarios para acceder al juicio en línea a través del sistema de justicia en línea del Tribunal.

En el caso de que alguna de las unidades mencionadas sea demanda en línea y no se encuentre registrada, todas las notificaciones que deben hacerse, incluyendo el emplazamiento, se realizarán a través del boletín procesal, hasta que se cumpla con dicha formalidad, conforme a lo dispuesto en el artículo 58 P de la LFPCA.[1355]

Por último, es menester destacar que no obstante que la modalidad de juicio en línea, que como se vio, está disponible para los ciudadanos y autoridades administrativas desde el 7 de agosto de 2011, aun no se ha generalizado su uso en el foro fiscal y administrativa, entre otras causas, porque es muy común la percepción de que es más seguro un expediente en papel que uno electrónico. Dicha percepción, que es ajena a la realidad, deriva del desconocimiento de las medidas de seguridad que existen en ámbito de las tecnologías y en

1353 Ley Federal de Procedimiento Contencioso Administrativo. Decreto publicado D.O.F el 12 de junio de 2009.
Cuarto**.** Las autoridades cuyos actos sean susceptibles de impugnarse ante el Tribunal Federal de Justicia Fiscal y Administrativa, a través del Sistema de Justicia en Línea, deberán tramitar su firma electrónica avanzada ante la Secretaría General de Acuerdos o ante la presidencia de las salas regionales, según corresponda, y registrar su dirección de correo electrónico institucional, así como el domicilio oficial de las unidades administrativas a las que corresponda su representación en los juicios contenciosos administrativos, para el efecto de emplazarlas electrónicamente a juicio, en aquellos casos en los que tengan el carácter de autoridades demandadas, a partir de los seis meses de la entrada en vigor del presente decreto, sin exceder para ello del plazo de 18 meses a que se refiere el artículo anterior.

1354 Ley Federal de Procedimiento Contencioso Administrativo. Decreto publicado DOF el 12 de junio de 2009.
Cuarto. Las autoridades cuyos actos sean susceptibles de impugnarse ante el Tribunal Federal de Justicia Fiscal y Administrativa, a través del Sistema de Justicia en Línea, deberán tramitar su firma electrónica avanzada ante la Secretaría General de Acuerdos o ante la presidencia de las salas regionales, según corresponda, y registrar su dirección de correo electrónico institucional, así como el domicilio oficial de las unidades administrativas a las que corresponda su representación en los juicios contenciosos administrativos, para el efecto de emplazarlas electrónicamente a juicio, en aquellos casos en los que tengan el carácter de autoridades demandadas, a partir de los seis meses de la entrada en vigor del presente decreto, sin exceder para ello del plazo de 18 meses a que se refiere el artículo anterior.

1355 Ley Federal de Procedimiento Contencioso Administrativo
ARTÍCULO 58-P. Las autoridades cuyos actos sean susceptibles de impugnarse ante el Tribunal deberán registrar en la Secretaría General de Acuerdos o ante la presidencia de las salas regionales, según corresponda, la dirección de correo electrónico institucional, así como el domicilio oficial de las unidades administrativas a las que corresponda su representación en los juicios contenciosos administrativos, para el efecto de emplazarlas electrónicamente a juicio en aquellos casos en los que tengan el carácter de autoridad demandada.
En el caso de que las autoridades demandadas no cumplan con esta obligación, todas las notificaciones que deben hacerse, incluyendo el emplazamiento, se harán a través del boletín procesal, hasta que se cumpla con dicha formalidad.

particular de las que se han adoptado para el juicio en línea, como la implementación de la firma electrónica que blinda todas las promociones, acuerdos, actas, oficios y resoluciones que se integran a los expedientes administrativos; o que los servidores del Tribunal se albergan en centros de alta disponibilidad (*data center*) debidamente resguardados; así como que dichos expedientes están ubicados en bases de datos de máxima seguridad a la cual solo puede accederse con claves de acceso y contraseñas, o rompiéndose las múltiples barreras tecnológicas de seguridad que existen en el sistema de justicia en línea.

Lo anterior también pese que, según estadísticas de ese órgano, al día de hoy[1356]se han incoado, substanciado y resuelto, a través de esa modalidad, sin ningún problema, poco más de 12 mil juicios, con valor superiors a los 60 mil millones de pesos, que supera por mucho la inversión de su implementación.

1356 15 de agosto 2018.

NOTAS

NOTAS

NOTAS

NOTAS

Listado de exclusión

María Solange Maqueo Ramírez

El listado de exclusión es una base de datos a través de la cual se lleva de manera gratuita un registro de todas aquellas personas físicas que han manifestado su negativa para que se efectúe el tratamiento de sus datos personales para determinadas finalidades. Es una medida preventiva y de fácil acceso, a través de la cual los responsables del tratamiento de datos personales ponen a disposición de los titulares una vía adicional al ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) y la revocación del consentimiento para limitar el tratamiento de sus datos personales.[1357]

El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) lo define en su artículo 2, fracción IV, como una "base de datos que tiene por objeto registrar de manera gratuita la negativa del titular al tratamiento de sus datos personales".

Distintos tipos de listados de exclusión

En términos de los Lineamientos del Aviso de Privacidad,[1358] emitidos por la Secretaría de Economía, además del Registro Público para Evitar la Publicidad de la Procuraduría Federal del Consumidor (PROFECO)[1359] y el Registro Público de Usuarios de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef),[1360] ambos creados para prevenir el tratamiento de datos personales con fines publicitarios o mercadotécnicos, los responsables del tratamiento podrán llevar el registro de titulares de datos personales en listados de exclusión propios, sectoriales o generales. Así, los listados de exclusión tienen como principal objetivo evitar la publicidad no deseada.

1357 Cfr. Instituto Federal de Acceso a la Información y Protección de Datos (ahora INAI). (2013). *El ABC del Aviso de Privacidad*. México, pp. 16 y 17.

1358 Lineamiento Trigésimo de los Lineamientos del Aviso de Privacidad, publicado en el *Diario Oficial de la Federación* el 17 de enero de 2017.

1359 Cfr. Ley Federal de Protección al Consumidor, publicada en el *Diario Oficial de la Federación* el 24 de diciembre de 1992 y el "Acuerdo por el que se reforman diversas disposiciones del acuerdo por el que se establecen las reglas de operación y funcionamiento del Registro Público de Consumidores, publicado en el *Diario Oficial de la Federación* el 8 de noviembre de 2007", publicado en el *Diario Oficial de la Federación* el 27 de enero de 2012.

1360 Cfr. Ley de Protección y Defensa al Usuario de Servicios Financieros, publicada en el *Diario Oficial de la Federación* el 10 de enero de 2014.

Si bien la inscripción de la negativa del titular de los datos personales, derivada del ejercicio del derecho de oposición al tratamiento de datos personales, generalmente está dirigida a las empresas o prestadores de servicios con los que no existe una relación jurídica, también puede darse el supuesto de que existe dicha relación entre ambos. En este caso, el listado de exclusión se constituye en un mecanismo que permite que los titulares manifiesten su negativa para el tratamiento de finalidades secundarias o accesorias a la principal por parte del responsable.

Finalmente, cabe advertir que la adopción de listados de exclusión propios de los responsables del tratamiento de datos personales es potestativa. No obstante, una vez adoptado y contemplado en el aviso de privacidad correspondiente, adquiere un carácter vinculante. Además, en términos de lo dispuesto por el artículo 110 del RLFPDPPP, la inscripción es gratuita y, por la misma, debe otorgarse al titular de los datos personales la correspondiente constancia de inscripción. [1361]

1361 Referencias de esta voz:
Instituto Federal de Acceso a la Información y Protección de Datos (INAI). (2013). *El ABC del Aviso de Privacidad.* México.
Ley de Protección y Defensa al Usuario de Servicios Financieros, publicada en el *Diario Oficial de la Federación* el 10 de enero de 2014.
Ley Federal de Protección al Consumidor, publicada en el *Diario Oficial de la Federación* el 24 de diciembre de 1992.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010.
Procuraduría Federal de Protección al Consumidor (Profeco), "Acuerdo por el que se reforman diversas disposiciones del acuerdo por el que se establecen las reglas de operación y funcionamiento del Registro Público de Consumidores, publicado en el Diario Oficial de la Federación el 8 de noviembre de 2007", publicado en el *Diario Oficial de la Federación* el 27 de enero de 2012.
RLFPDPPP, publicado en el *Diario Oficial de la Federación* el 21 de diciembre de 2011.
Secretaría de Economía, *Lineamientos del Aviso de Privacidad*, publicados en el *Diario Oficial de la Federación* el 17 de enero de 2017.

NOTAS

NOTAS

Mecanismos alternativos de solución de controversias

Kiyoshi Tsuru Alberú y
Patricio González Granados

Comúnmente, al mencionar términos tales como controversia, litis o justicia, nos vienen a la mente los procedimientos que se substancian ante el poder judicial; sin embargo, existen procedimientos no jurisdiccionales susceptibles de aplicación en diversas materias como civil, mercantil, familiar, penal, entre otras, que permiten la despresurización del sistema, y otorgan a las partes en conflicto mayor libertad en la composición de sus diferencias.[1362]

Las definiciones más aceptadas del concepto de "mecanismos alternativos de solución de controversias" comparten, generalmente, la siguiente estructura y composición: "El conjunto de procedimientos de índole jurisdiccional y potestativo situados fuera de sede judicial a los cuales acuden las partes en disputa con la finalidad de encontrar solución a sus diferendos, por sí o con el auxilio de un tercero imparcial".[1363]

Debido a la flexibilidad antes mencionada, existen diversos procedimientos con características peculiares que varían en función de la materia controversia en la que se enmarcan. Como se verá más adelante, a través de distintos ordenamientos de nuestra legislación nacional podemos encontrar la tipología de los medios alternativos de solución de controversias, incluyendo procedimientos de resolución de controversias en línea *Online Dispute Resolution* (ODR, por sus siglas en inglés), los cuales han ido tomando arraigo gracias al desarrollo de las tecnologías de la información y comunicación.

Por un lado, la Ley de Justicia Alternativa del Tribunal Superior de Justicia para el Distrito Federal (ahora Ciudad de México) proporciona en el artículo 2 una definición legal para mediación como el "procedimiento voluntario por el cual dos o más personas involucradas en una controversia, a las cuales se les denomina mediados, buscan y construyen una solución satisfactoria a la misma, con la asistencia de un tercero imparcial denominado mediador".

1362 Sánchez, M. y Ortíz, G. (2013, mayo-agosto). "Justicia Alternativa: Una visión panorámica", en *Revista Aequitas*. México. Núm. 3, pp. 41-43. Disponible en: http://www.stj-sin.gob.mx/assets/files/publicaciones/aequitas20.pdf.

1363 Salgado, E. (2007). *Defensa de los usuarios y consumidores*. México. Porrúa, p. 110.

Por su parte, la conciliación se puede definir como "el medio de carácter formal y privado por medio del cual dos o más personas buscan soluciones lícitas y equitativas para su conflicto, con la ayuda de un tercero imparcial llamado conciliador". [1364]

En materia de protección de datos personales, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) establece que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) podrá, dentro del procedimiento de protección de derechos, buscar una conciliación entre el titular de los datos y el responsable, siendo vinculante el acuerdo al que estos últimos lleguen y quedando el Instituto obligado a verificar su cumplimiento.[1365]

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) también prevé una etapa conciliatoria durante la tramitación del recurso de revisión en contra de una resolución dictada en un procedimiento administrativo, por el Instituto o por los órganos garantes. En relación con lo manifestado previamente sobre los procedimientos de resolución de controversias en línea, destaca que la ley en comento permite que esta conciliación se lleve presencialmente, por medios remotos o locales de comunicación electrónica, o por cualquier otro medio que la autoridad determine.[1366]

El artículo 217 de la Ley Federal del Derecho de Autor define al procedimiento administrativo de avenencia como "el que se substancia ante el Instituto, a petición de alguna de las partes para dirimir de manera amigable un conflicto surgido con motivo de la interpretación o aplicación de esta Ley".

Por su parte, el arbitraje es definido por la Organización Mundial de la Propiedad Intelectual como "un procedimiento por el cual se somete una controversia, por acuerdo de las partes, a un árbitro o a un tribunal de varios árbitros que dicta una decisión sobre la controversia que es obligatoria para las partes. Al escoger el arbitraje, las partes optan por un procedimiento privado de solución de controversias en lugar de acudir ante los tribunales".[1367] Inclusive, por la naturaleza de este tipo de procedimientos resolución de controversias, puede darse la vertiente en línea, pues al ser de carácter privado y voluntario, este procedimiento puede llevarse de manera remota haciendo uso de la tecnología.

Asimismo, encontramos un concepto denominado "junta restaurativa" en el artículo 27 de la Ley Nacional de Mecanismos Alternativos de Solución de Controversias en Materia Penal, según la cual "es el mecanismo mediante el cual la víctima u ofendido, el imputado y, en su caso, la comunidad afectada, en libre ejercicio de su autonomía, buscan, construyen y proponen opciones de solución a la controversia, con el objeto de lograr un acuerdo que atienda las necesidades y responsabilidades individuales y colectivas, así como la reintegración de la víctima u ofendido y del imputado a la comunidad y la recomposición del tejido social".

1. Antecedentes históricos

La legislación mexicana ya contemplaba desde hace varios años, como parte de algunos procesos judiciales, audiencias de conciliación. Sin embargo, se le consideraba como una etapa dentro del juicio, un requisito del procedimiento y no como uno independiente. Es

1364 Pérez, M. (2018, enero-abril). "Mediación familiar en el Distrito Federal. Un acercamiento al procedimiento y a su regulación", en *Boletín Mexicano de Derecho Comparado*. México. Núm.151. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/4074/5238.

1365 Artículo 54 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

1366 Artículo 106 y siguientes de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1367 Organización Mundial de la Propiedad Intelectual. Disponible en: http://www.wipo.int/amc/es/arbitration/what-is-arb.html.

hasta 1997 que se promulga la primera ley destinada a regular la justicia alternativa como una herramienta autónoma, la Ley de Justicia Alternativa del Estado de Quintana Roo. A partir de esa fecha, comienzan a crearse leyes análogas en los distintos estados de la República Mexicana. Sin embargo, hasta el 18 de junio de 2008 se hace un reconocimiento a nivel constitucional de los mecanismos alternativos de solución de controversias dentro de una reforma al sistema judicial.[1368]

Esta reforma generó un cambio de paradigma en el sistema mexicano de justicia, adoptando una óptica de justicia retributiva que incluye de manera generalizada, con criterios, principios y estándares uniformes, los mecanismos alternativos de solución de controversias en la legislación nacional.[1369]

Este cambio sustancial rompió con la interpretación conservadora que el Poder Judicial de la Federación había acogido hasta entonces. Anteriormente, el Pleno de la Suprema Corte de Justicia de la Nación (SCJN) había sostenido, entre otros criterios, que el principio de justicia pronta y expedita, establecido en el artículo 17 constitucional, era transgredido si se obligaba a las partes a someterse a un procedimiento conciliatorio previamente a acudir a los tribunales.[1370]

2. Análisis técnico

Los mecanismos más conocidos son la mediación, la conciliación y el arbitraje, aunque es posible enlistar también la negociación y, de incorporación más reciente a la legislación mexicana, la junta restaurativa.

La teoría general del proceso denomina a los mecanismos en los que las mismas partes involucradas proponen y acuerdan las decisiones que se tomaron dentro del proceso, como autocompositivos. Si un tercero intervino en la proposición o la toma de decisiones, se les denominará heterocompositivos. La principal diferencia entre este último tipo de mecanismos radica en los límites de la intervención del tercero ajeno al conflicto, ya que mientras un mediador únicamente puede ayudar a facilitar la comunicación entre las partes para que lleguen a un acuerdo que ponga fin a su conflicto de intereses, un conciliador, además, puede proponer posibles soluciones al conflicto.[1371]

En otras palabras, se puede decir que los medios alternativos de solución de conflictos constituyen mecanismos convencionales, expeditos y económicos de solución de controversias; los cuales se pueden resumir en: i) los sistemas de negociación que buscan crear un ambiente que permita a las partes alcanzar una solución razonable por sí mismos; ii) se extienden a los sistemas que cuentan con la intervención de un tercero ajeno a la disputa, que auxiliando (mediación) o proponiendo (conciliación) coopera para que éstas lleguen a un acuerdo por sí mismas y iii) alcanza a las modalidades adversas a través de las cuales el tercero decide o resuelve (arbitraje).[1372]

1368 Sánchez, M. y Ortiz, G. *op. cit.*, pp. 27-28.

1369 Exposición de motivos de la reforma el artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. (2016). México. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/87527/MASC.pdf.

1370 Tesis P. CXII/97 del Pleno de la Suprema Corte de Justicia de la Nación, publicada en el *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo VI, julio de 1997, página 15.

1371 Márquez, M. y De Villa Cortés, J., "Medios alternos de solución de conflictos", en Ferrer Mac-Gregor, Eduardo *et. al.* (coords.) *Derechos humanos en la Constitución*. Comentarios de jurisprudencia constitucional e interamericana. Tomo II. UNAM, Instituto de Investigaciones Jurídicas-Suprema Corte de Justicia de la Nación-Fundación Konrad Adenauer, p. 1588. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3568/41.pdf.

1372 Nava, W. y Breceda, J. (2017, julio-diciembre). "Mecanismos alternativos de resolución de conflictos: un acceso a la justicia consagrado como derecho humano en la Constitución Mexicana", en *Revista Mexicana de Derecho Constitucional*. México. Núm. 37. Disponible en: https://revistas.juridicas.unam.mx/index.php/cuestiones-constitucionales/article/view/11457/13362.

Como se refirió a partir de la reforma constitucional de 2008, las entidades federativas fueron incorporando en su marco jurídico mecanismos alternativos de solución de controversias (MARC), aunque con un nivel de desarrollo muy variable. Así, encontramos entidades en las cuales se ha creado un centro de justicia alternativa o un centro de mediación y conciliación (la denominación puede variar, dependiendo de cada estado), en donde se ofrecen los MARC que normalmente tratan exclusivamente de procedimientos de mediación y conciliación, aunque hay algunos estados que también hacen referencia a otros mecanismos alternativos como la negociación o el procedimiento restaurativo, por ejemplo, lo que también marca una diferencia importante entre unos y otros estados.[1373]

A continuación nos permitimos señalar a manera de ejemplo algunas de las regulaciones que, a nivel estatal, federal e internacionales, prevén mecanismos alternativos de solución de controversias como método de gestión de conflictos.

La antes citada Ley de Justicia Alternativa del Tribunal Superior de Justicia para el Distrito Federal señala como su objetivo: "Reglamentar el párrafo cuarto del artículo 17 y el párrafo sexto del artículo 18 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) y regular la mediación como método de gestión de conflictos para la solución de controversias entre particulares cuando éstas recaigan sobre derechos de los cuales pueden aquellos disponer libremente, sin afectar el orden público, basado en la autocomposición asistida".

La Ley Nacional de Mecanismos Alternativos de Solución de Controversias en Materia Penal introduce una figura de justicia alternativa denominada junta restaurativa. Durante dicha junta se deberá identificar la naturaleza y circunstancias de la controversia, así como las necesidades de los intervinientes y sus perspectivas individuales, evaluar su disposición para participar en el mecanismo, la posibilidad de realizar la reunión conjunta y las condiciones para llevarla a cabo. De esta manera, la persona facilitadora del mecanismo podrá concretar acuerdos que se acepten como resultado de la sesión de la junta, con base en las propuestas planteadas por todas las partes.

Es de suma importancia señalar que el Código Federal de Procedimientos Civiles le otorga fuerza vinculatoria a las transacciones y/o convenios extrajudiciales, así como a laudos arbitrales privados de carácter no comercial (artículo 405), sujeto al cumplimiento de ciertos requisitos (artículo 569), incluyendo aquellos de dictados en el extranjero (artículo 571).

Asimismo, el Código de Comercio señala en su artículo 1051 que una controversia mercantil puede ventilarse a través de un procedimiento convencional ante tribunales, o bien, mediante un procedimiento arbitral. Inclusive, en su artículo 1391, fracción VIII, prevé que "los convenios celebrados en los procedimientos conciliatorios tramitados ante la Procuraduría Federal del Consumidor o ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, así como los laudos arbitrales que éstas emitan" traerán aparejada ejecución.

En este sentido, La Ley Federal de Protección al Consumidor contempla un procedimiento conciliatorio que incluye amplias atribuciones para que el conciliador conduzca el proceso e, inclusive, para que imponga medidas de apremio en caso de que el proveedor en cuestión no comparezca a la audiencia o no rinda un informe relacionado con los hechos materia de la controversia.[1374]

1373 Márquez, M. y De Villa Cortés, J., "Medios alternos de solución de conflictos", en Ferrer Mac-Gregor, Eduardo *et. al.* (coords.) *Derechos humanos en la Constitución*. Comentarios de jurisprudencia constitucional e interamericana. Tomo II. UNAM, Instituto de Investigaciones Jurídicas-Suprema Corte de Justicia de la Nación-Fundación Konrad Adenauer, pp. 1592-1593.

1374 Artículos 111 a 116 de la Ley Federal de Protección al Consumidor.

Debido a la flexibilidad y conveniencia de este procedimiento, la Procuraduría Federal de Protección al Consumidor desarrolló la plataforma Concilianet, que es un módulo de solución de controversias en línea, en el que se desahogan las audiencias de conciliación vía internet con aquellos proveedores de bienes y servicios con quienes se tiene celebrado un convenio de colaboración para tal efecto.

En caso de que no se llegue a un acuerdo conciliatorio, la ley en comento establece que el conciliador deberá exhortar a las partes para que designen como árbitro a la Procuraduría Federal del Consumidor o a algún árbitro independiente para resolver la disputa, y deberá seguirse el procedimiento arbitral establecido para tal efecto.[1375]

Por su parte, la Ley de Protección y Defensa al Usuario de Servicios Financieros contempla también un extenso título para procedimientos de conciliación y arbitraje.[1376]

De igual manera encontramos otras disposiciones que facilitan a ciertos sujetos de derecho a asumir funciones de mediadores o árbitros. Por ejemplo, la Ley de Cámaras Empresariales y sus Confederaciones establece en su artículo 7, fracción quinta, que sus miembros pueden fungir como mediadores o árbitros, nacionales o internacionales de actividades comerciales, servicios de turismo o industriales, en tanto que la Ley Federal de Correduría Pública señala en el artículo 6, fracciones I y IV, que los corredores públicos podrán mediar y ser árbitros en el ámbito mercantil de los corredores.

Como se comentó previamente, la Ley Federal del Derecho de Autor contiene dos capítulos que abordan el procedimiento de avenencia (conciliación) y el procedimiento de arbitraje en materia de derechos de autor. Esta ley establece de manera opcional para las partes que vean afectados alguno de sus derechos tutelados por esa ley, optar entre hacer valer acciones judiciales o sujetarse a un procedimiento administrativo de avenencia. También establece que en caso de no lograrse la avenencia, el Instituto exhortará a las partes para que se acojan al arbitraje establecido en la misma ley.

El procedimiento de avenencia es sustanciado por el Instituto Nacional del Derecho de Autor con el fin de dirimir de manera amigable un conflicto surgido con motivo de la interpretación o aplicación de la citada ley (artículos 217 y 218). Esta avenencia puede clasificarse como una conciliación en la que el Instituto funge como conciliador, y si bien, no es obligatorio lograr un acuerdo durante el mismo, sí es obligatorio de conformidad con el artículo 218 fracción 3, que las partes asistan a ésta, de lo contrario, pueden ser multadas.

A este respecto podemos cuestionarnos si esta disposición resulta ilegal en tanto que viola el principio de voluntariedad de los mecanismos que establece la misma Ley Federal del Derecho de Autor en su artículo 217. Si bien la jurisprudencia no se ha manifestado respecto a la materia de propiedad intelectual, en materia penal, los tribunales han señalado que "el principio rector de voluntariedad, de acuerdo con el cual, la participación de los intervinientes debe ser por propia decisión, libre de toda coacción y no por obligación; es decir, no puede obligarse al requerido a asistir y participar en el mecanismo alternativo respectivo".[1377]

En la misma ley se establece un segundo mecanismo alternativo, el arbitraje, el cual estará regulado conforme a la ley supletoria, al Código de Comercio. Mediante una cláusula compromisoria o un compromiso arbitral, las partes en conflicto podrán acordar someterse a un procedimiento arbitral que será resuelto por árbitros autorizados por el Instituto.

1375 Artículos 117 a 122 de la Ley Federal de Protección al Consumidor.

1376 Artículos 60 a 84 Quinquies de la Ley de Protección y Defensa al Usuario de Servicios Financieros.

1377 Tesis XX.2o.P.C. J/1. *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo III, libro 53, abril 2018, p. 1844.

De acuerdo con la Ley Federal del Derecho de Autor, tanto el convenio firmado por las partes como resultado de un procedimiento de avenencia (artículo 218 fracción 4), como los laudos emitidos por el Instituto (artículo 226 fracción 4) tendrán el carácter de cosa juzgada y título ejecutivo.

En materia de protección de datos personales, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) contempla en su artículo 54 la facultad que tiene el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales para buscar una conciliación entre el titular de los datos personales y el responsable. En caso de que las partes lleguen a un acuerdo de conciliación, éste se hará constar por escrito y tendrá efectos vinculantes.

Ahora bien, en el capítulo IV del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) se establece la posibilidad de crear autorregulación vinculante en materia de protección de datos personales. Estos esquemas de autorregulación son mecanismos que permiten a los sujetos obligados implementar políticas y sistemas de gestión interna, así como mecanismos de control para regular la actuación de sus agremiados como responsables del tratamiento de datos personales. En el artículo 80 del RLFPDPPP se determina que dichos esquemas serán vinculantes para quienes se adhieran a ellos, previendo en la fracción 9 del citado artículo, la posibilidad de encauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.

Cabe mencionar que ni la ley y ni el reglamento antes referidos, contemplan un título, capítulo o algún artículo específico aborde la conciliación como mecanismo de solución de controversias, como sí lo hace la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual en su artículo 107 prevé específicamente un procedimiento de conciliación para los sujetos a los que va dirigida dicha ley, que "en el ámbito federal, estatal y municipal, son: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos".

Resulta trascedente señalar que las instituciones no se limitan a estructuras nacionales o locales, sino que tienen un ámbito extraterritorial (respecto al Estado), al observar tribunales, cortes y comisiones a nivel internacional. Para citar algunos ejemplos, encontramos que a la mediación y la conciliación como medios para resolver conflictos en el artículo 2007 del anterior Tratado de Libre Comercio de América del Norte, celebrado entre México, Estados Unidos y Canadá en 1992.

Asimismo, la Convención Interamericana sobre Arbitraje Comercial regula a nivel regional las reglas procedimentales de la Comisión Interamericana de Arbitraje para el caso de ausencia de normas preestablecidas por las partes.

Por su parte, la Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras establece como obligación de los países firmantes el reconocimiento y ejecución de los laudos arbitrales extranjeros.

De acuerdo con la jurisprudencia en México, el acceso a la justicia como derecho fundamental no solo se garantiza a través de la actividad judicial,[1378] sino que "debe concluirse que tanto la tutela judicial como los mecanismos alternos de solución de controversias, se establecen en un mismo plano constitucional y con la misma dignidad y tienen como objeto, idéntica finalidad, que es, resolver los diferendos entre los sujetos que se encuentren bajo el imperio de la ley en el Estado mexicano".[1379]

1378 Tesis: VII.1o.C.33 C. *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo III, libro 32, julio de 2016, p. 2163.

1379 Tesis III.2o.C.6 K. *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo 3, libro XXV, octubre de 2013, p. 1723.

Es conveniente enfatizar que las particularidades básicas de estos sistemas alternos radican en que las partes involucradas tienen la oportunidad de resolverlo de una manera rápida, económica, flexible y efectiva, encontrando el procedimiento que mejor se adapta a sus necesidades y circunstancias particulares. Además, estos sistemas se rigen por principios como la confidencialidad, neutralidad, imparcialidad, independencia, colaboración y voluntariedad, por destacar los más importantes.[1380]

Asimismo, la especialización de una materia como derechos de autor la cual ya hemos mencionado, o como derecho laboral, permiten la aplicación de mecanismos alternos. A partir de la ejecutoria "La Corona", de febrero de 1924, la Suprema Corte de Justicia de la Nación, reconoció a las juntas de conciliación y arbitraje como tribunales de derecho de competencia especializada.[1381]

En conclusión, los mecanismos alternativos de solución de controversias permiten al sistema de justica incluir a todos los actores de un conflicto en la búsqueda de una solución adecuada que favorezca el restablecimiento de la paz social, disminuya la intervención del Estado mexicano como ente punitivo y garantice el equilibrio en la satisfacción de las pretensiones de las partes involucradas en una controversia. Como bien lo adelantaba Carnelutti al hablar del proceso, "las leyes no son más que instrumentos, pobres e inadecuados, casi siempre, para tratar de dominar a los hombres cuando, arrastrados por sus intereses y sus pasiones, en vez de abrazarse como hermanos, tratan de despedazarse como lobos".[1382] Es precisamente esa imperfección del proceso la que pretende aminorarse con los mecanismos alternativos de solución de controversias.

Medidas de apremio

Gabriel López López

Son facultades de carácter coercitivo otorgadas por la Ley a la autoridad competente con el propósito de garantizar el cumplimiento eficaz e inmediato de sus determinaciones, dentro o fuera de un procedimiento administrativo.

Para Manuel Lucero Espinosa las medidas de apremio en el sistema jurídico mexicano son aquellos instrumentos jurídicos a través de los cuales un juzgador o una autoridad en un procedimiento administrativo pueden hacer cumplir coactivamente sus requerimientos o determinaciones.[1383]

1. Delimitación conceptual y conceptos relacionados

En la materia de protección de datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y los órganos garantes locales serán los encargados de aplicar las medidas de apremio correspondientes para garantizar el cumplimiento de sus determinaciones. Éstas se encuentran reguladas en los

1380 Nava, W. y Breceda, J. (2017, julio-diciembre). "Mecanismos alternativos de resolución de conflictos: un acceso a la justicia consagrado como derecho humano en la Constitución Mexicana", en *Revista Mexicana de Derecho Constitucional*. México. Núm. 37. p. 210.

1381 Sánchez-Castañeda, A. (2014). Amparo laboral en Ferrer Mac-Gregor, E. *et. al.* (coords.), *Diccionario de derecho procesal constitucional y convencional.* México. Instituto de Investigaciones Jurídicas, serie Doctrina jurídica, núm. 692-693, p. 92. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3683/27.pdf

1382 Carnelutti, F. (2007). *Cómo se hace un proceso*. Editorial Temis. Tercera edición. Colombia.

1383 Lucero, M. (2017). *Procedimiento de Responsabilidad Administrativa, respecto de faltas graves.* Tribunal Federal de Justicia Administrativa. México. Disponible en: http://cesmdfa.tfja.gob.mx/mat/SNA_MagMANUEL_LUCERO.pdf

artículos 152 a 162 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Particularmente, el artículo 153 de la LGPDPPSO establece como medidas de apremio la amonestación pública (ejecutada por el superior jerárquico inmediato del infractor con el que se relacione) y la multa (que se hará efectiva a través de la Servicio de Administración Tributaria (SAT) o las secretarías de finanzas de las entidades federativas, según corresponda) equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida Administrativa (UMA).[1384] Éstas deberán aplicarse e implementarse en un plazo máximo de 15 días, contados a partir de que sea notificada la medida de apremio al infractor.

Las medidas de apremio son actos definitivos e independientes del procedimiento dictado, es decir, su existencia y ejecución no dependerán del procedimiento en el que fueron dictadas, ya que su principal objetivo, como ya se mencionó anteriormente, es hacer cumplir coactivamente determinaciones o requerimientos adoptados por la autoridad.

Lo anterior es así porque cuando se hace efectiva alguna de las medidas de apremio, el afectado podría promover en contra de la misma un juicio contencioso administrativo ante el Tribunal Federal de Justicia Administrativa (TFJA), no con motivo de la substanciación de un procedimiento administrativo, o las posibles violaciones que pudieron ocurrir en éste o en la resolución que le puso, sino como un acto definitivo e independiente del que emana, ya que por su naturaleza su existencia no depende de lo que se resuelva en el procedimiento administrativo en el que se haya adoptado la medida.

Tan es así que la propia LGPDPPSO prevé, en su artículo 162, como supuesto normativo que en contra de la imposición de medidas de apremio procede el recurso correspondiente ante el PJF, o en su caso ante el Poder Judicial correspondiente en las entidades federativas.

Sirve de apoyo a lo anterior la tesis que a la letra dice:

> MULTA IMPUESTA COMO MEDIDA DE APREMIO CON FUNDAMENTO EN EL ARTÍCULO 25, FRACCIÓN II, DE LA LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR. ES IMPUGNABLE A TRAVÉS DEL JUICIO CONTENCIOSO ADMINISTRATIVO ANTE EL TRIBUNAL FEDERAL DE JUSTICIA FISCAL Y ADMINISTRATIVA. Las medidas de apremio constituyen instrumentos jurídicos a través de los cuales el juzgador o la autoridad en el procedimiento administrativo pueden hacer cumplir coactivamente sus requerimientos o determinaciones, lo que implica que, una vez dictadas, se convierten en actos definitivos e independientes del procedimiento del que derivaron; por ello, cuando una autoridad perteneciente a la Procuraduría Federal del Consumidor, en el desempeño de sus atribuciones legales, impone como medida de apremio la multa prevista en el indicado precepto, ésta es impugnable a través del juicio contencioso administrativo ante el Tribunal Federal de Justicia Fiscal y Administrativa, en términos de la fracción III del artículo 14 de su Ley Orgánica, en virtud del fundamento legal en que se apoyó su emisión, esto es, una norma administrativa federal y por la independencia que guarda la multa en relación con el procedimiento en el que se dictó (2a./ J. 153/2013).[1385]

1384 Artículo 153. El Instituto y los organismos garantes podrán imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:
I. La amonestación pública, o
II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.
El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y los organismos garantes y considerados en las evaluaciones que realicen éstos. En caso de que el incumplimiento de las determinaciones del Instituto y los organismos garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163 de la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

1385 Tesis 2a./ J. 153/2013. *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo II, enero de 2014, p. 1534.

En caso de que el sujeto obligado decidiera incumplir con alguna de las medidas de apremio impuesta por el INAI o los organismos garantes, dicho incumplimiento será difundido en los portales de obligaciones y será considerada en las evaluaciones que realicen éstos.

Si a pesar de la ejecución de las medidas de apremio no se cumpliere con la resolución, el artículo 154 de la LGPDPPSO señala que se le requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora. De persistir el incumplimiento, se aplicarán sobre aquéllas medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista la autoridad competente en materia de responsabilidades.

Medidas compensatorias

Jorge Antonio Orta Villar

Las medidas compensatorias son mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios de comunicación masiva u otros mecanismos de amplio alcance, en lugar de poner a disposición el aviso a cada titular, de manera personal o directa. La definición de este concepto previsto en la normatividad aplicable de sector privado es la siguiente: "Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros mecanismos de amplio alcance, que se instrumentan de manera excepcional cuando al responsable le resulta imposible poner a disposición de cada titular, de manera directa o personal, el aviso de privacidad, o ello exige esfuerzos desproporcionados".

Las medidas compensatorias tienen por efecto cumplir con la obligación de difundir y dar a conocer el aviso de privacidad del responsable a los titulares cuyos datos personales son sujetos de tratamiento. Aplicará el uso de estas medidas cuando al responsable le resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados en razón al número de titulares o a la antigüedad de los datos.

Ante tales imposibilidades o dificultades, el responsable podrá instrumentar las medidas compensatorias de acuerdo con los criterios generales expedidos por el Instituto,[1386] bajo los cuales podrán utilizarse los medios que se establecen en el artículo 35 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) de la materia.

El artículo antes referido a la letra se lee:

> Artículo 35. Las medidas compensatorias de comunicación masiva deberán contener la información prevista en el artículo 27[1387] del presente Reglamento y se darán a conocer a través de avisos de privacidad que se publicarán en cualquiera de los medios siguientes:
>
> I. diarios de circulación nacional;
>
> II. diarios locales o revistas especializadas, cuando se demuestre que los titulares de los datos personales residan en una determinada entidad federativa o pertenezcan a una determinada actividad;
>
> III. página de internet del responsable;
>
> IV. hiperenlaces o hipervínculos situados en una página de Internet del Instituto, habilitados para dicho fin, cuando el responsable no cuente con una página de Internet propia;

1386 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

1387 Artículo 27 del Reglamento… cuando los datos personales sean obtenidos directamente del titular, el responsable deberá proporcionar de manera inmediata al menos la siguiente información: I. La identidad y domicilio del responsable; II. Las finalidades del tratamiento, y III. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad…

V. carteles informativos;

VI. difusión en cápsulas informativas en radiodifusoras, o

VII. otros medios alternos de comunicación masiva.

Los casos que no actualicen los criterios generales emitidos por el Instituto requerirán su autorización expresa previo a que el responsable emprenda la instrumentación de alguna medida compensatoria.

Para estos casos, el responsable deberá realizar una solicitud para autorización de medidas compensatorias, solicitud que se interpondrá ante el Instituto, quien deberá atenderla. El responsable presentará su solicitud directamente ante el Instituto o a través de cualquier otro medio que la misma autoridad haya habilitado para tal efecto. La solicitud deberá contener la siguiente información:

a) nombre, denominación o razón social del responsable que la promueva y, en su caso, de su representante, así como copia de la identificación oficial que acredite su personalidad y original para su cotejo. En el caso del representante, se deberá presentar copia del documento que acredite la representación del responsable y original para su cotejo;

b) domicilio para oír y recibir notificaciones, y nombre de la persona autorizada para recibirlas;

c) tratamiento al que pretende aplicar la medida compensatoria y sus características principales, tales como finalidad; tipo de datos personales tratados; si se efectúan transferencias; particularidades de los titulares, entre ellas edad, ubicación geográfica, nivel educativo y socioeconómico, entre otros;

d) causas o justificación de la imposibilidad de dar a conocer el aviso de privacidad a los titulares o el esfuerzo desproporcionado que esto exige. El responsable deberá informar sobre el número de titulares afectados, antigüedad de los datos, si existe o no contacto directo con los titulares, y su capacidad económica;

e) tipo de medida compensatoria que pretende aplicar y por qué periodo la publicaría;

f) texto propuesto para la medida compensatoria y

g) documentos que el responsable considere necesarios presentar ante el Instituto.

Con la interposición de la solicitud realizada por el responsable se tendrá por iniciado el procedimiento para la autorización de medidas compensatorias. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) contará con 10 días para emitir la resolución correspondiente. Los 10 días con los que la autoridad cuenta para resolver correrán a partir del día siguientes a la recepción de la solicitud de medida compensatoria.

Si el INAI no emite un acuerdo mediante el cual conste su resolución a la petición dentro del plazo establecido antes mencionado, aplicará una *afirmativa ficta* en beneficio del responsable solicitante, es decir, que la solicitud de medida compensatoria se entenderá como autorizada.

Previo a que se emita una resolución, para los efectos de poderla emitir, el Instituto valorará los esfuerzos desproporcionados para dar a conocer el aviso de privacidad, tomando en cuenta los siguientes factores:

a) el número de titulares;

b) la antigüedad de los datos;

c) la capacidad económica del responsable;

d) el ámbito territorial y sectorial de operación del responsable y

e) la medida compensatoria a utilizar.

Cuando a criterio del INAI la medida compensatoria propuesta no cumple con el principio de información, podrá proponer al responsable la adopción de alguna medida compensatoria alterna a la propuesta por el responsable en su solicitud.

Esta propuesta será hecha del conocimiento del responsable, a fin de que éste exponga lo que a su derecho convenga en un plazo no mayor a cinco días, contados a partir del día siguiente en que haya recibido la notificación de la propuesta.

Si el responsable no responde en el plazo que señala el párrafo anterior, el Instituto resolverá con los elementos que consten en el expediente.

Cuando el Instituto determine que el responsable no justificó la imposibilidad de dar a conocer el aviso de privacidad al titular o que ello exige esfuerzos desproporcionados, no será autorizado el uso de medidas compensatorias.

La autorización que en su caso otorgue el Instituto estará vigente mientras no se modifiquen las circunstancias bajo las cuales se autorizó la medida compensatoria.

Se entenderá que resulta imposible o esfuerzos desproporcionados de acuerdo con las fracciones II y III del artículo tercero de los criterios generales explican que lo anterior ocurre cuando:

a) el responsable se enfrenta a alguna imposibilidad de hecho para dar a conocer a los titulares el aviso de privacidad, situación que ocurre cuando el responsable no cuente con los datos personales necesarios que le permitan tener contacto con el titular (como, número telefónico, dirección, correo electrónico, entre otros), ya sea porque no existen en sus archivos, registros, bases de datos, o bien, porque los mismos se encuentran desactualizados, son incorrectos, incompletos o inexactos o

b) dar a conocer el aviso de privacidad de manera personal o directa a los titulares requiere de esfuerzos que le resulten desproporcionados al responsable. Esto es, existen esfuerzos desproporcionados, cuando el número de titulares sea tal, que el hecho de poner a disposición de cada uno de ellos el aviso de privacidad, de manera personal o directa, implique al responsable un costo excesivo, al considerar su capacidad económica, o comprometa su estabilidad financiera, las actividades propias de su negocio o la viabilidad de su presupuesto programado; o bien que dicha actividad sea disruptiva, de manera significativa, de aquellas que el responsable lleva a cabo cotidianamente.

Medidas correctivas en caso de vulneraciones de seguridad

Christian Paredes González

La normatividad de datos personales establece la obligación de que cuando se actualice una vulneración de seguridad de datos personales,[1388] el responsable debe analizar las causas por las que se presentó el incidente e implemente medidas correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.[1389]

En primer lugar, en el orden privado, es el artículo 66 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) el que de manera clara instruye la adopción de las medidas correctivas en caso de vulneración al establecer que: "En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita".

En el orden del derecho público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) indica que cuando se presente una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso y evitar que la vulneración se repita.[1390]

En cuanto a la determinación de las medidas de seguridad, la *Guía para la Implementación del Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP),[1391] publicada en 2015, establece que como parte del paso 8 de la metodología para establecer un sistema de gestión de seguridad de datos personales (SGSDP), se deberán comprender revisiones y/o auditorías en las que se incluya la revisión de esquemas de atención a vulneraciones de seguridad de datos personales.

1388 El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares considera vulneraciones de seguridad a los siguientes incidentes:
Vulneraciones de seguridad
Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:
I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.
Por su parte, el artículo 38 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala:
Artículo 38. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:
I. La pérdida o destrucción no autorizada;
II. El robo, extravío o copia no autorizada;
III. El uso, acceso o tratamiento no autorizado, o
IV. El daño, la alteración o modificación no autorizada.

1389 Medidas correctivas en caso de vulneraciones de seguridad
Artículo 66. En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.

1390 Artículo 37. En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.

1391 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2015). *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementación_SGSDP(Junio2015).pdf

Destaca la GISGSDP que la organización debe contar con procedimientos para tomar acciones que permitan el manejo de las vulneraciones de seguridad que puedan ocurrir, considerando al menos:

a) la identificación de la vulneración;
b) la notificación de la vulneración y
c) la remediación del incidente.

Debemos considerar que en lo general, la pretensión principal de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) —en su artículo 20— es la de preservar el principio de responsabilidad ya en lo particular las medidas correctivas señaladas en el RLFPDPPP y la LGPDPPSO se identifican con la etapa del inciso c) del proceso de gestión de vulneraciones. Así, respecto de la remediación del incidente, la GISGSDP señala que una vez identificada la vulneración y después de haber realizado la respectiva notificación, se debe profundizar en el análisis de las causas del incidente para establecer medidas correctivas. Sobre las medidas correctivas se ha previsto que estas incluyen medidas inmediatas para reducir los efectos de la vulneración, así como medidas a largo plazo, por ejemplo, implementar controles técnicos o actualizar las políticas del SGSDP para evitar que incidentes similares o relacionados vuelvan a ocurrir.

Medidas de seguridad

Uciel Fragoso Rodríguez

Las medidas de seguridad son elementos de control que tienen el objetivo de garantizar la confidencialidad, integridad y disponibilidad de la información. En el caso de los datos personales, las medidas de seguridad se implementan a lo largo de su ciclo de vida para evitar que los datos sean expuestos, alterados o bloqueados por personas o entidades no autorizadas.

Las medidas de seguridad se clasifican por su naturaleza en:

a) administrativas;
b) operacionales y
c) tecnológicas.

Las medidas de seguridad administrativas son elementos o acciones que se enfocan generalmente a los roles y responsabilidades asignados a las personas, grupos de personas o entidades que intervienen en algún paso en el tratamiento de la información.

Algunos ejemplos de medidas de seguridad administrativas para protección de la información son entre otros:

a) control de acceso;
b) programas de concientización y capacitación;
c) creación de normas y políticas y
d) contratos y acuerdos de confidencialidad.

El control de acceso tiene el objetivo de permitir únicamente a las personas autorizadas acceder la información con los permisos adecuados. El control de acceso está compuesto por dos funciones: la autenticación y la autorización.

La autenticación es el procedimiento a través del cual se verifica la identidad de una persona, grupo de personas o en general a cualquier entidad, para ello, se solicita a la entidad que se quiere autenticar, una evidencia que compruebe su identidad.

La evidencia, conocida como factor de autenticación se clasifica de la siguiente manera:

a) Factor 1: "algo que sé", como por ejemplo una contraseña, un código, una respuesta, una imagen, entre otros.
b) Factor 2: "algo que tengo", como por ejemplo un *token*, un certificado digital, una *cookie*, una credencial de proximidad, entre otros.
c) Factor 3: "algo que soy", refiere a cualquier elemento biométrico, por ejemplo, la huella digital, reconocimiento facial, reconocimiento de voz, patrón de venas, patrón de la mano, entre otros.

Por otro lado, la autorización es el conjunto de acciones para garantizar que la información accedida y el tipo de tratamiento sea el adecuado. Una correcta autorización se logra mediante la adecuada definición de roles y asignación de privilegios. En términos de seguridad de la información, existe dos principios básicos relacionados con la autorización: separación de actividades y asignación del mínimo privilegio.

Los programas de concientización y capacitación son de las medidas de seguridad más efectivas y eficientes. Mediante un programa de difusión de cultura de la seguridad de la información, las personas están conscientes de la sensibilidad de la información que están manejando. Y los programas de capacitación permiten que dicho manejo de la información se haga correctamente y se eviten errores que pongan en peligro la confidencialidad, integridad y disponibilidad de la información.

Las normas y políticas constituyen una medida de seguridad administrativa que permite establecer las directrices para el correcto uso de la información en términos de su seguridad. Las normas y políticas de seguridad de la información, deben estar incluidas en un marco normativo que defina claramente el gobierno de normatividad, el ciclo de vida y la estandarización de la documentación.

Los contratos y acuerdos de confidencialidad se consideran medidas de seguridad administrativas ya que establecen claramente las responsabilidades de las personas que manejan información en términos de seguridad de la información. Las obligaciones que emanan de los contratos y acuerdos resultan en un tratamiento más seguro de la información y deja claro las sanciones correspondientes en caso de un manejo inadecuado e inseguro.

Las medidas de seguridad operacionales consisten en la implementación de procesos o modificación de tareas dentro de un proceso con el objetivo de garantizar la seguridad de la información.

Ejemplo de medidas de seguridad operacionales tenemos:

a) administración de activos;
b) administración de la configuración;
c) auditorías y
d) monitoreo y registro.

La administración de activos consiste en crear un inventario de activos de la organización para clasificarlos y priorizados de acuerdo con su criticidad para la organización. La información, los procesos, la infraestructura tecnológica, los proyectos, entre otros, constituyen activos que deben estar perfectamente identificados y caracterizados para asegurarlos adecuadamente.

La administración de la configuración se considera una buena medida de seguridad ya que permite establecer guías para la configuración segura de componentes *hardware* y *software*, así como el establecimiento de un proceso de control de cambios en la configuración. Existen estándares o mejores prácticas para la creación de guías de configuración, pero en general las guías de configuración se crean como resultados del análisis de riesgo realizado y de la propia experiencia de las personas encargadas de la administración de los componentes a configurar.

Las auditorías son medidas de seguridad del tipo procedimiento ya que permiten identificar no conformidades en las diferentes fases donde existe tratamiento de información. Las auditorías pueden ser internas o externas y ayudan a realizar ajustes en los procedimientos enfocados a garantizar la seguridad de la información, asimismo, permiten encontrar la causa raíz de algún incidente de seguridad.

El monitoreo y registro de eventos constituyen medidas de seguridad muy importantes ya que permiten visualizar cualquier evento que pueda poner en peligro la seguridad de la información. Con un adecuado mecanismo de monitoreo y registro de eventos se pueden implementar procedimientos de seguridad preventivos, así como también procedimientos de respuesta a incidentes.

Las medidas de seguridad tecnológicas están conformadas por soluciones de *hardware* y *software* que mitigan los riesgos que pudiera tener la información cuando es generada, procesada, almacenada o eliminada en sistemas informáticos.

Algunos ejemplos de medidas de seguridad tecnológica son:

a) protección de redes y comunicaciones;
b) protección de datos y aplicaciones y
c) detección de *malware*, *spam* e intrusos.

La protección de redes y comunicaciones se implementa con dispositivos que protegen el flujo de la información. Existen diversas técnicas de protección para la información que está en circulación como por ejemplo el empleo de canales cifrados que garantizan que la información en caso de ser interceptada no pueda ser interpretada. Otra medida de seguridad para el flujo de la información es mediante reglas de filtrado que permiten circular solo la información autorizada.

La protección de datos y aplicaciones se realiza mediante soluciones tecnológicas que aseguran la información que es procesada y almacenada. Para la información que es almacenada se utilizan mecanismos de cifrado para garantizar su confidencialidad y para asegurar la integridad se los datos se emplean algoritmos de *hash*, los cuales obtienen un resumen o huella de los datos y se revisan periódicamente para verificar si los datos han sufrido alguna modificación. Para asegurar las aplicaciones se emplean herramientas para verificar el código y revisar que no exista ninguna vulnerabilidad, también se utilizan técnicas de validación de datos de entrada.

Para la detección de *malware*, *spam* o intrusos se utilizan medidas de seguridad basadas en *software* o *hardware* que detectan y eliminan código malicioso (*malware*), correo no deseado (*spam*) y flujo de datos de ataque (intrusos). Estas herramientas utilizan diversas técnicas para la detección como firmas, patrones de datos o comportamiento inusual.

Las medidas de seguridad, además de clasificarse como administrativas, operacionales o tecnológicas, también se pueden catalogar como preventivas, de detección y de recuperación.

Las medidas de seguridad preventivas tienen como objetivo evitar que la información sea atacada por alguna amenaza. Las de detección permiten conocer cuando se está realizando un ataque y tienen el objetivo de mitigar al mínimo el impacto del ataque. Las medidas de seguridad de recuperación permiten que, en caso de un incidente sobre la información, la operación de la organización continúe. Las medidas de seguridad de recuperación también se utilizan para llevar a cabo un análisis forense y conocer las causas raíces del ataque.

Existen varios estándares internacionales para la selección e implementación de medidas de seguridad, entre las principales tenemos al ISO/IEC 27002,[1392] NIST 800-53[1393] o el CIS CSC.[1394]

Sin embargo, el estándar más utilizado es el ISO/IEC 27002, el cual está diseñado para que las organizaciones lo utilicen como referencia en la selección de controles en la implementación de un sistema de gestión de seguridad de la información.

Para lograr una mejor organización, el estándar organiza los controles con funcionalidades relacionadas en las siguientes familias:

a) políticas de seguridad de la información;
b) estructura organizacional de la seguridad de la información;
c) seguridad en recursos humanos;
d) gestión de activos;
e) control de acceso;
f) criptografía;
g) seguridad física y del medio ambiente;
h) seguridad en la operación;
i) seguridad en las comunicaciones;
j) adquisición, desarrollo y mantenimiento de sistemas de información;
k) relación con proveedores;
l) gestión de incidentes;
m) gestión de la continuidad del negocio, y
n) cumplimiento.

En materia de seguridad de datos personales, la LFPDPPP[1395] establece, en su artículo 19, que todo responsable y encargado de tratamiento de datos personales debe implementar medidas de seguridad no menores a las utilizadas para la protección de su información general. De igual forma, el RLFPDPPP[1396] hace referencia detallada a las medidas de seguridad en sus artículos: 4, 50, 52, 57,59, 60, 61,62, 66 y 84. Específicamente se establecen obligaciones sobre la implementación de medidas de seguridad para el responsable y encargado del manejo de datos personales y se hacen recomendaciones para su correcta implementación y mantenimiento.

1392 ISO/IEC 27002. (2013). *Information technology —Security techniques— Code of practice for information security controls.* ISO/IEC. Segunda edición.

1393 NIST. (2013, abril). *Security and Privacy Controls for Federal Information Systems and Organizations*. Publicación especial. 800-53.

1394 Center for Internet Security. (2015, agosto). *The CIS Critical Security Controls for Effective Cyber Defense.*

1395 DOF. (2010, julio). Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010

1396 DOF. (2011, diciembre). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* Artículo 61. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

Medidas de seguridad administrativas

Uciel Fragoso Rodríguez

Las medidas de seguridad corresponden al conjunto de acciones que tienen como objetivo preservar la confidencialidad, integridad y disponibilidad de la información. En este sentido las medidas de seguridad pueden clasificarse en técnicas, físicas y administrativas.

Las medidas de seguridad técnicas se apoyan en infraestructura tecnológica (*hardware y software*), mientras que las medidas físicas incluyen todas las acciones que tienen que ver con el entorno físico de la información y de los elementos físicos asociados a la misma.

Por otro lado, las medidas de seguridad administrativas corresponden a todas las acciones encaminadas a la protección de la información y que están relacionadas con la gente y los procesos. Las medidas de seguridad administrativas se categorizan de la siguiente manera:

a) políticas de seguridad;
b) administración de activos;
c) asignación de roles y privilegios;
d) realización de auditorías;
e) contratos y acuerdos legales y
f) concientización y capacitación.

Las políticas de seguridad establecen lineamientos normativos para indicar que acciones pueden o no realizar las personas en términos de seguridad de la información. Las políticas de seguridad se consideran medidas de seguridad de tipo preventivo ya que tratan de evitar que se realicen acciones que vayan en contra de la seguridad de la información.

Las políticas de seguridad deben seguir los principios y valores de la organización y estar alineadas a su misión y visión. De igual forma, las políticas deben formar parte integral de un marco normativo de la organización.

El marco normativo está conformado por al menos los siguientes componentes:

1) Gobierno normativo. Estructura organizacional que define los roles y responsabilidades para la creación y aprobación de políticas.
2) Proceso de gestión. Pasos a seguir para gestionar el ciclo de vida de las políticas.
3) Colección documental. Conjunto de políticas y documentos relacionados a la normatividad de seguridad de la información.

La administración de activos se considera una medida de seguridad administrativa y consiste en registrar todos los activos tanto físicos como informáticos que intervienen en el tratamiento de la información. En este sentido, se debe realizar un inventario de todo elemento que participe en el ciclo de vida de la información desde su creación, procesamiento, almacenamiento o eliminación. En el caso de activos informáticos deben registrarse todo equipo de cómputo, dispositivos de comunicaciones, elementos de almacenamiento, base de datos, sistemas operativos y aplicativos. La administración de activos gestiona el alta, baja, uso y modificación de activos, además los asocia a los procesos de negocio y al flujo de la información.

La asignación de roles y privilegios en una de las medidas de seguridad administrativa del tipo preventivo de mayor impacto en el proceso de control de acceso. Una buena definición de roles garantiza que las personas que tratan información solo realicen aquellas actividades asociadas a su función y que no comprometan la seguridad de la información.

La correcta definición de roles evita que se presente un posible conflicto de intereses en las actividades cotidianas de las personas.

Por otro lado, la asignación de privilegios asegura que las personas que tengan acceso a la información solo puedan realizar operaciones que estén explícitamente autorizadas. La correcta asignación de privilegios garantiza que la información no sea modificada o dañada por error o por mala intención. La asignación de privilegios debe basarse en el principio del mínimo privilegio, el cual establece que se deben asignar a las personas los privilegios mínimos para que pueda desarrollar adecuadamente sus actividades relacionadas con el tratamiento de la información.

La realización de auditorías (internas o externas) se considera una medida de seguridad administrativas catalogadas como de detección ya que permiten identificar eventos o incidentes anómalos relacionados con el tratamiento de la información. Las auditorías permiten verificar los procesos, la asignación de roles y privilegios, las bitácoras de acceso, el registro de incidentes, configuraciones de *hardware* y *software* y en general cualquier evidencia que muestre el cumplimiento de lo establecido como operación normal o planeada.

Las auditorías deben llevarse a cabo en forma periódica tanto de manera interna como externa. Las inconformidades encontradas como resultado de cada auditoría deben ser atendidas siguiendo un proceso formal, de tal forma que para la siguiente sean eliminadas y el hallazgo de las nuevas se planee su atención. Una buena métrica de desempeño debe indicar una disminución del número de inconformidades al final de cada auditoría.

Los contratos y acuerdos legales son medidas de seguridad administrativas del tipo preventivo ya que establecen las obligaciones en términos de seguridad que deben cumplir las personas que tratan información. En el caso de la protección de datos personales, los contratos y acuerdos legales garantizan que las personas o entidades reconocidas como encargados del tratamiento de los datos personales tengan la obligación de cumplir lo establecido por la legislación vigente.

Finalmente, los programas de concientización y capacitación se consideran medidas de seguridad administrativas del tipo preventivo. La concientización y capacitación en términos de protección de la información permiten a las personas identificar el tipo de información que manejan y el nivel de sensibilidad de la misma, además de conocer las mejores prácticas de tratamiento de la información desde el punto de vista de seguridad. Esta medida de seguridad protege a las personas contra una de las formas más comunes y eficientes de ataque que es la ingeniería social. Los programas de concientización y capacitación deben diseñarse e implementarse de acuerdo con los roles de las personas y deben aplicarse a todos los miembros de la organización y personal externo relacionado en el tratamiento de la información.

Existen estándares de seguridad internacionales que permiten la correcta selección e implementación de medidas de seguridad administrativas como por ejemplo los estándares ISO/IEC 27002[1397] y NIST 800-53.[1398]

En el caso del estándar de seguridad ISO/IEC 27002 contiene la descripción de 114 medidas de seguridad agrupadas en 35 categorías y 13 dominios. Ocho de los 13 dominios están enfocados a medidas de seguridad administrativas las cuales son:

1) Políticas de seguridad de la información. Permiten establecer directrices para la seguridad de la información en concordancia con los requerimientos del negocio, regulaciones y leyes relevantes.

1397 ISO/IEC 27002. (2013). "Information technology —Security techniques— Code of practice for information security controls". ISO/IEC. Segunda edición.

1398 NIST. (2013, abril). *Security and Privacy Controls for Federal Information Systems and Organizations*. Publicación especial. 800-53.

2) Estructura organizacional de seguridad de la información. El objetivo es establecer un marco de trabajo para gestionar la implementación y operación de la seguridad de la información en una organización.
3) Seguridad en recursos humanos. Medidas de seguridad para asegurar que los empleados y empleadores entiendan sus responsabilidades en función del rol asignado.
4) Administración de activos. Tiene como objetivo identificar los activos de la organización y definir las protecciones apropiadas.
5) Relación con proveedores. Medida enfocada a proteger los activos de la organización que son accedidos por los proveedores.
6) Plan de gestión de incidentes. Tiene como objetivo garantizar un enfoque efectivo y consistente para la administración de incidentes de seguridad de la información.
7) Plan de continuidad de negocio. Medida que permite soportar la continuidad de negocio en situaciones adversas como, por ejemplo, durante una crisis o un desastre.
8) Cumplimiento. Medidas que evitan la falta de cumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas con requerimientos de seguridad de la información.

Por otro lado, el estándar NIST 800-53 provee 265 medidas de seguridad agrupadas en 18 familias de las cuales seis corresponden a medidas de seguridad administrativas, las cuales son:

1) Capacitación y concientización. Conjunto de medidas de seguridad para establecer las políticas y procedimientos de entrenamiento basado en roles.
2) Auditorías. El objetivo de estas medidas es establecer el procedimiento para la gestión de bitácoras y definir las fases de revisión, análisis y reporte de auditorías.
3) Administración de la configuración. Medidas de seguridad que permiten definir guías seguras de configuración, gestionar cambios, realizar inventario de componentes, establecer planes de administración de configuraciones y restringir uso de *software*.
4) Planes de contingencia. Tienen como objetivo definir infraestructura y procesamiento alterno en caso de que se presente una contingencia.
5) Planes de respuesta a incidentes. Medida de seguridad que permite establecer un plan para manejar, monitorear, reportar y responder a incidentes de seguridad.
6) Seguridad en el personal. Las medidas para la seguridad del personal tienen como objetivo establecer políticas y procedimientos para la contratación, asignación de roles y responsabilidades, cambios y terminación de relación laboral. También tiene que ver con la seguridad personal de terceros y con el establecimiento de sanciones.

Con respecto a las medidas de seguridad administrativas para la protección de datos personales, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[1399] define, en su artículo 2, las medidas de seguridad administrativas como:

> V. Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.

1399 DOF. (2011, diciembre). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* Artículo 61. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

Para el sector público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[1400] define de manera similar en su artículo 3, sección XXI, las medidas de seguridad administrativas de la siguiente forma:

> Artículo 3. Para los efectos de la presente Ley se entenderá por:
>
> XXI. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales.

Medidas de seguridad físicas

Uciel Fragoso Rodríguez

La seguridad de la información se define como el conjunto de normas, controles y procesos que tienen como objetivo garantizar la confidencialidad, integridad y disponibilidad de la información sin importar el formato en que esté representada.

Las medidas de seguridad físicas refieren a todos los controles que tienen como objetivo asegurar el acceso físico a la información y a todo su entorno.

La información puede estar expresada en diferentes formatos: escrita, gráfica, en audio, en símbolos o electrónica entre otros. Sin embargo, sin importar el formato en que la información esté representada, esta puede ser:

a) robada, espiada o expuesta afectando la confidencialidad;
b) modificada, dañada o eliminada afectando la integridad y
c) secuestrada o denegada afectando la disponibilidad.

1. Ataque a la confidencialidad

La información es robada cuando no se dispone de un control de acceso adecuado a las áreas donde se tiene almacenada la información sensible. Cuando la información está en forma escrita, los archiveros que contienen la documentación es posible que no dispongan de chapa de seguridad y que no existan mecanismos de control de acceso al área. En este sentido es relativamente fácil para un intruso entrar al área y extraer la información sensible. Lo mismo ocurre en los centros de datos con la información almacenada en forma electrónica, si no se tiene controlado el acceso, cualquier persona puede acceder al centro de datos y robar medios de almacenamiento como discos duros, cintas magnéticas, memorias, entre otros. Otra forma de robar la información es teniendo acceso a los equipos donde se encuentra almacenada y mediante un dispositivo móvil copiar la información.

En caso de que la información sea transportada en papel o en medios de almacenamiento electrónico por personas a pie o vehículos terrestres, marítimos o aéreos, existe el riesgo de que la información sea robada.

Hay diversas medidas de seguridad físicas para tener un control de acceso seguro a las áreas con información crítica, por ejemplo:

a) oficiales de vigilancia;
b) registros o bitácoras de entrada;

1400 DOF. (2017, enero). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", en *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

c) gafetes;
d) torniquetes, puertas electromagnéticas y arcos;
e) credenciales de proximidad;
f) teclados para introducción de claves;
g) dispositivos biométricos (lector de huella, reconocimiento facial, reconocimiento de voz, entre otros) y
h) sistema de videovigilancia.

En caso de que el intruso haya accedido físicamente a las áreas con información crítica se deberá de disponer de chapas mecánicas o electrónicas de seguridad para los archiveros con documentación en papel y bloqueo de puertos de comunicación en caso de equipo de cómputo con información almacenada en forma electrónica.

Para el caso de personas que manejen información sensible en sus equipos de cómputo personal y en su área de trabajo, es importante concientizarlos y establecer políticas de seguridad para que resguarden la documentación de manera segura y sus equipos móviles los aseguren mediante candados o con cualquier otro dispositivo.

Para el transporte físico de información, es recomendable emplear medidas de seguridad físicas como tecnologías de geolocalización para el rastreo de la información y procedimientos de verificación de entrega y recepción de información.

La información puede ser espiada cuando se transmite en forma electrónica en medios de comunicación no protegidos. Los atacantes instalan dispositivos que analizan el flujo de la información, estos dispositivos se conocen como analizadores de tráfico o *sniffers*. Otra forma de espiar la información es mediante una técnica de ingeniería social llamada "mirar por encima del hombro" o *shoulder surfing* y consiste en que el atacante ve la información sensible en el momento que la persona autorizada está accediendo a ella.

Algunas medidas de seguridad física contra el espionaje de la información son:

a) bloquear conexiones físicas a canales de comunicación privados;
b) cubrir físicamente la información con algún cuerpo opaco o con micas protectoras las pantallas de los equipos de cómputo y
c) bloquear las sesiones de los sistemas de cómputo cuando no se estén utilizando.

Cuando la información es expuesta a personas no autorizadas, generalmente se debe a un error o descuido de las personas responsables del tratamiento de la información. Es común dejar información sensible impresa sobre las mesas de trabajo o tirar documentos y medios magnéticos a la basura. Otra manera de exponer información sensible es a través de la comunicación verbal cuando se está charlando en persona o por teléfono.

Algunas medidas de seguridad física para evitar exponer información son entre otras:

a) implementar programas de concientización y capacitación para que las personas tengan conocimiento sobre la información sensible que procesan;
b) crear, difundir y forzar políticas de escritorio limpio;
c) implementar procedimientos para la trituración de documentos y la destrucción de medios magnéticos y
d) crear políticas para no difundir información sensible en forma oral.

2. Ataque a la integridad

La información puede ser atacada en su integridad cuando es modificada, dañada o eliminada por personas no autorizadas.

La información sensible es modificada sin autorización cuando no existe un control de acceso físico a dicha información. Las personas pueden cambiar el contenido de un documento o suplantar los documentos por otros que sean falsos. En caso de que la información esté en formato electrónico, la modificación se lleva a cabo cuando el atacante tiene acceso físico a la infraestructura tecnológica utilizada para llevar a cabo la actualización de la información, por ejemplo, desatender sesiones en sistemas de cómputo.

Algunos controles de seguridad física para evitar la modificación no autorizada de la información son:

a) implementar procedimientos de control de acceso seguro a las áreas donde se encuentra información sensible;
b) bloquear las sesiones de cómputo que no se estén utilizando;
c) emplear material que no sean fácilmente alterables en documentos u otros medios e
d) implementar algún mecanismo de registro del contenido de la información que permita verificar cuando esta haya sido alterada.

La información puede ser dañada en forma accidental o de manera intencional. Cuando se encuentra contenida en algún medio físico, es posible que un manejo manual inadecuado afecte el contenido de la información, lo mismo ocurre cuando está expuesta a elementos químicos, fenómenos naturales o a posibles incidentes físicos. En caso de que la información se encuentre en formato electrónico, el riesgo de que sea dañada se debe principalmente a fallas en la infraestructura tecnológica y en los mecanismos de control del medio ambiente como pudiera ser la energía eléctrica, temperatura o humedad. Cuando la información se encuentra almacenada en medios magnéticos, la interferencia electromagnética puede ocasionar daños.

Algunos mecanismos de seguridad física para evitar el daño a la información son:

a) establecer procedimientos de manejo adecuado de los materiales y medios en donde se encuentra la información sensible;
b) resguardar la información de agentes químicos, fenómenos naturales o incidentes de carácter físico;
c) crear programas de mantenimiento para la infraestructura tecnológica;
d) implementar mecanismos de control del medio ambiente y
e) aislar los dispositivos de almacenamiento de fuentes de interferencia electromagnética.

Cuando se requiere eliminar la información dentro de su ciclo de vida, un mecanismo de seguridad física que protege contra un uso inadecuado de la misma es establecer procedimientos de destrucción segura de documentos y medios electrónicos.

En materia de medidas de seguridad física para la protección de datos personales, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[1401] establece las siguientes acciones:

1401 DOF. (2011, diciembre). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Diario Oficial de la Federación.* Artículo 61. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5226005&fecha=21/12/2011

a) prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;

b) proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;

c) proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad y

d) garantizar la eliminación de datos de forma segura.

En tanto que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO),[1402] en su artículo 3, fracción XXII, define medidas de seguridad físicas como:

> XXII. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:
>
> a) prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;
>
> b) prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;
>
> c) proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización y
>
> d) proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad.

Ambas regulaciones se enfocan a medidas de seguridad físicas que garanticen un adecuado control de acceso, evitar daños a las instalaciones físicas donde está localizada información sensible, cuidar los dispositivos móviles, establecer programas de mantenimiento de la infraestructura tecnológica y garantizar una eliminación segura de datos de los medios de almacenamiento.

Medidas de seguridad técnicas

Uciel Fragoso Rodríguez

Las medidas de seguridad comprenden el conjunto de elementos y acciones cuyo objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información. Las medidas de seguridad se aplican a lo largo del ciclo de vida de la información y deben estar inmersas en cada una de las actividades que conforman los procesos de negocio, y pueden ser del tipo administrativas o técnicas.

Las medidas de seguridad administrativas están enfocadas básicamente a la gente y a los procesos. Algunos ejemplos son la creación de políticas, la definición de roles, la asignación de permisos, la especificación de tareas, la difusión de una cultura de la seguridad y la implementación de programas de capacitación.

Por otro lado, las medidas de seguridad técnicas refieren a todas las acciones apoyadas de infraestructura tecnológica (*hardware* y *software*) que intervienen en la creación, procesamiento, transmisión o almacenamiento de la información.

1402 DOF. (2017, enero). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

Las medidas de seguridad técnicas pueden aplicarse en cualquier parte de la infraestructura tecnológica y se clasifican en las siguientes categorías:

a) control de acceso
b) operación de la infraestructura y comunicaciones
c) sistemas de información

1. Control de acceso

El control de acceso es el mecanismo a través del cual se garantiza que solo las personas autorizadas podrán acceder la información correspondiente y podrán realizar el tratamiento que les está permitido. Para lograr el objetivo, el control de acceso se compone de dos funciones: autenticación y autorización.

La autenticación es el proceso por medio del cual se verifica la identidad de la persona o en general de cualquier entidad que requiera acceder a la información. Para verificar la identidad se solicita la presentación de credenciales las cuales pueden ser de tres tipos o factores:

a) factor 1: algo que sé;
b) factor 2: algo que tengo, y
c) factor 3: algo que soy.

Las credenciales del tipo Factor 1 son elementos que la persona sabe o reconoce, como: palabras clave o contraseñas, NIP (números de identificación personal), preguntas secretas, imágenes, entre otros. Este tipo de credenciales tiene un costo bajo y son relativamente sencillas de implementar, sin embargo, tienen algunas desventajas como que pueden ser adivinadas, robadas o prestadas.

Las credenciales del tipo Factor 2 son elementos que el usuario posee y que le permiten validar su identidad como: *tokens*, tarjetas inteligentes, certificados digitales, *cookies*, entre otros. Proveen un mayor nivel de seguridad que las del tipo Factor 1, aunque siguen teniendo el problema de que pueden ser extraviadas, robadas o prestadas.

Las credenciales del tipo Factor 3 son elementos asociados a características biológicas de los usuarios, tales como huella digital, reconocimiento facial, reconocimiento de voz, patrón de iris, patrón de venas, geometría de la mano, entre otros. Son credenciales altamente confiables que se emplean cuando se requiere un nivel robusto de autenticación. Sin embargo, tienen la desventaja de que requieren la presencia física de la persona, son mecanismos de alto costo y difíciles de gestionar, además, bajo cierto contexto puede representar un riesgo a la privacidad de las personas.

Una vez que se ha realizado el proceso de autenticación, el siguiente paso para el control de acceso es la función de autorización. La autorización es el mecanismo a través del cual se define a qué información tiene acceso el usuario y que tipo de procesamiento o tratamiento tiene permitido. La autorización usualmente se implementa mediante el uso de medidas de seguridad administrativas y técnicas. Las medias de seguridad administrativas consisten en una correcta definición de roles y una adecuada asignación de permisos o privilegios, mientras que las medidas de seguridad técnicas implican en uso de componentes de *hardware* o *software* para forzar el cumplimiento de políticas de acceso a la información.

2. Operación de la infraestructura y comunicaciones

Las medidas de seguridad técnicas empleadas en la infraestructura tecnológica se pueden clasificar dependiendo en cuál de los elementos siguientes se aplica:

a) red de datos y telecomunicaciones

b) equipo de cómputo

c) servidores y bases de datos

Las medidas de seguridad técnicas para las redes de datos y telecomunicaciones protegen la información que se encuentra en circulación. Una forma de garantizar la confidencialidad de la información en tránsito es mediante el uso de mecanismos de cifrado en los canales de comunicación. Otra medida de seguridad técnica consiste en el filtrado del flujo de la información, es decir, permitir solo la transmisión de información autorizada. La función de filtrado también permite detectar y bloquear tráfico malicioso utilizado en los ataques de denegación de servicio.

Los mecanismos de seguridad técnicos empleados en los equipos de cómputo tienen como objetivo salvaguardar la información que es accedida, procesada o almacenada por el usuario. Una medida de seguridad ampliamente utilizada es el software antivirus que evita que un código malicioso destruya, robe o secuestre la información contenida en el equipo de cómputo personal. Para evitar la fuga de información se emplea una aplicación denominada *DLP (Data Loss Prevention)* que evita que información sensible sea extraída a través de diversos dispositivos periféricos. De igual forma, mecanismos de cifrado son utilizados para garantizar la privacidad de la información almacenada en dispositivos locales.

La tercera categoría de infraestructura tecnológica en donde se implementan medidas de seguridad técnicas son los servidores y bases de datos. Los primeros son equipos con alto poder de cómputo que procesan la información, mientras que las bases de datos son sistemas de almacenamiento donde se guarda la información. Algunas de las medidas de seguridad técnicas utilizadas en servidores y bases de datos son: programas de actualización y mantenimiento, mecanismos de cifrado, arreglos de alta disponibilidad, verificación de integridad de datos, respaldos de información, configuración segura de parámetros, correlacionador de eventos.

3. Sistemas de información

Los sistemas de información son las aplicaciones que permiten a los usuarios acceder y procesar la información. Sin embargo, a través de aplicaciones, los atacantes pueden acceder, modificar, dañar o bloquear información sensible. Existen diversas medidas de seguridad técnicas que pueden emplearse en los sistemas de información, por ejemplo:

a) Verificación de datos de entrada. Consiste en un mecanismo que revisa los datos de entrada a los aplicativos, detectando y filtrando aquellos patrones que pudieran representar algún riesgo como inyección de comandos o de código.

b) Metodologías de desarrollo seguro de código. Son mejores prácticas que permiten a los desarrolladores crear aplicaciones seguras.

c) Herramientas de análisis de vulnerabilidades. Permiten encontrar fallas en la funcionalidad de la aplicación.

d) Validación de integridad transaccional. Realiza verificaciones de que el procesamiento de la información sea íntegro y que no haga uso inapropiado de la misma.

Existen estándares de seguridad internacionales que permiten la adecuada selección e implementación de medidas de seguridad técnicas como por ejemplo los estándares ISO/IEC 27002[1403] y NIST 800-53.[1404]

En el caso del estándar de seguridad ISO/IEC 27002 contiene la descripción de 114 medidas de seguridad agrupadas en 35 categorías y 13 dominios, cinco de los 13 dominios están enfocados a medidas de seguridad técnicas las cuales son:

1) Control de acceso. El objetivo de esta familia de medidas de seguridad es limitar el acceso a la información y a los componentes que la procesan.
2) Criptografía. Medidas de seguridad que tienen como finalidad garantizar el correcto uso de técnicas criptográficas para proteger la confidencialidad, autenticidad e integridad de la información.
3) Seguridad operativa. Conforman un conjunto de medidas de seguridad técnicas cuyo objetivo es garantizar la operación correcta y segura de todos los componentes de procesamiento de la información.
4) Seguridad en las comunicaciones. Estas medidas de seguridad tienen como objetivo asegurar la protección de la información que es transmitida a través de la red de comunicaciones.
5) Adquisición, desarrollo y mantenimiento de sistemas. Medidas de seguridad técnicas que garantizan la seguridad de la información a lo largo del ciclo de vida de los sistemas informáticos.

El estándar NIST 800-53 provee 265 medidas de seguridad agrupadas en 18 familias de las cuales cinco corresponden a medidas de seguridad técnicas y son:

1) control de acceso
2) identificación y autenticación
3) protección de media
4) protección de sistemas y comunicaciones
5) integridad en sistemas e información

Respecto a las medidas de seguridad técnicas para la protección de datos personales, el Reglamento de la Ley de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[1405] define, en su artículo 2, las medidas de seguridad técnicas:

> VII. Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:
>
> a) el acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;
>
> b) el acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
>
> c) se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y
>
> d) se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

1403 ISO/IEC 27002. (2013). "Information technology —Security techniques— Code of practice for information security controls". ISO/IEC. Segunda edición.

1404 NIST. (2013, abril). *Security and Privacy Controls for Federal Information Systems and Organizations*. Publicación especial. 800-53.

1405 *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, *Diario Oficial de la Federación,* enero 2017, disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

Para el sector público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[1406] en su artículo 3, sección XXIII, define de manera similar las medidas de seguridad técnicas:

> XXIII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con *hardware* y *software* para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa, más no limitativa, se deben considerar las siguientes actividades:
>
> a) prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;
>
> b) generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;
>
> c) revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del *software* y *hardware*, y
>
> d) gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Medios de impugnación en el amparo

Jean Claude Tron Petit

Los medios de impugnación tienen como propósito luchar contra una decisión judicial cuestionando su validez o legalidad, a efecto que se anule, revoque, modifique o se ordene subsanar la omisión mediante instancias o procedimientos previstos en ley a través de los cuales las partes y los demás sujetos legitimados controvierten los actos procesales y las omisiones de un órgano jurisdiccional.

Para Alcalá-Zamora "los medios de impugnación son actos procesales de las partes, dirigidos a obtener un nuevo examen, total o limitado a determinados extremos y un nuevo proveimiento acerca de una resolución judicial que el impugnador no estima apegada a derecho, en el fondo o en la forma, o que reputa errónea en cuanto a la fijación de los hechos".

La finalidad o propósito de los medios de impugnación es obtener un nuevo examen, que puede ser total o parcial —limitado a algunos extremos — y una nueva decisión acerca una resolución judicial.

El juicio de amparo acoge los principios del derecho procesal y dispone que las resoluciones judiciales de primera instancia pueden ser objeto de estudio por un tribunal de mayor jerarquía mediante la interposición del recurso correspondiente.

Sin embargo, la Ley de Amparo amplía el espectro o alcance de los instrumentos de inconformidad y comprende a) las inconformidades de las partes contra los actos o decisiones del tribunal, a efecto de refutar la validez o legalidad de los mismos y b) las objeciones que se formulan contra actos de las propias partes (*v. gr.* objeción de documentos u obtención de ellos cuando alguna de las partes o un tercero obligado no los exhiba en juicio).

El problema de los medios de impugnación es una pugna entre las exigencias de: a) sentencias estrictamente justas, que requieren una serie ilimitada de recursos; frente a b) firmeza en la justicia que exige se declare de una vez por todas qué fallo debe prevalecer o regir.

1406 DOF. (2017, enero). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", en *Diario Oficial de la Federación.* Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

Sin embargo, la tendencia actual es aumentar los poderes del juez y disminuir el número de recursos, es el triunfo de una justicia pronta y firme sobre una justicia buena pero lenta.

En conclusión, existen medios de impugnación en cada especialidad del derecho, aunque los clásicos y de más raigambre son los previstos en las materias civil y penal, aun cuando en la materia administrativa existe todo un sistema de medios y el juicio de amparo tiene su propia regulación.

1. Clasificación de los medios de impugnación en el amparo

Existe una serie de categorías acorde a las variadas especies de medios que permiten clasificar a los medios de impugnación. Las más destacadas son:

a) Incidentes impugnativos. Mediante los cuales se enmienda la validez de actuaciones y no de resoluciones judiciales, tales como los incidentes de nulidad de notificaciones, falsedad de firma, violación a la suspensión del acto reclamado, reposición de autos y de no ejecución.

b) Recursos. Se revisa la validez o legalidad de resoluciones judiciales, tales como el de apelación en instancias locales, recurso de revisión principal e incidental, de queja, reclamación e inconformidad en juicio de amparo.

c) Procesos impugnativos. Apelación extraordinaria, juicio ordinario de anulación de cosa juzgada fraudulenta, reconocimiento de inocencia o indulto, juicio de amparo directo.

En razón de quién decidirá la impugnación, debe distinguirse la identidad o diversidad entre el órgano que dictó la resolución impugnada y el que revisa. Existen estos supuestos:

a) Verticales. Resuelve un juzgador distinto, así tenemos al *ad quem* y *a quo* —apelación, revisión, queja.

b) Horizontales. Resuelve el mismo juzgador —revocación, regularizar el procedimiento, aclaración de sentencia.

Otra importante distinción radica en los poderes atribuidos a quien toma las decisiones y los efectos que generan, siendo estos:

a) Anulación. El acto impugnado pierde eficacia y validez, y los nuevos actos son llevados a cabo por el juez original, v. gr. juicio contencioso administrativo y revisión fiscal complementaria al juicio de amparo directo.

b) Sustitución. El *ad quem* se coloca en la situación del *a quo* en sustitución y le revisa (revoca, modifica o confirma).

c) Control. Decide aplicar o no un acto. No lo invalida ni revisa (revoca, modifica o confirma), v. gr. juicio de amparo en ciertos casos, especialmente cuando lo reclamado son facultades discrecionales.

d) En el amparo, los medios de impugnación son, generalmente, de plena jurisdicción y por excepción con reenvío, lo que se actualiza solo cuando debe reponerse el procedimiento o no existen condiciones suficientes para decidir.

En lo concerniente a los sujetos que participan, los roles se ejercen por:

a) La parte o tercero legitimado. Son quienes pueden interponer el medio de impugnación, impugnador, recurrente, apelante, etc. Los juzgadores no pueden revocar sus determinaciones, a excepción de ciertos medios de control que permiten al juzgador, o a su superior, la revisión de oficio.

b) El órgano jurisdiccional responsable del acto o de la omisión impugnada, juez *a quo*.

c) El órgano jurisdiccional competente para conocer y resolver, juzgador *ad quem*.

d) La contraparte del impugnador, a quien normalmente se le permite intervenir en defensa de la validez o legalidad del acto reclamado.

Finalmente, una importante consideración tiene que ver con los momentos, etapas y actuaciones que surgen durante el trámite, lo cual Ovalle Favela describe atinadamente así:

> A su vez, el procedimiento impugnativo se desenvuelve a través de un conjunto de actos procesales, de los cuales los principales son los siguientes:
>
> a) la interposición, acto con el cual se inicia el procedimiento;
>
> b) la motivación, que es la exposición de las razones con base en las cuales el impugnador estima que el acto o la omisión combatidos no se apegan a derecho;
>
> c) la admisión y efectos del medio de impugnación;
>
> d) la sustanciación, y
>
> e) la resolución sobre el acto o la omisión impugnados.
>
> Los razonamientos que exprese el impugnador pueden tratar de demostrar que el acto impugnado:
>
> a) infringió las normas procesales que regulan las condiciones de tiempo, forma o lugar de aquel (errores in procedendo, de actividad o de procedimiento);
>
> b) violó las normas sustantivas, por aplicar una ley que no era aplicable, por interpretar indebidamente la ley aplicable o por no aplicar la ley aplicable (errores in iudicando, de juicio o de fondo), o
>
> c) se basó en un juicio erróneo sobre los hechos, por haber valorado indebidamente las pruebas o por no haberlas valorado.[1407]

2. Significado del concepto "recurso"

Los recursos suelen ser considerados como una especie destacada de los medios de impugnación, que vienen a ser el género.

Ovalle comenta que generalmente se identifican los conceptos de medios de impugnación con el de recursos, como si fueran sinónimos. Esto ocurre por la importancia que los recursos tienen dentro del conjunto.

El concepto "recurso" alude a reiterar el curso del conflicto, es como volver sobre lo andado, pero en plan revisor.

Serrano Robles comenta que en la instancia concurren las partes que contendieron ante el inferior a pedir que se vuelva a analizar la cuestión controvertida para que decida si la apreciación efectuada se ajustó o no a la ley correspondiente y, en su caso, a solicitarle que reforme la determinación.

Ovalle expresa que los recursos se plantean y resuelven dentro del mismo proceso, combatiendo resoluciones dictadas en el curso de éste o la sentencia definitiva, abriendo una segunda instancia dentro del mismo proceso.

Para Couture el concepto de recurso significa regresar al punto de partida, es recorrer de nuevo el camino ya hecho.[1408]

1407 Ovalle, Favela, (2017) "Medios de impugnación en el Amparo" en *Revista jurídica del Instituto de Investigación jurídicas de la UNAM*. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/9/4317/29.pdf

1408 Couture, Eduardo J. (1993). *Los fundamentos del Derecho Procesal Civil*. Porrúa, México.

Los recursos pueden ser considerados como un medio técnico de impugnación y subsanación de los errores que, eventualmente, puede adolecer una resolución judicial, dirigidos a provocar la revisión de la misma, ya sea por el juez que la dictó o por otro de superior jerarquía.

Por su parte, Guasp[1409] define el recurso como a una pretensión de reforma de una resolución judicial dentro del mismo proceso en que ha sido dictada.

En México se suscitó un interesante debate académico entre los profesores Héctor Fix Zamudio e Ignacio Burgoa Orihuela, tocante a la naturaleza del juicio de amparo, especialmente por lo que concierne al directo. ¿El juicio de amparo es, auténticamente un recurso o bien, un juicio? Cabría agregar si también pueda ser considerado un proceso impugnativo como la apelación extraordinaria, entendido como un proceso de nulidad de sentencias definitivas.

El objeto del recurso de revisión en el juicio de amparo es combatir las decisiones más importantes dictadas durante la secuela del juicio, ya sea en el cuaderno principal o incidental, y puede ser en vía directa o adhesiva.

En esencia, el recurso de revisión es un medio de control de la primera instancia, pero no supone la renovación del debate ni de las pruebas, es un control de la sentencia en lo concerniente a las cuestiones de hecho y de derecho.

Por tanto, incluye y abarca todas las violaciones cometidas i) *in procedendo* o ii) *in iudicando* —tanto de carácter formal como de fondo.

Los sujetos legitimados para interponer la revisión en el amparo son:

a) Partes. No basta serlo, sino que su legitimación deriva de no haber visto satisfechas las pretensiones deducidas y el perjuicio causado. Si la sentencia las acoge solo en parte, es apelable en cuanto desecha. El agravio es la medida de la legitimación.
b) Terceros. Si bien jurídicamente no son afectados, prácticamente pueden serlo cuando la sentencia proyecta sus efectos hacia terceros a condición de que tengan un interés legítimo en el litigio ajeno y ello les cause un agravio.

Como consecuencia de la interposición de los recursos, se da un efecto devolutivo, lo que sucede cuando la jurisdicción se desplaza y la sumisión al superior hace desaparecer los poderes del juez *a quo* por lo que el *ad quem* asume la facultad de:

a) declarar improcedente el recurso y la de
b) revocación o modificación.

El juez superior no puede empeorar la situación del apelante en los casos en que no ha mediado recurso del adversario, lo que se conoce como el principio de *non reformatio in peius*.

Un efecto distinto es el suspensivo y consiste en la paralización o enervamiento provisional de los efectos de las sentencias o proveídos, que quedan detenidos para evitar perjuicios irreparables si se cumplieran. Convierte al cumplimiento en una expectativa. En el juicio de amparo esta hipótesis se presenta con el recurso de queja en los casos que prevé el artículo 102 de la Ley de Amparo.

La procedencia de los recursos requiere se satisfagan las siguientes condiciones:

a) previsto en ley;
b) competencia de la autoridad revisora;

1409 Guasp, J. (1961). *Derecho procesal civil*. Instituto de Estudios Políticos, Madrid. 1961. Tomo II, p.1326.

c) idóneo;
d) oportuno en tiempo, lugar y forma y
e) legitimación del recurrente.

Para el caso de que el recurso sea procedente, la pretensión del recurrente será satisfecha dependiendo de que los agravios sean fundados o infundados. Ello implica examinar la legalidad del acto recurrido a la luz de los argumentos expresados (salvo los casos de suplencia) y de su justificación o no justificación, dependerá que el acto sea:

a) revocado;
b) modificado, o
c) confirmado.

Los recursos pueden ser improcedentes por:

a) no ser la vía pertinente para cuestionar determinadas decisiones;
b) incumplir con las condiciones para su promoción;
c) por falta de legitimación, o
d) no incidencia de lo resuelto en los intereses del inconforme y ocasiona que:
    1. sea desechado el recurso;
    2. no logre su objetivo el recurso; o que
    3. quede firme la sentencia o acto recurrido.

En esencia, lo que sucede es que no se estudia el mérito.

3. Los medios de impugnación que contempla la Ley de Amparo

3.1. Aspectos generales

La actual Ley de Amparo,[1410] en su artículo 80, prevé un sistema simplificado que alude a los medios de impugnación, señalando que son los recursos de revisión, queja y reclamación; pero, además, tratándose del cumplimiento de sentencias, el de inconformidad. Adicionalmente se prevén incidentes impugnativos como nulidad de notificaciones, etc.

Cabe puntualizar que la Ley Federal de Procedimiento Contencioso Administrativo, en su artículo 63, prevé el recurso de revisión complementario[1411] al juicio de amparo directo. Este medio se tramita y decide siguiendo las reglas de los recursos, aunque su finalidad es controvertir decisiones del Tribunal Federal de Justicia Administrativa y no de resoluciones dictadas en el juicio de amparo.

Los medios de impugnación se pueden interponer y sustanciar en forma impresa o electrónica conforme a lo que dispone el artículo tercero. Es así que las promociones deberán hacerse por escrito —en forma impresa o electrónica. Pueden ser orales solamente aquellas que se hagan en las audiencias, notificaciones y comparecencias autorizadas por la ley, dejándose constancia de lo esencial, siendo optativo para el promovente presentar su escrito en forma impresa o electrónica.

1410 Publicada en el *Diario Oficial de la Federación* del 2 de abril de 2013.

1411 Las sentencias del Tribunal Federal de Justicia Administrativa pueden ser reclamadas por los particulares mediante el juicio de amparo directo y, en concordancia, se concede a las autoridades este medio de impugnación.

Sobre el particular es ilustrativo lo que dispone la tesis de jurisprudencia P. VII/2015 (10a.):

> MEDIOS DE IMPUGNACIÓN PREVISTOS EN LA LEY DE AMPARO EN VIGOR. PUEDEN INTERPONERSE VÍA ELECTRÓNICA, POSTAL O PERSONALMENTE ANTE LA OFICINA DE CORRESPONDENCIA DEL ÓRGANO DE AMPARO QUE CONOZCA DEL JUICIO, YA QUE NO SON EXCLUYENTES ENTRE SÍ. De los artículos 80 y 23 de la Ley de Amparo se advierte, respectivamente, que los medios de impugnación, así como los escritos y las promociones que se realicen en ellos, podrán presentarse en forma impresa o electrónicamente, y en este último caso las copias o constancias impresas no serán exigidas a los que hagan uso de dicha tecnología, salvo que sea necesario proporcionarlas por esa misma vía; y que si alguna de las partes reside fuera de la jurisdicción del órgano de amparo que conozca o deba conocer del juicio, la demanda y la primera promoción del tercero interesado podrán presentarse, dentro de los plazos legales, en la oficina pública de comunicaciones del lugar de su residencia, en la más cercana en caso de no haberla, o bien, en forma electrónica a través del uso de la firma electrónica. Ahora bien, la interpretación sistemática de ambas disposiciones conduce a concluir que la vía electrónica y las diversas impresa a través de la oficina de comunicaciones, o bien, la que se hace personalmente en la oficina de correspondencia del órgano que conozca del juicio, o del que deba conocer y resolver los recursos respectivos, en los casos en que se exija su presentación ante este último, no son excluyentes entre sí, pues cualquiera de ellas tiende a facilitar el acceso de las partes a los tribunales encargados de impartir justicia y salvaguarda los principios consagrados en el artículo 17 de la Constitución Política de los Estados Unidos Mexicanos.

3.2. Revisión

El objeto del recurso de revisión en amparo permite combatir las decisiones más importantes dictadas durante la secuela del juicio, ya sea en el cuaderno principal o incidental y puede ser propuesto en vía directa o adhesiva.

De acuerdo con la abundante jurisprudencia existente, es el caso que la sentencia se somete a una operación de control, tendiente a examinar la validez formal, pero también la justicia del fallo.

Su reglamentación la contemplan los artículos 81 al 96 de la Ley de Amparo.

3.3. Procedencia

La Ley de Amparo dispone en sus artículos 81 y relativos los supuestos de procedencia del recurso de revisión, acorde a lo siguiente:

En amparo indirecto, en contra de las resoluciones:

a) que concedan o nieguen la suspensión definitiva;
b) las que modifiquen o revoquen el acuerdo en que se conceda o niegue la suspensión definitiva, o las que nieguen la revocación o modificación de esos autos; en su caso, deberán impugnarse los acuerdos pronunciados en la audiencia correspondiente;
c) las que decidan el incidente de reposición de constancias de autos;
d) las que declaren el sobreseimiento fuera de la audiencia constitucional, y
e) las sentencias y acuerdos pronunciados en la propia audiencia constitucional.

En amparo directo, en contra de:

a) las sentencias que resuelvan sobre la constitucionalidad de normas generales que establezcan la interpretación directa de un precepto de la Constitución o de los derechos humanos establecidos en los tratados internacionales de los que el Estado mexicano sea parte;

b) omisiones al decidir sobre tales cuestiones cuando hubieren sido planteadas, siempre que fijen un criterio de importancia y trascendencia, según lo disponga la Suprema Corte de Justicia de la Nación en cumplimiento de acuerdos generales del pleno.

Al respecto es pertinente el criterio jurisprudencial expresado en la tesis: 2a./J. 128/2015 (10a.) que dice:

> REVISIÓN EN AMPARO DIRECTO. REQUISITOS PARA SU PROCEDENCIA. Por regla general, las sentencias dictadas por los tribunales colegiados de circuito en amparo directo son definitivas y solo de manera extraordinaria, pueden impugnarse mediante el recurso de revisión previsto en los artículos 107, fracción IX, de la Constitución Política de los Estados Unidos Mexicanos y 81, fracción II, de la Ley de Amparo, conforme a los cuales, una vez actualizados los presupuestos procesales (competencia, legitimación, oportunidad del recurso —en su caso—, entre otros), procede el mencionado medio de defensa siempre que: 1) en la sentencia de amparo directo combatida se decida sobre la constitucionalidad o inconstitucionalidad de una norma general, o se establezca la interpretación directa de un precepto constitucional o de los derechos humanos reconocidos en los tratados internacionales de los que el Estado mexicano sea parte, o bien, si en dichas sentencias se omite el estudio de las cuestiones referidas, cuando se hubieren planteado en la demanda de amparo; y 2) el problema de constitucionalidad entrañe la fijación de un criterio de importancia y trascendencia. Ahora bien, con el fin de armonizar la normativa de la Suprema Corte de Justicia de la Nación con los preceptos citados, el Pleno emitió el acuerdo general 9/2015 (*), que regula la procedencia del recurso de revisión interpuesto contra sentencias de amparo directo, el cual, en vez de privilegiar el análisis de los agravios en la revisión, permite al Alto Tribunal hacer una valoración discrecional de los méritos de cada recurso, para determinar si a su juicio el asunto reúne los requisitos de importancia y trascendencia, para lo cual, su punto segundo señala que la resolución de un amparo directo en revisión permite fijar un criterio de importancia y trascendencia cuando: (i) pueda dar lugar a un pronunciamiento novedoso o de relevancia para el orden jurídico nacional o (ii) lo decidido en la sentencia recurrida pueda implicar el desconocimiento de un criterio sostenido por la Suprema Corte de Justicia de la Nación relacionado con alguna cuestión propiamente constitucional, por haberse resuelto contra ese criterio o se hubiere omitido aplicarlo.

La parte que obtuvo resolución favorable en el juicio de amparo puede adherirse a la revisión interpuesta por otra de las partes dentro del plazo de cinco días, contados a partir del día siguiente a aquél en que surta efectos la notificación de la admisión del recurso, expresando los agravios correspondientes. La adhesión al recurso sigue la suerte procesal de éste, de acuerdo con el artículo 82.

3.4. Interposición

El recurso de revisión se interpondrá por escrito y se expresarán los agravios que cause la resolución impugnada.

Si el recurso se interpone en contra de una resolución dictada en amparo directo, el recurrente deberá transcribir textualmente la parte de la sentencia que contenga un pronunciamiento sobre constitucionalidad de normas generales o establezca la interpretación directa de un precepto de la Constitución Política de los Estados Unidos Mexicanos, o la parte del concepto de violación respectivo cuyo análisis se hubiese omitido en la sentencia.

En caso que el escrito de expresión de agravios se presente en forma impresa, el recurrente deberá exhibir una copia del mismo para el expediente y una para cada una de las partes. Esta exigencia no será necesaria en los casos que el recurso se presente en forma electrónica.

Cuando no se haga la transcripción a que se refiere el párrafo primero o no se exhiban las copias a que se refiere el párrafo anterior, se requerirá al recurrente para que en el

plazo de tres días lo haga; si no lo hiciere se tendrá por no interpuesto el recurso, salvo que se afecte al recurrente por actos restrictivos de la libertad, se trate de menores o de incapaces, o se afecten los derechos agrarios de una población ejidal o comunal o de ejidatarios o comuneros en lo individual, o quienes por sus condiciones de pobreza o marginación se encuentren en clara desventaja social para emprender un juicio, en los que el órgano jurisdiccional expedirá las copias correspondientes.

Son competentes para conocer el recurso de revisión:

a) La Suprema Corte de Justicia de la Nación. Por disposición legal, por acuerdos generales, o cuando ejerce su facultad de atracción (oficiosa o a solicitud tribunal colegiado).[1412]

b) Los tribunales colegiados de circuito.

El plazo para interponerlo es de 10 días hábiles contados a partir de la fecha en que sea notificado de la resolución recurrida.[1413]

Son condiciones de legitimación:

a) gozar del atributo de parte, acorde a lo previsto en el artículo quinto de la Ley de Amparo y

b) tener interés para que subsista o desaparezca una resolución determinada.

La autoridad responsable solo podrá interponer el recurso de revisión contra sentencias que afecten directamente el acto reclamado de cada una de ellas.

Empero, las autoridades judiciales o jurisdiccionales carecen de legitimación para recurrir las sentencias que declaren la inconstitucionalidad del acto reclamado, cuando este se hubiera emitido en ejercicio de la potestad jurisdiccional, ya que este tipo de autoridades tienen como característica esencial la imparcialidad que es intrínseca a la función jurisdiccional.[1414]

3.5. Reglas al decidir

El proceso de decisión se describe con todo detalle en los siguientes preceptos de la Ley:

> Artículo 93. Al conocer de los asuntos en revisión, el órgano jurisdiccional observará las reglas siguientes:
>
> I. si quien recurre es el quejoso, examinará, en primer término, los agravios hechos valer en contra del sobreseimiento decretado en la resolución recurrida.
>
> Si los agravios son fundados, examinará las causales de sobreseimiento invocadas y no estudiadas por el órgano jurisdiccional de amparo de primera instancia, o surgidas con posterioridad a la resolución impugnada;

1412 "Artículo 85. Cuando la Suprema Corte de Justicia de la Nación estime que un amparo en revisión, por sus características especiales deba ser de su conocimiento, lo atraerá oficiosamente conforme al procedimiento establecido en el artículo 40 de esta Ley.

El tribunal colegiado del conocimiento podrá solicitar a la Suprema Corte de Justicia de la Nación que ejercite la facultad de atracción, para lo cual expresará las razones en que funde su petición y remitirá los autos originales a ésta, quien, dentro de los treinta días siguientes al recibo de los autos originales, resolverá si ejercita la facultad de atracción, procediendo en consecuencia en los términos del párrafo anterior".

1413 "Artículo 86. El recurso de revisión se interpondrá en el plazo de diez días por conducto del órgano jurisdiccional que haya dictado la resolución recurrida".

1414 "Artículo 87. Las autoridades responsables solo podrán interponer el recurso de revisión contra sentencias que afecten directamente el acto reclamado de cada una de ellas; tratándose de amparo contra normas generales podrán hacerlo los titulares de los órganos del Estado a los que se encomiende su emisión o promulgación.
Las autoridades judiciales o jurisdiccionales carecen de legitimación para recurrir las sentencias que declaren la inconstitucionalidad del acto reclamado, cuando éste se hubiera emitido en ejercicio de la potestad jurisdiccional".

II. si quien recurre es la autoridad responsable o el tercero interesado, examinará, en primer término, los agravios en contra de la omisión o negativa a decretar el sobreseimiento; si son fundados se revocará la resolución recurrida;

III. para los efectos de las fracciones I y II, podrá examinar de oficio y, en su caso, decretar la actualización de las causales de improcedencia desestimadas por el juzgador de origen, siempre que los motivos sean diversos a los considerados por el órgano de primera instancia;

IV. si encontrare que por acción u omisión se violaron las reglas fundamentales que norman el procedimiento del juicio de amparo, siempre que tales violaciones hayan trascendido al resultado del fallo, revocará la resolución recurrida y mandará reponer el procedimiento;

V. si quien recurre es el quejoso examinará los demás agravios; si estima que son fundados, revocará la sentencia recurrida y dictará la que corresponda;

VI. si quien recurre es la autoridad responsable o el tercero interesado, examinará los agravios de fondo, si estima que son fundados, analizará los conceptos de violación no estudiados y concederá o negará el amparo; y

VII. solo tomará en consideración las pruebas que se hubiesen rendido ante la autoridad responsable o el órgano jurisdiccional de amparo, salvo aquéllas que tiendan a desestimar el sobreseimiento fuera de la audiencia constitucional.

Artículo 94. En la revisión adhesiva el estudio de los agravios podrá hacerse en forma conjunta o separada, atendiendo a la prelación lógica que establece el artículo anterior.

Artículo 95. Cuando en la revisión concurran materias que sean de la competencia de la Suprema Corte de Justicia de la Nación y de un tribunal colegiado de circuito, se estará a lo establecido en los acuerdos generales del Pleno de la propia Corte.

Artículo 96. Cuando se trate de revisión de sentencias pronunciadas en materia de amparo directo por tribunales colegiados de circuito, la Suprema Corte de Justicia de la Nación resolverá únicamente sobre la constitucionalidad de la norma general impugnada, o sobre la interpretación directa de un precepto de la Constitución Política de los Estados Unidos Mexicanos o de los derechos humanos establecidos en los tratados internacionales de los que el Estado mexicano sea parte.

Complementariamente, resulta pertinente invocar la tesis I.15º.A.J/10, que dice:

AMPARO EN REVISIÓN. MÉTODO DE ESTUDIO QUE DEBE SEGUIR EL TRIBUNAL COLEGIADO DE CIRCUITO AL QUE SE TURNA EL RECURSO MEDIANTE EL QUE SE IMPUGNA UNA SENTENCIA QUE VERSA SOBRE LA CONSTITUCIONALIDAD DE LEYES RESPECTO DE LAS QUE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN TIENE COMPETENCIA ORIGINARIA. De conformidad con lo previsto en los artículos 82, 83, 84 y 85 de la Ley de Amparo, en relación con el Acuerdo General 5/2001 emitido por el Tribunal Pleno de la honorable Suprema Corte de Justicia de la Nación, el Tribunal Colegiado de Circuito al que se turne el recurso de revisión interpuesto contra la sentencia dictada en un juicio de amparo indirecto en el que se cuestione la constitucionalidad de leyes cuya competencia originaria de estudio en revisión corresponde a ese Alto Tribunal, debe proceder de la siguiente forma: 1) examinar la procedencia del citado medio de impugnación, es decir, determinar si el escrito que lo contiene cumple con los requisitos formales establecidos en la ley de la materia; si el recurso se ubica en alguna de las hipótesis de procedencia a que se refiere el artículo 83 de la legislación en comento; si quien acude a la instancia está legitimado tanto en el proceso como en la causa, y finalmente si la interposición del medio de impugnación se realizó dentro del plazo legal; 2) verificar la regularidad del procedimiento del juicio, advirtiendo si se actualiza alguna violación que conduzca a revocar el fallo impugnado y a ordenar su reposición de conformidad con lo previsto en el numeral 91, fracción IV, del ordenamiento legal en cita; 3) dilucidar si en la sentencia recurrida el juzgador de garantías estudió en su integridad las causas de improcedencia hechas valer por las partes, aun cuando no sean las propuestas por aquellas que se hayan inconformado y, en su caso, analizar las omitidas; determinar si existe un diverso motivo de inejercitabilidad de la acción de garantías que deba estudiarse de oficio y abordar el

análisis de los agravios expuestos por la parte recurrente en relación con las causas de improcedencia que se estimaron actualizadas o, en su caso, infundadas; 4) una vez superados los presupuestos anteriores, establecer si el asunto se encuentra comprendido en alguna de las hipótesis por las que tiene competencia originaria la Suprema Corte de Justicia de la Nación, como es la subsistencia del problema de constitucionalidad respecto de una ley, a efecto de reservarle o no jurisdicción sobre el particular, para lo cual en principio es necesario que se verifique si el tema debatido se identifica con alguno de los que integran la competencia delegada a los tribunales colegiados de circuito según lo dispuesto en el Acuerdo General referido, a saber, que exista jurisprudencia definida del Alto Tribunal que resuelva el problema jurídico controvertido o que coincida con alguno de los enunciados en el catálogo previsto en el artículo quinto del mencionado acuerdo; y 5) determinar si existe algún tema de legalidad cuyo estudio no deba emprender hasta en tanto la superioridad defina el problema de constitucionalidad de leyes.

3.6. Queja

El recurso de queja es complementario al de revisión y tiene la particularidad que procede en contra de decisiones de menor entidad, de acuerdo con lo previsto en los numerales 97 al 103 de la Ley de Amparo.

Los supuestos de procedencia para el amparo indirecto se precisan en el artículo 97, fracción I; en tanto que para el directo las prevé la fracción II.

Puede hacerse valer en diversas etapas del juicio, tanto en el cuaderno principal como incidental, incluso después de dictada sentencia, incluso se puede detener el proceso en ciertos supuestos, según el ordinal 102.

El plazo para interponer una queja se estipula en el numeral 98 y su trámite se describe en los diversos 99 y 101. En el escrito de queja se deben expresar los agravios a que alude el dispositivo 100.

Sobre el tema resulta pertinente citar la tesis: XXVII.3o.19 K (10a.) que explica y aclara varios aspectos:

RECURSO DE QUEJA. REQUISITOS PARA SU ADMISIÓN (INTERPRETACIÓN DE LOS ARTÍCULOS 97 A 103 DE LA LEY DE AMPARO, VIGENTE A PARTIR DEL 3 DE ABRIL DE 2013). De la interpretación sistemática de los artículos 97 a 103 de la Ley de Amparo, vigente a partir del 3 de abril de 2013, que regulan el trámite del recurso de queja, se advierten los requisitos de admisibilidad siguientes: a) supuesto de hecho. La actuación o resolución que pretende refutarse debe ser subsumible en alguno de los casos previstos en el artículo 97 de la citada ley, de lo contrario, el recurso es improcedente; b) legitimación del recurrente. Es un presupuesto procesal que debe observarse en la controversia impugnativa del mismo modo que en la principal; por lo que debe revisarse tanto la correspondiente a la parte formal (procesal) como la que atañe a la parte material (causa) y, de encontrarse que no se colma este presupuesto, ya sea porque quien promueve no es parte material en el juicio de amparo o porque su representante no acredite su personalidad, debe estimarse que el recurso es improcedente; c) gravamen o perjuicio. Al igual que todo recurso, supone la existencia de una diferencia injustificada y desfavorable entre lo debido y lo actualizado, que la parte que se estima agraviada atribuye al proceder del juzgador del conocimiento. Esta diferencia debe importar un perjuicio o daño real y no solo aparente o supuesto, a los intereses o derechos del recurrente. Por tanto, si la resolución o acto que se combate no significa agravio o afectación alguna para el recurrente, debe considerarse que el recurso es improcedente; d) deducción oportuna. Debe presentarse dentro de los rangos de oportunidad que se encuentran previstos por la propia ley, por lo que si se hace fuera de los plazos especificados en su artículo 98, el recurso es improcedente por extemporáneo y e) formalidades de ley. Debe interponerse con las formalidades que la ley prevea para darle trámite, pues estas exigencias tienden a facilitar la debida integración de la controversia impugnativa, para lograr un pronunciamiento más expedito respecto de la materia del recurso. Así que se exija su presentación por

> escrito, que se expresen agravios, y se exhiban las copias para el expediente y las otras partes, son elementos que ayudan a dar celeridad al trámite y resolución del recurso; por ello, cuando se omiten dichos requerimientos, la ley sanciona su inobservancia con la consecuencia de tenerlo por no interpuesto.

La regla general es que no existe el reenvío (artículo 103) y por tanto, es de plena jurisdicción, a menos que el tribunal revisor decida reponer el procedimiento o carezca de elementos para tomar la decisión.

Es ilustrativo el criterio de la tesis: IV.3o.C.3 K (10a.) que dice:

> RECURSO DE QUEJA. SI SE DECLARA FUNDADO CONTRA EL AUTO QUE DESECHÓ PRUEBAS QUE NO SE OFRECIERON DENTRO DEL TÉRMINO PREVISTO EN EL ARTÍCULO 119 DE LA LEY DE AMPARO, EL TRIBUNAL COLEGIADO DE CIRCUITO DEBE DEVOLVER LOS AUTOS AL JUEZ DE DISTRITO A EFECTO DE QUE SE PRONUNCIE SOBRE LA IDONEIDAD Y/O PERTINENCIA DE LOS MEDIOS DE PRUEBA OFRECIDOS. De conformidad con el artículo 103 de la Ley de Amparo vigente, por regla general, en caso de resultar fundado el recurso de queja, el tribunal revisor está obligado a dictar la resolución que corresponda sin necesidad de reenvío y, solo por excepción, cuando la resolución implique la reposición del procedimiento, es permisible regresar el asunto al inferior a fin de que emita otra resolución en la que se subsanen los vicios concretos advertidos por el superior. En esos términos, al tratarse del supuesto previsto en el artículo 97, fracción I, inciso e), de la ley citada, cuando se declara fundado el recurso de queja contra el auto que desechó pruebas que no se ofrecieron dentro del término previsto en el artículo 119 de la Ley de Amparo, ello se equipara a una reposición del procedimiento, pues para desechar se basó únicamente en razón de la temporalidad. Y, si el Tribunal Colegiado de Circuito está limitado para analizar la idoneidad y/o pertinencia de los medios de prueba ofrecidos, al no contar con la totalidad de las constancias que conforman el sumario, de las cuales podrían emerger datos relevantes que influyan en la decisión correspondiente; entonces, es conveniente que el juez de distrito realice esa tarea acorde con las constancias de los autos, pues solo de esa manera, podrá verificar si los medios de prueba respectivos son idóneos (o no), a efecto de acreditar los extremos que pretende el oferente de la prueba.

Tocante a la resolución del recurso, Ovalle explica atinadamente que "una vez recibidas las constancias, el órgano jurisdiccional que conozca de la queja deberá dictar resolución dentro de los 40 días siguientes, o dentro de las 48 horas cuando se trate de resoluciones que concedan o nieguen la suspensión de plano o la provisional (artículo 101, párrafo final). Si el tribunal que conoce de la queja la considera fundada, deberá dictar la resolución que corresponda sin necesidad de reenvío, salvo que la resolución implique la reposición del procedimiento. En este supuesto, se dejará sin efecto la resolución recurrida y se ordenará al órgano que la hubiere emitido dictar otra, para lo cual la sentencia debe precisar los efectos concretos para llevar a cabo la reposición (artículo 103)".

3.7. Reclamación

Este recurso, previsto en los artículos 104 al 106 de la Ley de Amparo, procede en contra de los acuerdos de trámite dictados por los presidentes de la Suprema Corte de Justicia de la Nación, de sus salas o de los tribunales colegiados de circuito.

Lo puede interponer cualquiera de las partes, expresando los agravios, dentro del plazo de tres días siguientes al en que surta efectos la notificación de la resolución. La resolución debe dictarse dentro de los 10 días siguientes. Para el caso que la reclamación resulte fundada, dejará sin efectos el acuerdo impugnado y el presidente del órgano colegiado deberá emitir una nueva resolución en los términos determinados por el pleno del tribunal.

3.8. Inconformidad

Este recurso novedoso, previsto por primera vez en la Ley de Amparo de 2013 (artículos 201 al 203), tiene el objetivo de presentar un amplio espectro de impugnación contra cualquier decisión asumida en la etapa de cumplimiento de la sentencia definitiva.

> Los supuestos de procedencia referidos en el artículo 201 son los siguientes:
>
> Artículo 201. El recurso de inconformidad procede contra la resolución que:
>
> I. tenga por cumplida la ejecutoria de amparo, en los términos del artículo 196 de esta Ley;
>
> II. declare que existe imposibilidad material o jurídica para cumplir la misma u ordene el archivo definitivo del asunto;
>
> III. declare sin materia o infundada la denuncia de repetición del acto reclamado; o
>
> IV. declare infundada o improcedente la denuncia por incumplimiento de la declaratoria general de inconstitucionalidad.
>
> Cabe agregar otras causales más, tal como la declaratoria de incumplimiento dictada por el juez, las decisiones terminales sobre cumplimiento sustituto o en el incidente que califica el cumplimiento.
>
> El objetivo del recurso en cita aparece especificado en la jurisprudencia 1a./J. 120/2013 (10a.):
>
> RECURSO DE INCONFORMIDAD. MATERIA DE ESTUDIO DE DICHO RECURSO. La materia del recurso de inconformidad previsto en el artículo 201 de la Ley de Amparo, publicada en el *Diario Oficial de la Federación* el 2 de abril de 2013, conforme a su fracción I, la constituye la resolución que tenga por cumplida la ejecutoria de amparo, en los términos del artículo 196 de la propia ley; es decir, el estudio de legalidad de la determinación de la autoridad que haya conocido del juicio de amparo, en el sentido de que la ejecutoria ha sido cumplida totalmente. Por tanto, su análisis debe atender a la materia determinada por la acción constitucional, así como al límite señalado en la ejecutoria en que se otorgó la protección de la justicia federal, sin excesos ni defectos, y no a la legalidad de la resolución emitida por la autoridad responsable en aspectos novedosos que no fueron analizados por el juzgador de amparo. Así, el cumplimiento total de las sentencias, sin excesos ni defectos, a que se refiere el primer párrafo del citado artículo 196, supone el análisis y la precisión de los alcances y efectos de la ejecutoria, a partir de la interpretación del fallo protector y de la naturaleza de la violación examinada en él, para que, una vez interpretada esa resolución, se fijen sus consecuencias para lograr el restablecimiento de las cosas al estado que guardaban antes de la violación constitucional de que se trate, sin que ello signifique que el juez pueda incorporar elementos novedosos a su análisis para extender los efectos precisados en el fallo a otras posibles violaciones aducidas por los quejosos, que no hayan sido motivo de protección por parte de la justicia de la Unión.

Su trámite está previsto en los artículos 202 y 203.

Tienen legitimación para interponerlo los sujetos señalados en el numeral 202 que dice:

> Artículo 202. El recurso de inconformidad podrá interponerse por el quejoso o, en su caso, por el tercero interesado o el promovente de la denuncia a que se refiere el artículo 210 de esta Ley, mediante escrito presentado por conducto del órgano judicial que haya dictado la resolución impugnada, dentro del plazo de quince días contados a partir del siguiente al en que surta efectos la notificación.
>
> La persona extraña a juicio que resulte afectada por el cumplimiento o ejecución de la sentencia de amparo también podrá interponer el recurso de inconformidad en los mismos términos establecidos en el párrafo anterior, si ya había tenido conocimiento de lo actuado ante el órgano judicial de amparo; en caso contrario, el plazo de quince días se contará a partir del siguiente al en que haya tenido conocimiento de la afectación. En cualquier caso, la persona extraña al juicio de amparo solo podrá alegar en contra del cumplimiento o ejecución indebidos de la ejecutoria en cuanto la afecten, pero no en contra de la ejecutoria misma.

> Cuando el amparo se haya otorgado en contra de actos que importen peligro de privación de la vida, ataques a la libertad personal fuera de procedimiento, incomunicación, deportación o expulsión, proscripción o destierro, extradición, desaparición forzada de personas o alguno de los prohibidos por el artículo 22 de la Constitución Política de los Estados Unidos Mexicanos, así como la incorporación forzosa al Ejército, Armada o Fuerza Aérea nacionales, la inconformidad podrá ser interpuesta en cualquier tiempo.

Sobre el tema hay diversos criterios jurisprudenciales, siendo destacables los siguientes:

RECURSO DE INCONFORMIDAD. ALCANCES Y LÍMITES EN SU ESTUDIO. El artículo 107, fracción XVI, párrafo último, de la Constitución Política de los Estados Unidos Mexicanos establece que no podrá archivarse juicio de amparo alguno sin que la sentencia relativa quede enteramente cumplida; por ello, el análisis que se emprenda en el recurso de inconformidad para determinar si fue correcta o no la determinación que la tuvo por cumplida, no debe limitarse a los argumentos planteados por el recurrente, pues la Suprema Corte de Justicia de la Nación cuenta con facultades amplias para analizar oficiosamente si la ejecutoria de amparo fue o no acatada. Ahora, si bien es cierto que en la legislación de amparo abrogada, para dicho análisis bastaba con realizar un estudio comparativo general o básico entre lo ordenado en la ejecutoria y lo ejecutado por la autoridad responsable, también lo es que ello obedecía a que en esa legislación se contemplaba al recurso de queja como un medio para combatir el exceso o defecto en el cumplimiento; de ahí que para tener por cumplida la sentencia protectora, era suficiente con que la autoridad acreditara haber realizado lo ordenado, sin que al respecto debiera analizarse si había incurrido en exceso o defecto pues, de ser así, las partes podían interponer el recurso de queja; no obstante, éste ya no se contempla para ese fin en la Ley de Amparo vigente, en tanto que ahora el exceso o defecto puede combatirse a través del recurso de inconformidad. En efecto, aunque el artículo 201, fracción I, de la Ley de Amparo, vigente a partir del 3 de abril de 2013, solo señala que el recurso de inconformidad procede contra la resolución que tenga por cumplida la ejecutoria de amparo, sin especificar que en él puedan combatirse los excesos o defectos en que incurra la responsable en el cumplimiento, de una interpretación armónica de ese numeral con los artículos 192, párrafo primero, 196 y 197 de la propia ley, se concluye que en este medio de impugnación pueden combatirse esos vicios, pues para que una ejecutoria pueda declararse cumplida es preciso que la responsable acate puntualmente lo ordenado sin incurrir en exceso o defecto. Atento a ello, si la materia del recurso de inconformidad, vista en relación con la anterior Ley de Amparo, ha sido ampliada, entonces para resolver este recurso ya no basta con realizar un examen comparativo general o básico entre las conductas señaladas por el órgano jurisdiccional como efecto de la concesión del amparo y las adoptadas por la autoridad responsable, pues ahora, en adición a ese examen, también debe verificarse que en el cumplimiento de la ejecutoria no haya habido exceso o defecto, para lo cual deberá tenerse presente que hay exceso, cuando la responsable se extralimita en el cumplimiento por ir más allá de lo ordenado en la ejecutoria y que, por el contrario, habrá defecto, cuando la autoridad cumple parcialmente con lo ordenado, o lo hace deficientemente; sin embargo, al hacer ese análisis, debe tenerse presente el límite señalado en la ejecutoria donde se otorgó la protección de la justicia federal, así como la libertad de jurisdicción que, en su caso, se haya otorgado a la responsable, pues a pesar de la ampliación en su materia, no es factible que a través de este medio se analice la legalidad de la resolución emitida por la autoridad responsable, ni mucho menos introducir aspectos novedosos que no fueron analizados por el juzgador de amparo.[1415]

La jurisprudencia 1a./J. 36/2017 indica que la principal ratio constitucional y convencional del recurso de inconformidad es garantizar que el juicio de amparo sea un medio ju-

1415 Tesis de jurisprudencia 1a./J. 76/2014 (10a.).

dicial eficaz para la protección de los derechos humanos reconocidos por la Constitución y por los tratados internacionales.

> RECURSO DE INCONFORMIDAD. SU RATIO CONSTITUCIONAL Y CONVENCIONAL. Cuando una ejecutoria de amparo no es cumplida en su totalidad, ya sea porque la autoridad responsable incurre en exceso o en defecto respecto de lo ordenado por la autoridad de amparo, se menoscaba el mandato constitucional y convencional según el cual el juicio de amparo debe constituir un medio judicial eficaz para la protección de los derechos que la propia Constitución reconoce. El derecho humano a contar con una protección judicial eficaz de todos los derechos constituye uno de los pilares básicos del estado de derecho en México y, por ende, desde una interpretación sistemática de los artículos 1o., 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, en conexión con los artículos 1.1. y 25 de la Convención Americana sobre Derechos Humanos y 2.3. del Pacto Internacional de Derechos Civiles y Políticos, implica la obligación del Estado mexicano en su conjunto de establecer e implementar los medios procesales adecuados para que las ejecutorias de amparo sean cumplidas de manera que se protejan eficazmente los derechos declarados o reconocidos en la correspondiente ejecutoria; siendo así, el Estado está obligado a garantizar el debido cumplimiento de las sentencias protectoras, por parte de las autoridades responsables. De esta manera, la principal ratio constitucional y convencional del recurso de inconformidad es garantizar que el juicio de amparo sea un medio judicial eficaz para la protección de los derechos humanos reconocidos por la Constitución y por los tratados internacionales.

Resulta aplicable también el criterio que informa la Jurisprudencia 1a./J. 121/2013 (10a.):

> RECURSO DE INCONFORMIDAD. SON INOPERANTES LOS AGRAVIOS QUE NO CONTROVIERTEN LO RESUELTO POR EL ÓRGANO DE AMPARO EN RELACIÓN CON EL CUMPLIMIENTO DEL FALLO PROTECTOR. El hecho de que el artículo 196 de la Ley de Amparo, publicada en el *Diario Oficial de la Federación* el 2 de abril de 2013, establezca que la ejecutoria de amparo se entiende cumplida cuando lo sea en su totalidad, sin excesos ni defectos, no implica el estudio de aspectos que no fueron materia de análisis en el juicio de amparo, sino exclusivamente del exacto cumplimiento de las cuestiones que sí lo fueron, concretamente, de aquellas que dieron lugar a la concesión de la protección de la justicia federal. Por tanto, los agravios expuestos en el recurso de inconformidad resultan inoperantes cuando no controvierten lo resuelto por el órgano de amparo en relación con el cumplimiento del fallo dictado en el juicio, sino la forma en que la autoridad responsable cumplió con la sentencia protectora, con la pretensión de analizar aspectos ajenos a la materia del recurso de inconformidad hecho valer.

Asimismo, tiene aplicación la jurisprudencia 1a./J. 89/2007 emitida por la Primera Sala de la Suprema Corte de Justicia de la Nación, cuyos rubro y texto son:

> INCONFORMIDAD INTERPUESTA CONTRA LA RESOLUCIÓN QUE TIENE POR CUMPLIDA LA EJECUTORIA DE AMPARO. LA MATERIA DE SU ESTUDIO DEBE LIMITARSE AL ANÁLISIS DEL CUMPLIMIENTO RELATIVO, SIN PRONUNCIARSE SOBRE LA LEGALIDAD DE LAS CONSIDERACIONES DE LA RESPONSABLE. La materia de estudio de la inconformidad prevista en el artículo 105 de la Ley de Amparo, planteada contra la resolución de un juez de Distrito o de un tribunal colegiado de circuito, que estima cumplimentada la ejecutoria concesoria del amparo debe limitarse al análisis del cumplimiento de dicha sentencia, sin pronunciarse sobre la legalidad de las consideraciones en que la autoridad responsable haya fundamentado el acto con el que pretende acatarla, pues ello es ajeno a la indicada inconformidad.[1416]

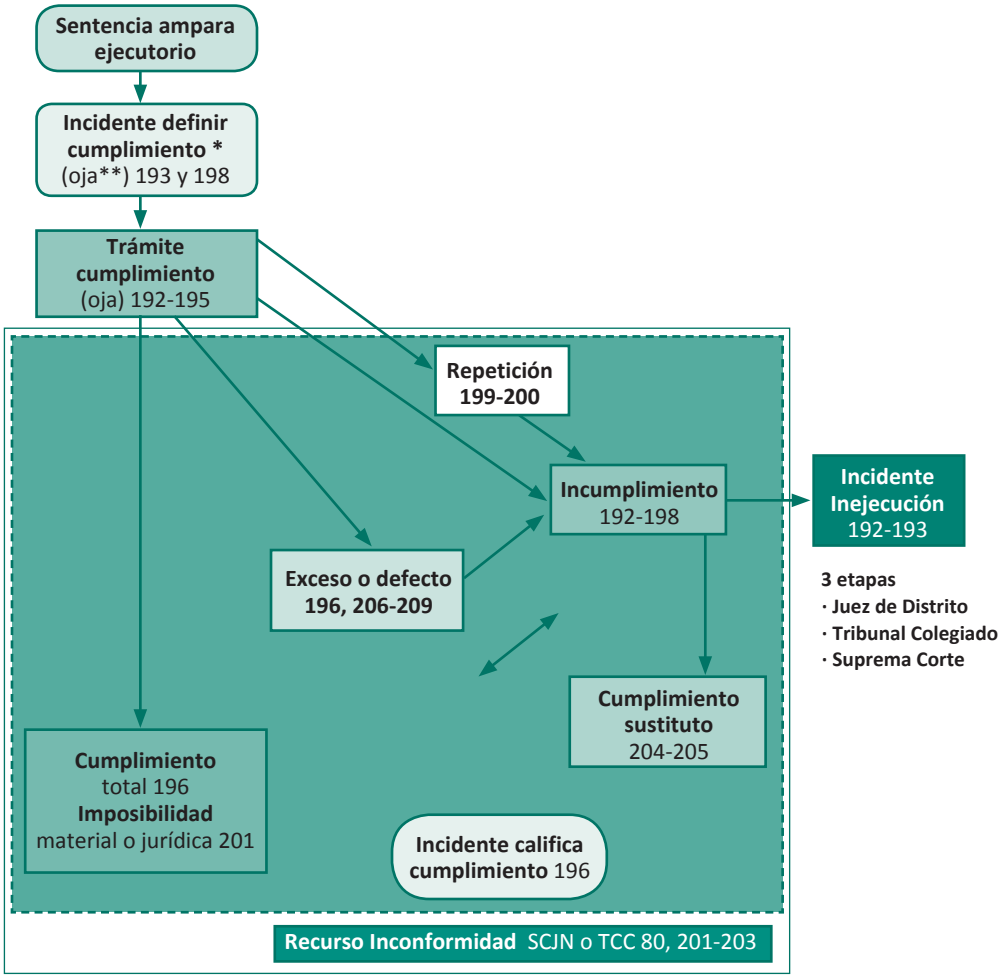
También es pertinente citar el criterio de la Tesis: IV.2o.A.7 K:

> RECURSO DE INCONFORMIDAD PREVISTO POR EL ARTÍCULO 105 DE LA LEY DE AMPARO. ÚNICAMENTE PROCEDE EN CONTRA DE LA RESOLUCIÓN QUE TIENE POR CUMPLIDA UNA EJECUTORIA. Del contenido del artículo 105 de la Ley de Amparo se advierten los requisitos que deben concurrir para la procedencia del medio de impugnación (inconformidad) en contra de la declaratoria que hacen los órganos de amparo, en lo atinente al cumplimiento de una sentencia de amparo que conceda la protección constitucional, que son: a) que se promueva por la parte interesada, que es el quejoso

1416 Época: Novena época. Registro: 172207. Instancia: Primera Sala. Tipo de Tesis: jurisprudencia. Fuente: *Semanario Judicial de la Federación y su Gaceta*. Tomo XXV, junio de 2007. Materia(s): común. Tesis: 1a./J. 89/2007, p. 66.

que obtuvo la protección de garantías; b) que se plantee en contra de la resolución que tenga por cumplida la ejecutoria de amparo y c) que se haga valer dentro del plazo de cinco días siguientes al de la notificación de la resolución correspondiente. Por ende, si en el caso la autoridad responsable en el juicio de garantías pretendió promover el mismo "en contra de los efectos que se le pretenden dar a la ejecutoria pronunciada", es inconcuso que el medio de inconformidad resulta notoriamente improcedente, ya que se encuentra contemplado en la Ley de Amparo, para combatir la resolución que tuvo por cumplida la ejecutoria de amparo. Además, la parte interesada, acorde con el espíritu de la norma, es la que obtuvo la protección constitucional, según su contenido normativo y la consecuente interpretación del propio precepto invocado, que permite reiterar que las autoridades, por imperativo legal del artículo 80 de la Ley Reglamentaria de los Artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos, solo les queda la obligación de cumplir fielmente la sentencia de amparo, mediante la restitución de la garantía violada. SEGUNDO TRIBUNAL COLEGIADO EN MATERIA ADMINISTRATIVA DEL CUARTO CIRCUITO.

En seguida se muestra un esquema, con vocación de síntesis y exhaustividad, sobre los supuestos de procedencia del recurso de inconformidad:



* En cualquier momento que sobrevenga incertidumbre sobre el modo a cumplir, deberá tramitarse o repetirse el incidente para definir cumplimiento.
oja**: órgano que tramitó el juicio de amparo, juzgado de distrito o Tribunal Colegiado de Circuito.

3.9. Incidentes impugnativos

De manera complementaria y por similitud en cuanto a efectos impugnativos, conviene considerar algunos incidentes, ejemplos de ellos son el de nulidad de notificaciones o el de exceso o defecto en el cumplimiento de la suspensión, falsedad de firma, de violación a la suspensión del acto reclamado, de reposición de autos y de inejecución.

Modalidades del aviso de privacidad

Jorge Antonio Orta Villar

La normatividad del sector privado establece tres modalidades o tipos de avisos de privacidad: el integral, el simplificado y el corto. En cambio, en la esfera pública únicamente se regulan dos modalidades: la integral y la simplificada.

En el sector privado, la modalidad en la que deberá ponerse a disposición del titular el aviso de privacidad estará condicionada por la manera en que el responsable obtenga los datos personales del titular.

Aplicación de las modalidades del aviso de privacidad		
Integral	Simplificado	Corto
Cuando los datos personales se obtengan personalmente del titular.	Cuando los datos personales se obtengan de manera directa o indirecta del titular.	Cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de forma tal que los datos personales recabados o el espacio para la difusión o reproducción del aviso de privacidad también lo sean.
Obligatorio en todo caso, aunque se pueda utilizar el simplificado o corto.	El responsable deberá proveer gratuitamente los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad integral.	

Por su parte, en el sector público las reglas respecto de la modalidad que deberá utilizarse para poner a disposición del titular el aviso de privacidad son que en un primer momento será la modalidad simplificada que deberá utilizar el responsable, no obstante, si el responsable lo cree conveniente, se podrá poner a disposición el aviso de privacidad en su modalidad integral. En todo caso, el aviso de privacidad integral deberá estar publicado, de manera permanente, en el medio señalado en el aviso de privacidad simplificado.

En la siguiente tabla se describen los requisitos que debe contener el aviso de privacidad en su modalidad integral, tanto para el sector público como para el privado.

Requisitos de información del aviso de privacidad integral	
Sector privado	Sector público
1) Identidad y domicilio del responsable: se debe señalar el nombre completo cuando se trate de persona física, o en su caso, la denominación o razón social de la persona moral, así como el domicilio completo del responsable. El domicilio del responsable deberá indicar, al menos, la calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa, y deberá corresponder a aquél para oír y recibir notificaciones. 2) Datos personales que se tratarán: se deben indicar para el cumplimiento de las finalidades para las que los obtiene, tanto los que recaba personal o directamente del titular, como aquéllos que obtiene indirectamente, por medio de fuentes de acceso público o transferencias. Para cumplir con lo anterior, el responsable deberá: a) Identificar los datos personales que trata o las categorías de los mismos. b) La mención de las categorías no deberá incluir frases inexactas, ambiguas o vagas, como "entre otros datos personales" o "por ejemplo". 3) Señalamiento expreso de datos personales sensibles: el listado de datos personales sujetos a tratamiento debe informar de manera expresa los datos personales sensibles que se tratarán. 4) Finalidades del tratamiento: se deben describir las finalidades para las cuales se tratarán los datos personales, conforme a lo siguiente: a) El listado de finalidades descritas debe ser completo y no utilizar frases inexactas, ambiguas o vagas como "entre otras finalidades", "otros fines análogos" o "por ejemplo". b) Las finalidades descritas en el aviso de privacidad deben ser determinadas, es decir, se requiere especificar sin lugar a confusión y de manera objetiva para qué objeto serán tratados los datos personales. c) En caso de existir, se deben incluir las finalidades relativas al tratamiento con fines de mercadotecnia, publicidad o prospección comercial. d) Se debe identificar y distinguir entre las finalidades que dieron origen y son necesarias para la existencia, mantenimiento y cumplimiento de la relación jurídica entre el responsable y titular, de aquéllas que no lo son. e) Se debe informar sobre el mecanismo que el responsable tiene implementado para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales en relación con las finalidades que no son necesarias para la relación jurídica entre el responsable y titular. 5) Mecanismo para manifestar la negativa: este mecanismo puede ser implementado a través de la inclusión de casillas u opciones de marcado en el propio aviso de privacidad, o bien fuera de éste, siempre que se encuentre disponible al momento en que el titular consulta el aviso de privacidad. En todos los casos, este mecanismo debe permitir que el titular manifieste su negativa previo al tratamiento de sus datos personales o al aprovechamiento de los mismos. 6) Transferencias de datos personales: el responsable debe informar al titular si el tratamiento de sus datos implica la transferencia de los mismos dentro o fuera del territorio nacional, para lo cual debe preverse lo siguiente: a) Los terceros receptores o destinatarios de los datos personales, ya sea identificando cada uno de éstos por su nombre, denominación o razón social o indicando su tipo, categoría o sector de actividad.	1) La denominación completa del responsable y, de manera opcional, las abreviaturas o acrónimos por los cuales es identificado por el público. 2) Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular. El listado de finalidades deberá ser completo y no utilizar frases inexactas, ambiguas o vagas. Las finalidades deberán ser específicas y claras, de tal forma que el titular identifique cada una de ellas sin confusión. 3) Cuando se realicen transferencias de datos personales que requieran consentimiento del titular, se deberá informar: los destinatarios o terceros públicos o privados, nacionales o internacionales a los que se transfieren los datos personales, identificándolos por su nombre, denominación o razón social, o bien, clasificándolos por categoría y las finalidades de las transferencias relacionándolas por cada destinatario o tercero receptor. 4) Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular. Se podrán incluir casillas u opciones de marcado u otro medio pertinente, siempre y cuando esté disponible al momento en que el titular consulte el aviso de privacidad y permita que manifieste su negativa, previo al tratamiento de sus datos personales o a la transferencia de éstos, según corresponda. 5) Fecha de elaboración o de última actualización del aviso de privacidad. 6) De manera opcional, las transferencias que no requieran el consentimiento identificando lo siguiente: i) los destinatarios o terceros receptores de los datos personales (públicos o privados, nacionales o internacionales) por su nombre, denominación o razón social; ii) las finalidades de las transferencias, relacionadas con cada destinatario o tercero receptor y iii) el fundamento legal que faculta o autoriza al sujeto obligado a llevar a cabo la transferencia, señalando los artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente, precisando su fecha de publicación o, en su caso, la fecha de la última reforma o modificación. 7) El domicilio del responsable (incluir calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa). Se podrán incluir datos de contacto como la dirección de la página de Internet, correo electrónico y número telefónico habilitados para la atención del público en general. 8) Los datos personales que serán sometidos a tratamiento (tanto los que recaba directa como indirectamente), identificando aquéllos que son sensibles. Los datos personales podrán identificarse puntualmente cada uno de ellos, o bien, mediante su tipo de identificación (laborales, académicos, biométricos, patrimoniales, sobre procedimientos judiciales o seguidos en forma de juicio, características físicas, migratorios y socioeconómicos, entre otros). De manera opcional, se podrán informar los medios y/o fuentes mediante los cuales se obtienen los datos personales, asociados con los datos personales.

continúa...

b) Las finalidades que justifican las transferencias de datos personales, las cuales deberán ser determinadas y distinguir entre aquéllas que requieren del consentimiento del titular para que se realicen, de las que se puedan llevar a cabo sin dicho consentimiento.

7) Cláusula para consentir la transferencia de datos personales: cuando las transferencias no actualicen los casos de excepción al consentimiento, el aviso de privacidad debe incluir una cláusula que permita al titular señalar si consiente o no la transferencia de los datos personales.

8) Medios para el ejercicio de derechos ARCO: el aviso de privacidad deberá informar al titular sobre:

a) Los medios habilitados por el responsable para atender las solicitudes de ejercicio de derechos ARCO, los cuales deberán implementarse de forma tal que no se limite el ejercicio de estos derechos por parte de los titulares.

b) Los procedimientos establecidos para el ejercicio de los derechos ARCO o los medios a través de los cuales el titular podrá conocer dichos procedimientos, los cuales deberán ser de fácil acceso para los titulares y con la mayor cobertura posible, (considerando su perfil y la forma en que mantienen contacto cotidiano o común con el responsable) gratuitos, debidamente habilitados y que hagan sencillo el acceso a la información.

c) Los datos de identificación y contacto de la persona o departamento de datos personales que dará trámite a las solicitudes de los titulares para el ejercicio de los derechos ARCO.

d) Los procedimientos referidos en el inciso b) anterior deben incluir lo siguiente:

i. Los requisitos, entre ellos, los mecanismos de acreditación de la identidad del titular y la personalidad de su representante, y la información o documentación que se deberá acompañar a la solicitud.

ii. Los plazos dentro del procedimiento.

iii. Los medios para dar respuesta.

iv. La modalidad o medio de reproducción mediante la cual el titular podrá obtener la información o datos personales solicitados a través del ejercicio del derecho de acceso, es decir, copias simples, documentos electrónicos o cualquier otro medio.

v. Los formularios, sistemas y otros métodos simplificados que, en su caso, el responsable haya implementado para facilitar al titular el ejercicio de los derechos ARCO.

9) Mecanismos y procedimientos para la revocación del consentimiento: el aviso de privacidad debe señalar expresamente la siguiente información:

a) Los medios habilitados por el responsable para atenderlas solicitudes de revocación del consentimiento de los titulares, los cuales deberán implementarse de forma tal que no se limite el ejercicio de este derecho por parte de los titulares.

b) El procedimiento establecido para la atención de las solicitudes de revocación del consentimiento, o bien, los medios a través de los cuales el titular podrá conocer dicho procedimiento, mismos que deben ser de fácil acceso para los titulares y con la mayor cobertura posible, considerando su perfil y la forma en que mantienen contacto cotidiano o común con el responsable, gratuitos, que estén debidamente habilitados, y que hagan sencillo el acceso a la información.

9) El fundamento legal que faculta al responsable para llevar a cabo el tratamiento, con independencia de que se requiera o no el consentimiento (incluir artículos, apartados, fracciones, incisos y nombre de los ordenamientos o disposición normativa vigente que lo faculta o le confiera atribuciones para realizar el tratamiento de datos personales que informa en el aviso de privacidad, precisando su fecha de publicación o, en su caso, la fecha de la última reforma o modificación).

a. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO. El procedimiento se podrá describir puntualmente en el aviso de privacidad, o bien, se podrá remitir al titular a un medio disponible para que lo conozca. En cualquiera de los dos casos, se deberá informar al menos lo siguiente: i) los requisitos que deberá contener la solicitud para el ejercicio de los derechos ARCO a que se refiere el artículo 52 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); ii) los medios a través de los cuales el titular podrá presentar solicitudes para el ejercicio de los derechos ARCO; iii) los formularios, sistemas y otros métodos simplificados que, en su caso, el INAI hubiere establecido para facilitar al titular el ejercicio de sus derechos ARCO; iv) los medios habilitados para dar respuesta a las solicitudes para el ejercicio de los derechos ARCO; v) la modalidad o medios de reproducción de los datos personales; vi) los plazos establecidos dentro del procedimiento, los cuales no deberán contravenir lo previsto en los artículos 51, 52, 53 y 54 de la LGPDPPSO y vii) el derecho que tiene el titular de presentar un recurso de revisión ante el INAI en caso de estar inconforme con la respuesta.

b. El domicilio de la unidad de transparencia (calle, número, colonia, ciudad, municipio o delegación, código postal y entidad federativa, así como su número y extensión telefónica).

c. Los medios a través de los cuales el responsable comunicará a los titulares los cambios o actualizaciones efectuados a los avisos de privacidad simplificados e integrales.

10) Opciones y medios para limitar el uso o divulgación de los datos personales: el aviso de privacidad debe informar sobre las opciones y medios que el responsable haya instrumentado para que el titular pueda limitar el uso y divulgación de sus datos personales, distintos al ejercicio de los derechos ARCO o a la revocación del consentimiento, como pueden ser la inscripción en el Repep (Registro Público Para Evitar Publicidad), el Reus (Registro Público de Usuarios que no deseen información publicitaria de Productos y Servicios Financieros), el registro en listados de exclusión propios del responsable, sectoriales o generales y la habilitación de medios por los cuales el titular pueda manifestar su negativa a seguir recibiendo comunicados o promociones por parte del responsable. 11) Uso de *cookies*, *web beacons* u otras tecnologías similares: cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología que le permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento deberá informar al titular, a través de una comunicación o advertencia colocada en un lugar visible, sobre el uso de esas tecnologías y sobre el hecho de que a través de las mismas se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos. 12) Cambios al aviso de privacidad: se debe señalar el medio y procedimiento implementado por el responsable para dar a conocer al titular los cambios o actualizaciones efectuados al mismo.	

Tanto en la normatividad del sector privado como en la de público se prevé la posibilidad de utilizar un aviso de privacidad en su modalidad simplificada. Lo que diferencia a la modalidad integral de la simplificada, es que esta última exige menos requisitos de información que el integral, de ahí su nombre.

Uno de los requisitos de información que caracteriza a la modalidad simplificada del aviso de privacidad es que ésta, en todos los casos, deberá informar al titular de los datos sobre los medios para que éste último pueda conocer el contenido del aviso de privacidad integral.

La última de las modalidades de avisos de privacidad existentes en México, y que únicamente aplica para el sector privado, es la del aviso de privacidad corto, el cual puede emplearse cuando el espacio para la obtención de los datos personales y para difundir el aviso de privacidad es mínimo y limitado, y los datos personales que se recaban también son mínimos. Esta modalidad de aviso de privacidad debe contener los siguientes elementos:

1) la identidad y domicilio del responsable;
2) las finalidades del tratamiento, y
3) los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral.

De la misma forma que en el caso del aviso de privacidad simplificado, será necesario también que el responsable proporcione al titular los medios para que éste último pueda conocer el contenido del aviso de privacidad integral.

Monetización de datos personales

Isabel Davara Fernández de Marcos,[1417]
Gregorio Barco Vega y
Alexis Cervantes Padilla

En la búsqueda del crecimiento económico y/o la eficiencia administrativa, el alto valor alcanzado por el tratamiento y análisis de datos personales en los últimos años ha llevado a las organizaciones de los sectores público y privado a invertir, de manera intensiva, en tecnologías como analítica de *big data*, inteligencia artificial, aprendizaje automatizado, internet de las cosas y cómputo en la nube, entre otras.

El concepto de "monetización de datos personales" adquiere una especial relevancia precisamente cuando los responsables visualizan a los datos personales como uno de sus principales activos.

En términos generales, podemos señalar que la "monetización de datos personales" es el acto de convertir los datos personales en dinero, o bien el acto a través del cual se intercambian los datos personales por algún bien o servicio. Algunas personas suelen señalar que la monetización de datos personales también implica utilizar los datos personales como materia prima respecto del desarrollo de un nuevo producto o servicio.

Aunque el término es relativamente reciente, podemos destacar varias definiciones:

1. "La monetización de datos personales implica utilizar los datos personales para obtener un beneficio económico cuantificable" (Gartner, 2016).[1418]
2. "El acto de intercambiar productos y servicios basados en información por moneda de curso legal o algo de valor equivalente percibido" (Barbara H. Wixom , 2014).[1419]
3. "La monetización de los datos se produce cuando el valor intangible de los datos se convierte en valor real, generalmente, vendiéndolos, o convirtiéndolos en otros beneficios tangibles" (Najjar y Kettinger, 2013).[1420]

Son dos los principales factores que actualmente impulsan a los responsables a monetizar los datos personales en su posesión:

1. el auge de tecnologías disruptivas: no puede cuestionarse, como adelantábamos, que el desarrollo de las prácticas actuales de monetizar datos personales es consecuencia directa del desarrollo tecnológico, principalmente del auge de las tecnologías como analíticas de *big data*, inteligencia artificial, aprendizaje automatizado, internet de las cosas y cómputo en la nube, y
2. las nuevas maneras de hacer negocio: algunos de los cambios radicales que se están dando en las organizaciones y que impulsan la práctica de monetizar datos personales son los siguientes:
   a) las organizaciones han establecido como una de sus principales prioridades destinar su inversión en tecnologías de la información;

1417 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

1418 Gartner. (2016). *Data Monetization-Gartner IT Glossary.* Disponible en: http://www.gartner.com/it-glossary/data monetization

1419 Wixom, B. (2014). *Cashing in on your data.* S.l. MIT Sloan School of Management.

1420 Najjar, M. y Kettinger, W. (2013). *Data Monetization: Lessons from a Retailer's Journey*. MIS Quarterly Executive, pp. 213-225.

b) las organizaciones han tenido una apertura en realizar prácticas de intercambio de información. Las empresas buscan allegarse de información mediante el intercambio de información con terceros;

c) las organizaciones buscan incentivar a sus clientes para que estos les compartan información que puedan monetizar y

d) las organizaciones han optado por implementar "lagos de datos"[1421] que les permite extraer conocimiento para conocer mejor a sus clientes.

La combinación de algunos de los factores antes mencionados ha provocado que distintas organizaciones impulsen la práctica de monetizar los datos personales en su posesión. La práctica de monetizar datos personales está presente en diversas industrias y sectores (público y privado), donde destacan los sectores de salud, educación, telecomunicaciones, bancario y financiero y el automotriz.[1422] Así, las organizaciones, a través de aplicar tecnologías como *big data* a los datos personales en su posesión, pueden generar (de manera lícita si se hace conforme a los requerimientos normativos) ingresos adicionales, independientemente de la industria específica en la que opere.

En este orden de ideas, deviene imprescindible que las organizaciones adopten las medidas necesarias para asegurarse de que el derecho de protección de datos personales de los individuos, titulares de los datos personales, sea respetado en todo momento. Para evitar una transgresión al derecho de protección de datos personales de los titulares, las organizaciones deben asegurarse de que los tratamientos de datos personales que tengan como propósito la monetización de estos se apegue a los principios y deberes previstos en la normatividad de datos personales que resulte aplicable.

Uno de los grandes retos que hoy en día enfrentan las organizaciones que llevan a cabo prácticas de monetizar datos personales es legitimar el uso de dichos datos personales para los anteriores fines, sin que dicho tratamiento vulnere el derecho a la protección de datos personales de los titulares. En este sentido, algunos de los riesgos en los que podría incurrir una organización al realizar prácticas de monetización de datos personales son los siguientes:

a) No ser suficientemente transparentes con los titulares de los datos personales.

b) Tomar decisiones equivocadas por la utilización de datos personales que no estén actualizados, esto es, que sean incorrectos.

c) Dejar de cumplir con los requerimientos legales en materia de protección de datos personales que resulten aplicables.

d) Causar una afectación al titular de los datos personas al tomar una decisión que pudiere resultar discriminatoria.

1421 Un lago de datos puede entenderse como un repositorio de datos masivo y de fácil acceso para realizar tratamientos mediante el uso de analíticas de *big data*.

1422 Como ejemplo práctico, una operadora de telecomunicaciones en 2012 en los Países Bajos celebró un acuerdo comercial con una empresa dedicada, principalmente, a realizar análisis a través de información relacionada con la ubicación de dispositivos móviles. El acuerdo entre las mencionadas empresas conlleva que la operadora le transfiera a la otra empresa información de carácter disociada generada a través de los datos personales de sus usuarios, a cambio de recibir un porcentaje de los ingresos que obtenga esta última como consecuencia de la utilización de dichos datos. Mediante el uso de los datos que la operadora le comparte a la otra empresa, esta última es capaz de generar información como el número de personas que entran o salen de determinado lugar, los destinos que visitan, la frecuencia en que realizan un viaje, los medios de transporte más utilizados, etc. Asimismo, con base en dichos datos la empresa es capaz de anticipar problemas de tráfico, o prevenir posibles situaciones de riesgo en determinado evento.

Para evitar la materialización de los riesgos antes señalados es indispensable que las organizaciones cuenten con un adecuado programa de privacidad y protección de datos personales al interior que les permita, en una primera instancia, identificar los posibles riesgos al tratamiento y, posteriormente, implementar los controles necesarios para lidiar correctamente con los riesgos identificados.

Monitoreo de datos personales

María Solange Maqueo Ramírez

El monitoreo de datos personales puede ser concebido como una forma de tratamiento de datos personales, especialmente cuando implica la recolección, uso o almacenamiento de los mismos y va más allá de la simple observación. Se trata de la utilización de distintos medios o herramientas, usualmente tecnológicas, que permiten dar seguimiento a las actividades, comportamientos, interacciones o comunicaciones de un individuo o grupo de individuos durante un periodo de tiempo, sea de manera ocasional o sistemática. De igual forma, el monitoreo de datos personales ha sido tradicionalmente considerado como una injerencia del Estado o de los particulares en la privacidad de las personas, por lo que se sujeta a las previsiones propias del derecho a la vida privada tanto en el ámbito nacional como internacional de los derechos humanos, esto es, que esté previsto en ley, que persiga un fin legítimo y que sea una medida idónea, necesaria y proporcional.[1423]

En la actualidad, dado el avance tecnológico y los crecientes flujos de información que ello conlleva, el monitoreo de datos personales se constituye en uno de los principales riesgos para la privacidad y la protección de datos personales de los individuos. Si bien puede producirse a través de la interferencia en los medios convencionales, tales como la correspondencia mediante el servicio postal, las llamadas telefónicas o la video vigilancia, el advenimiento de internet y otras tecnologías de la comunicación e información no solo incrementan el riesgo u oportunidad sino también el potencial impacto que pudiera tener una injerencia o tratamiento indebido de datos personales. Esta situación puede agravarse cuando se añaden otras técnicas de procesamiento de datos que permiten elaborar perfiles cada vez más precisos de las personas.[1424]

1. Algunos aspectos destacados en el ámbito de la protección de datos personales

Si bien las posibilidades de monitoreo de datos personales son muy amplias y abarcan distintos ámbitos de protección, los legisladores y las autoridades y otras organizaciones en materia de protección de datos personales al rededor del mundo se han ocupado de algunos aspectos de manera más específica para salvaguardar los derechos de las personas físicas.

1423 Cfr. Alexy, R. (2014). "Constitutional Rights and Proportionality", en *Revus, Journal for Constitutional Theory and philosophy of law*. Núm. 22, p. 52.

1424 El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), publicado en el *Diario Oficial de la Unión Europea* el 4 de mayo de 2016 define a la elaboración de perfiles como "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física." (Artículo 4).

Entre dichos aspectos cabe destacar los siguientes: (1) las prácticas de videovigilancia[1425] (incluido el uso de drones), (2) el monitoreo en el uso de internet, como el que se hace a través de *cookies*[1426] y (3) en las relaciones laborales.[1427]

Ninguna de estas actividades está prohibida *per se* pues son muchos los beneficios potenciales que supone su utilización, por ejemplo, en materia de seguridad pública y *compliance*. No obstante, existe un reconocimiento compartido en el sentido de que se requiere de salvaguardas y políticas específicas que mitiguen el riesgos de afectación a los derechos a la privacidad y la protección de los datos personales. De tal forma que, si bien están sujetas a los principios, deberes y procedimientos que de forma general comprende el derecho a la protección de datos personales, han recibido, en ocasiones, una atención particularizada por sus propias características.

En cualquier caso, la adopción de estas medidas tiene que ser idónea, necesaria y proporcional a los fines (legítimos) perseguidos. También debe ser transparente, no solo en su utilización sino también en los propósitos que persigue, salvo que con ello se impida el objetivo legítimo buscado, por ejemplo, por razones de seguridad pública o nacional; su alcance debe de ser lo más acotado posible y estar sujeto a límites temporales y, en su caso, espaciales; y, si ello es posible, se sugiere incorporar algunas medidas adicionales que mitiguen el impacto que ello representa en el tratamiento de los datos personales. En general, dado que el monitoreo implica un tratamiento de datos personales, debe cumplir con todos los principios del derecho a la protección de datos personales previstos en la legislación.

1425 A manera de ejemplo cabe mencionar la existencia de diversas leyes y reglamentos en materia de videovigilancia en Aguascalientes, Colima, Durango y Jalisco. Sobre el particular véase a Arteaga, N. (2016, mayo-agosto). "Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad", en *Espiral* (Guadalajara). Vol. 23, núm. 66. Guadalajara. México. De igual forma, el llamado entonces Instituto Federal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (IFAI) publicó en 2013 un modelo específico de aviso de privacidad para que pueda ser utilizado por los responsables del tratamiento de datos personales que utilizan sistemas de videovigilancia.

1426 En el ámbito de la Unión Europea existe una regulación específica para la utilización de *cookies* además de su incorporación expresa al Reglamento General de Protección de Datos, publicado en el *Diario Oficial de la Unión Europea,* el 4 de mayo de 2016. Al respecto véase la Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 que modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores, publicada en el *Diario Oficial de la Unión Europea* el 18 de diciembre de 2009. Además, actualmente está en proceso de aprobación el llamado Reglamento sobre privacidad de las comunicaciones electrónicas (o Reglamento *e-privacy*), presentado por la Comisión Europea el 10 de enero de 2017, a través del cual se pretende substituir la Directiva 2002/58/CE aún vigente.

1427 Cfr. Grupo de Trabajo del Artículo 29 sobre Protección de Datos, *Opinión 2/2017 on data processing at work*, adoptada el 8 de junio de 2017; Office of the Privacy Commisionar for Personal Data, Hong Kong, *Privacy Guideliness: Monitoring and Personal Data Privacy at Work*, Hong Kong, octubre de 2015; Information Commissioner´s Office (ICO), *The employment practices code*, Reino Unido, noviembre de 2011.

Multa

Gabriel López López

La multa es la consecuencia jurídica gravosa para el sujeto administrado que representa el pago en dinero de una prestación económica determinada derivada de la comisión de una conducta antijurídica considerada, en una hipótesis normativa, como infracción o bien, por la omisión en el cumplimiento de una obligación preexistente.

1. Naturaleza jurídica

Para Alfonso Nava Negrete, la multa es una sanción de carácter pecuniario que se aplica al infractor de una ley o reglamento administrativo. Aunque también se llegan a imponer por desacato a órdenes administrativas como son las de comparecencia. La persona infractora paga una cantidad en dinero a la autoridad sancionadora. Es distinta a la que también se llega a imponer a personas que han cometido un delito, multa que se previene en el código o ley penal como pena.[1428]

De conformidad con el artículo tercero del Código Fiscal de la Federación, las multas por infracción a normas administrativas federales tienen el carácter de aprovechamientos, no así de contribuciones, las que, por su parte, se encuentran previstas por el artículo segundo del CFF.

Al respecto, el primer párrafo del artículo tercero del CFF establece que las multas constituyen aprovechamientos al tratarse de ingresos que percibe el Estado por funciones de derecho público, distintos de las contribuciones, de los ingresos derivados de financiamientos y de los que obtengan los organismos descentralizados y las empresas de participación estatal.

Adicionalmente, las multas tienen el carácter de crédito fiscal, en tanto que el primer párrafo del artículo cuarto del CFF define a los créditos fiscales de la siguiente manera: "Son créditos fiscales los que tenga derecho a percibir el Estado o sus organismos descentralizados que provengan de contribuciones, de sus accesorios o de aprovechamientos, incluyendo los que deriven de responsabilidades que el Estado tenga derecho a exigir de sus funcionarios o empleados o de los particulares, así como aquellos a los que las leyes les den ese carácter y el Estado tenga derecho a percibir por cuenta ajena".

De conformidad con los dispositivos legales transcritos, las multas decretadas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) pertenecen al concepto de aprovechamientos, definidos en el artículo tercero del CFF, como los ingresos que percibe el Estado por funciones de derecho público, distintos de los que obtiene por contribuciones o ingresos derivados de financiamientos y de los que obtienen los organismos descentralizados y las empresas de participación estatal. La afirmación de que las multas administrativas constituyen aprovechamientos se ve corroborada por el hecho de que el artículo segundo del CFF, se clasifican a las contribuciones en impuestos, aportaciones de seguridad social y contribuciones de mejoras y derechos, siendo evidente que aquellas multas no están comprendidas en esta clasificación.

No pasa desapercibido el hecho de que todas las multas se catalogan dentro de los cobros fiscales, en razón de que se sigue el procedimiento económico-coactivo para hacerlas efectivas. Sin embargo, la naturaleza jurídica del crédito que implican varía según la materia del ordenamiento legal que establece tales sanciones y la autoridad que las aplica, como, por ejemplo, tratándose de multas fiscales, administrativas, judiciales, penales, etc.

1428 Nava, A. (1995). *Derecho Administrativo Mexicano*. 1a. ed. México. Fondo de Cultura Económica, p. 324.

La multa constituye tanto un instrumento económico sancionador, como una fuente de ingresos públicos para el Estado, a pesar de que con su imposición se logre una baja recaudación, pudiendo además ser impuestas tanto a particulares como a funcionarios y empleados públicos, a éstos últimos, por responsabilidades administrativas.

Al respecto, Giuliani Fonrouge define a los ingresos públicos como las entradas que obtiene el Estado, preferentemente en dinero, para la atención de las erogaciones determinadas por exigencias administrativas o de índole económico social.[1429]

2. Garantías y principios constitucionales.

Las garantías constitucionales contenidas en los artículos 14, 21, 22 y 23, que se refieren a las reglas y limitaciones para la imposición de penas, resultan plenamente aplicables tratándose de multas administrativas y a los procedimientos administrativos que establecen los lineamientos previos a su imposición, pues en todos esos casos se trata de la imposición de sanciones por la comisión de una infracción, y tanto las multas administrativas, como las penales, participan en alguna forma de la misma naturaleza y tienen el mismo origen y la misma finalidad, pero en algunos casos, la sanción penal puede reducirse a la sola multa, y los motivos de justicia y protección a la dignidad de la persona que rigen tales garantías tienen la misma validez en los casos apuntados, y tienden con las mismas bases a limitar la actuación discrecional del Estado.

Al resolver el amparo en revisión 2164/99, la Segunda Sala de la Suprema Corte de Justicia de la Nación emitió la tesis que dice:

> RESPONSABILIDADES DE LOS SERVIDORES PÚBLICOS. LAS SANCIONES ADMINISTRATIVAS PREVISTAS EN LA LEY FEDERAL RELATIVA TAMBIÉN SE RIGEN POR EL PRINCIPIO CONSTITUCIONAL DE EXACTA APLICACIÓN DE LA LEY QUE IMPERA EN LAS DE CARÁCTER PENAL, AUN CUANDO SEAN DE DIVERSA NATURALEZA. La marcada diferencia entre la naturaleza de las sanciones administrativas y las penales, precisada en la exposición de motivos del decreto de reformas y adiciones al título cuarto de la Constitución Federal, publicado en el *Diario Oficial de la Federación* el 28 de diciembre de 1982, en los artículos que comprende dicho título y en la propia Ley Federal de Responsabilidades de los Servidores Públicos, con base en la cual se dispone que los procedimientos relativos se desarrollarán en forma autónoma e independiente, no significa que en el ámbito sancionador administrativo dejen de imperar los principios constitucionales que rigen en materia penal, como es el relativo a la exacta aplicación de la ley (*nullum crimen, sine lege* y *nulla poena, sine lege*), que constituye un derecho fundamental para todo gobernado en los juicios del orden criminal, garantizado por el artículo 14 de la Constitución Federal, sino que tal principio alcanza a los del orden administrativo, en cuanto a que no se podrá aplicar a los servidores públicos una sanción de esa naturaleza que previamente no esté prevista en la ley relativa. En consecuencia, la garantía de exacta aplicación de la ley debe considerarse, no solo al analizar la legalidad de una resolución administrativa que afecte la esfera jurídica del servidor público, sino también al resolver sobre la constitucionalidad de la mencionada ley reglamentaria, aspecto que generalmente se aborda al estudiar la violación a los principios de legalidad y seguridad jurídica previstos en los artículos 14 y 16 constitucionales con los que aquél guarda íntima relación (2a. CLXXXIII/2001).[1430]

1429 Guiliani, C. (1973). *Derecho Financiero*. Vol. I, 2a. ed. Ediciones Depalma. Buenos Aires, p. 199.

1430 Tesis 2a. CLXXXIII/2001, *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XIV, septiembre de 2001, p. 718.

Debe tomarse en cuenta que al otorgar un amplio margen al INAI sobre el cual puede oscilar la cuantía de una multa (artículo 64 de la LFPDPPP)[1431] considerando para tales los elementos normativos establecidos en el artículo 65 de la misma Ley[1432] sobre la metodología para la imposición de la sanción, debe imperar el principio *lex certa*, a fin de que tanto las normas que contengan la hipótesis normativa considerada infractora, la sanción aplicable a dicha conducta y la metodología que se emplee para cuantificar el importe de la sanción, deben motivarse en hechos específicos y comprobables, de tal forma que se imposibilite a la autoridad de cualquier interpretación o aplicación analógica.

Tal es el criterio del cuarto tribunal colegiado en materia administrativa del primer circuito, según se advierte de la tesis I.4o.A.104 A (10a.), conforme al cual, cuando la norma habilitante en el derecho administrativo sancionador confiere pautas para amplias elecciones del operador, lo cual involucra diversos grados de discrecionalidad, la aplicación del principio aludido exige la más completa, adecuada y precisa motivación, como mecanismo de rendición de cuentas y antídoto de algún grado de eventual arbitrariedad.[1433]

1431 Artículo 64. Las infracciones a la presente Ley serán sancionadas por el Instituto con:
I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior.
II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior.
III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior.
IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

1432 Artículo 65. El Instituto fundará y motivará sus resoluciones, considerando:
i. la naturaleza del dato;
ii. la notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos de esta ley;
iii. el carácter intencional o no, de la acción u omisión constitutiva de la infracción;
iv. la capacidad económica del responsable, y
v. la reincidencia.

1433 Tesis I.4o.A.104 A (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo III, abril de 2018, p. 2258.

NOTAS

NOTAS

NOTAS

NOTAS

Neutralidad tecnológica

Jonathan Gabriel Garzón Galván

En el ámbito de las normas del uso de medios electrónicos en los actos jurídicos, resaltan varios principios en la interpretación, aplicación y regulación, entre ellos, el principio de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional. Estos principios se especifican, entre otros, en el artículo 89 del Código de Comercio.[1434]

El principio de neutralidad tecnológica establece que los cuerpos normativos que determinen la posibilidad del uso de medios tecnológicos en las distintas materias legales, así como su aceptación y valoración legal, deben ser neutrales desde un punto de vista tecnológico, en otras palabras, no deben obligar a las personas al uso de una tecnología específica.

La neutralidad tecnológica supone que la legislación debe definir los objetivos a conseguir, sin imponer ni discriminar el uso de cualquier otro tipo de tecnología para conseguir los objetivos fijados.[1435] Cristina Cullell señala que la neutralidad tecnológica tiene su sustento en cuatro compromisos:[1436]

1. No discriminación, al otorgar una aceptación y valoración jurídica igualitaria, sin favorecer una tecnología por encima de otra y no afectar así la competencia en el mercado.
2. Sostenibilidad, en cuanto a los medios tecnológicos, la regulación a usar debe ser flexible y sostenible, dado que la tecnología evoluciona más rápidamente que la propia regulación, y así se evitan revisiones legales periódicas, con el objetivo de adecuarla a los desarrollos tecnológicos constantes.

1434 Código de Comercio, última reforma DOF 28/03/2018. Disponible en: http://www.diputados.gob.mx /LeyesBiblio/pdf /3_280318.pdf
Artículo 89. (…) Las actividades reguladas por este título se someterán en su interpretación y aplicación a los principios de neutralidad tecnológica, autonomía de la voluntad, compatibilidad internacional y equivalencia funcional del mensaje de datos en relación con la información documentada en medios no electrónicos y de la firma electrónica en relación con la firma autógrafa.

1435 Cullell, C. (2010). "El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico", en *IDP. Revista de Internet, Derecho y Política*. Número 11. Fecha de consulta: agosto 2018.
Disponible en: http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-cullell/n11-cullell-e_

1436 Cullell, C. (2010). "El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico", en *IDP. Revista de Internet, Derecho y Política*. Número 11. Fecha de consulta: agosto 2018.
Disponible en: http://idp.uoc.edu/ojs/index.php/idp/article/view/n11-cullell/n11-cullell-e_

3. Eficiencia, se refiere a la no imposición de características específicas en la legislación por cada medio tecnológico, ya que la multiplicidad de tecnología actual y futura daría como resultado un exceso de normativa diferenciada que limite el potencial desarrollo tecnológico.
4. Certeza del usuario, brindar seguridad jurídica al usuario, quien no debe preocuparse de la tecnología utilizada por un proveedor de servicios o su contraparte, sino que será respaldado por la ley en caso de algún incumplimiento, independientemente de la tecnología que se utilice para el acto jurídico.

Los puntos anteriores son relevantes porque de emitirse regulaciones que obliguen o prefieran el uso de una tecnología o medio sobre otro, afecta de forma negativa al desarrollo de la tecnología y la innovación, por dos posibles escenarios:

a) hace a un lado la tecnología existente por falta de conocimiento, y por tanto, vuelve su uso algo casi ilegal al no reconocerles valor u aceptación, y
b) se requeriría una reforma de varias leyes, códigos, reglamentos, circulares o reglas, cada vez que se quisiera incorporar textualmente una nueva tecnología o medio tecnológico para realizar actos jurídicos, esto resultaría complicado ya que el proceso de reforma va a un ritmo mucho más lento que la innovación tecnológica.

Por ello, este principio debe inspirar a la actividad reguladora del Estado a enfocarse en los efectos jurídicos de los actos de las personas y no a los medios por los cuales se realizaron, es decir que contrario a centrarse en la tecnología, debe prestar especial atención a los efectos que emanan de su uso.

Para lograr lo anterior, la Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) incorporó en su definición de "mensajes de datos" la no discriminación de alguna tecnología al agregar las palabras "por medios electrónicos, ópticos o similares", dejando abierto dicho concepto.[1437]

Así mismo, la legislación mexicana incorporó en el concepto "mensajes de datos", y en los diversos ordenamientos donde se establece la posibilidad y aceptación del uso de los medios tecnológicos, las leyendas "medios electrónicos, ópticos o cualquier otra tecnología",[1438] "medios de comunicación electrónica o cualquier otro medio" y "medios de comunicación electrónica u otro medio similar",[1439] entre otras leyendas que tiene el mismo objetivo.

1437 El párrafo 31 de Ley Modelo de la CNUDMI sobre Comercio Electrónico y su guía para su incorporación al derecho interno. Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf. Establece que:
"La referencia a medios similares pretende reflejar el hecho de que la Ley Modelo no está únicamente destinada a regir las técnicas actuales de comunicación, sino que pretende ser apta para acomodar todos los avances técnicos previsibles. La definición de 'mensaje de datos' está formulada en términos por los que se trata de abarcar todo tipo de mensajes generados, archivados o comunicados en alguna forma básicamente distinta del papel. Por ello, al hablar de medios similares se trata de abarcar cualquier medio de comunicación y archivo de información que se preste a ser utilizado para alguna de las funciones desempeñadas por los medios enumerados en la definición, aunque, por ejemplo, no cabe decir que un medio 'óptico' de comunicación sea estrictamente similar a un medio 'electrónico' (…)".

1438 Algunos artículos son:
34, 38, 46 bis, 80, 89 y 1061 bis del Código de Comercio, última reforma DOF 28/03/2018. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf /3_280318.pdf
1803, 1805, 1811 y 1834 bis del Código Civil Federal, última reforma DOF 09/03/2018. Disponible en: http://www.diputados.gob.mx/LeyesBiblio /pdf/2_090318.pdf
210-A del Código Federal de Procedimientos Civiles, última reforma DOF 09/04/2012. Disponible en: http://www. diputados.gob.mx/LeyesBiblio/pdf/6.pdf
1-A de la Ley Federal del Procedimiento Contencioso Administrativo, última reforma DOF 27/01/201x7. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf
8 y 17 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el DOF 05/07/2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

1439 Artículo 35 de la Ley Federal del Procedimiento Administrativo, última reforma DOF 18/05/2018.
Disponible en: http://www. diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf

En el escenario en el que la regulación no establezca textualmente estas leyendas, el juzgador o la autoridad deberá tomar en cuenta la vertiente interpretativa de este principio, para que, al aplicar la ley lo haga de modo tal que no excluya, restrinja o favorezca alguna tecnología en particular.

La neutralidad tecnológica implica también el compromiso de la administración pública de no intervenir en el desarrollo de la tecnología, puesto que no debe primar una tecnología sobre otra, imponer una tecnología determinada o establecer barrera alguna al uso de una tecnología específica en su actos y resoluciones, de manera que se garantice el acceso a los servicios tecnológicos por todos los ciudadanos en los mismos términos y condiciones.

Finalmente, cabe señalar que este principio aplica tanto para la generación, almacenamiento, transmisión, firmado y autenticación de los actos jurídicos. En este sentido, la Ley Modelo sobre las Firmas Electrónicas de la CNUDMI, así como nuestro código de comercio tratan de reflejar el principio de la neutralidad respecto de los medios técnicos utilizados para firmar electrónicamente estableciendo que no se excluirán o privaran de efectos jurídicos a cualquier método para crear una firma electrónica, y que se aceptará cualquier método o sistema para crearla.[1440]

Nivel adecuado de protección de datos personales

Alejandro Alday González

La expresión "nivel adecuado de protección de datos personales" se refiere a un acto de ejecución, que respecto de un tercer Estado (no miembro de la Unión Europea) realiza la Comisión Europea[1441] (Comisión o CE) para legitimar las comunicaciones internacionales de datos (sean transferencias o transmisiones internacionales de datos) sobre la base de un apropiado nivel de protección a los datos personales provenientes de un determinado país que no forma parte de la Unión Europea, previo examen de aspectos relacionados con el cumplimiento de los derechos humanos, la existencia de legislación aplicable al tratamiento de datos personales, autoridades de control independientes, asunción de compromisos internacionales por parte del tercer Estado, entre otros aspectos que permitan acreditar que se otorga una adecuada protección a los datos personales.

1. Antecedentes

La noción de nivel adecuado de protección de datos personales surge a partir de la necesidad de establecer controles comunes para facilitar los flujos transfronterizos de datos personales entre los países y proteger la privacidad de las personas, evitando barreras innecesarias para la libre circulación de información entre los países.[1442]

1440 Artículos 3 de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas. Disponible en: http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf y 96 del Código de Comercio, última reforma DOF 28/03/2018. Disponible en: http://www.diputados.gob.mx/ LeyesBiblio/pdf /3_280318.pdf

1441 Debido a que este concepto ha sido creado y abordad en el territorio europeo hacemos referencia a los términos señalados en dicha legislación, así como a las y asociamos el concepto de tercer Estado con cualquier país que no sea parte de la Unión Europea. Sin embargo, en la práctica podrían darse casos en los que exista esta figura en otros Estados que han adoptado dicho término a su legislación ya sea de manera independiente o tomando como referencia los Estándares de Protección de Datos para los Estados Iberoamericanos.

1442 Cerda, A. (2011). "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea", en *Revista de derecho.* Valparaíso, pp. 327-356. Fecha de consulta: 30 de agosto de 2018. Disponible en https://dx.doi.org/10.4067/S0718-68512011000100009

Fue en la Organización para la Cooperación y el Desarrollo Económicos (OCDE) donde se realizaron los primeros esfuerzos para regular el tratamiento de datos personales y su comunicación entre países mediante la adopción de las Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales,[1443] del 23 de septiembre de 1980. En el Apartado 17[1444] de las Directrices se autorizó la restricción del flujo de datos cuando un tercer país no proporcionara un nivel de protección "equivalente".[1445]

Por otra parte, el 28 de enero de 1981, el Consejo de Europa adoptó el convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, conocido como Convenio 108 (ver definición de Convenio 108 en la presente obra) con el objeto de garantizar el derecho a la protección de datos personales en cada Estado parte.[1446] En relación con el flujo transfronterizo de datos personales, el Convenio 108 previó que podría darse cuando se brindara una protección equivalente entre los Estados parte de dicho instrumento.[1447]

Sin embargo, no sería sino hasta la emisión de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, el 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE) cuando se instituiría el concepto "nivel adecuado de protección de datos personales" para los flujos internacionales de datos.[1448]

La Directiva 95/46/CE distinguiría así dos conceptos fundamentales. Por un lado el concepto "nivel de protección equivalente" aplicable a las transferencias entre los países

1443 Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OCDE, de 23 de septiembre de 1980, consultadas el 30 de agosto de 2018. Disponibles en: http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf

1444 17. Todo país miembro debería evitar el restringir los flujos transfronterizos de datos personales entre él y otro país miembro, excepto si este último todavía no respeta sustancialmente estas Directrices o si la reexportación de esos datos pudiera transgredir su legislación nacional sobre privacidad. Pero un país miembro puede imponer restricciones respecto de ciertas categorías de datos personales para los que su legislación doméstica sobre privacidad contempla normas concretas dictadas por la naturaleza de esos datos, y para los que los demás Estados miembros no tienen prevista una protección similar.

1445 De acuerdo a los comentarios pormenorizado de la OCDE, el apartado 17 establece una norma de protección equivalente en la que la protección es sustancialmente similar en sus efectos a la del país exportador, pero que no tiene que ser idéntica en la forma ni en todos sus aspectos.

1446 Artículo 1. Objeto y fin
El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos).

1447 1. Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal que sean objeto de un tratamiento automatizado o reunidos con el fin de someterlos a ese tratamiento.
2. Una parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte.
3. Sin embargo, cualquier parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:
a) En la medida en que su legislación prevea una reglamentación específica para determinadas categorías de datos de carácter personal o de ficheros automatizados de datos de carácter personal, por razón de la naturaleza de dichos datos o ficheros, a menos que la reglamentación de la otra parte establezca una protección equivalente;
b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la parte a que se refiere el comienzo del presente párrafo.

1448 Artículo 1
Objeto de la Directiva
1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

miembros de la Unión Europea (UE) según se declara en los considerandos 8[1449] y 9[1450] del referido instrumento, y por otra parte el concepto "nivel adecuado de protección"[1451] en el supuesto de comunicaciones internacionales de datos personales con terceros Estados que no son parte de la UE, prohibiéndose la transferencia de datos personales a terceros países que no garantizaran un nivel adecuado de protección.[1452]

De esta manera, la Directiva 95/46/CE estableció el concepto de nivel adecuado de protección de datos personales, concepto que subiste aun con la reciente emisión del Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés).

2. Elementos de la definición y evaluación del nivel adecuado de protección conforme a la Directiva 95/46/CE

A pesar de que el concepto "nivel adecuado de protección" es instituido por la Directiva 95/46 y que subsiste en términos del RGPD,[1453] ninguna de estas disposiciones ha definido dicho término. Sin embargo, a lo largo de las disposiciones de ambos ordenamientos y las recomendaciones emitidas por el Grupo de Trabajo del Artículo 29 en materia de Protección de Datos (GT29 o WP29 por sus siglas en inglés)[1454] se puede advertir cuáles son sus elementos y alcance.

1449 (8) Considerando que para eliminar los obstáculos a la circulación de datos personales el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros; que ese objetivo, esencial para el mercado interior, no puede lograrse mediante la mera actuación de los Estados miembros, teniendo en cuenta, en particular, las grandes diferencias existentes en la actualidad entre las legislaciones nacionales aplicables en la materia y la necesidad de coordinar las legislaciones de los Estados miembros para que el flujo transfronterizo de datos personales sea regulado de forma coherente y de conformidad con el objetivo del mercado interior definido en el artículo 7 A del Tratado; que, por tanto, es necesario que la Comunidad intervenga para aproximar las legislaciones;

1450 (9) Considerando que, a causa de la protección equivalente que resulta de la aproximación de las legislaciones nacionales, los Estados miembros ya no podrán obstaculizar la libre circulación entre ellos de datos personales por motivos de protección de los derechos y libertades de las personas físicas, y, en particular, del derecho a la intimidad; que los Estados miembros dispondrán de un margen de maniobra del cual podrán servirse, en el contexto de la aplicación de la presente Directiva, los interlocutores económicos y sociales; que los Estados miembros podrán, por lo tanto, precisar en su derecho nacional las condiciones generales de licitud del tratamiento de datos; que, al actuar así, los Estados miembros procurarán mejorar la protección que proporciona su legislación en la actualidad; que, dentro de los límites de dicho margen de maniobra y de conformidad con el derecho comunitario, podrán surgir disparidades en la aplicación de la presente Directiva, y que ello podrá tener repercusiones en la circulación de datos tanto en el interior de un Estado miembro como en la Comunidad;

1451 (56) Considerando que los flujos transfronterizos de datos personales son necesarios para la desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;

1452 (57) Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;

1453 En relación con lo anterior, el considerando 106 del RGPD dispone lo siguiente:
La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado 6, o el artículo 26, apartado 4, de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) no. 182/2011 del Parlamento Europeo y del Consejo (12), establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

1454 El Grupo de Trabajo del Artículo 29 fue un organismo de consulta independiente, creado bajo el amparo de la anterior Directiva 95/46/CE formado por representantes de la totalidad de las autoridades de control nacionales de los Estados miembros, así como por el supervisor europeo de protección de datos y representantes también de la propia Comisión Europea encargados principalmente del estudio y análisis relativos a la aplicabilidad de la legislación europea en materia de protección de datos de carácter personal.

En primer lugar, conviene señalar (dado que las decisiones de adecuación otorgadas conforme a ese régimen subsisten en la actualidad hasta en tanto no sean modificadas o sustituidas)[1455] que, de acuerdo con lo previsto en el artículo 25.2 de la Directiva 95/46/CE, para evaluar el carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos y en particular lo siguiente:

a) la naturaleza de los datos;
b) la finalidad y la duración del tratamiento o de los tratamientos previstos;
c) el país de origen y el país de destino final;
d) las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, y
e) las normas profesionales y las medidas de seguridad en vigor en dichos países.

En este contexto, el WP29 destaca que todo análisis significativo de la protección adecuada debe comprender los dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz.[1456] Así, se ha considerado que, tomando como punto de partida la Directiva 95/46/CE, y teniendo en cuenta las disposiciones de otros textos internacionales sobre la protección de datos es posible realizar la compilación de una lista básica de condiciones mínimas para lograr un núcleo de principios de contenido de protección de datos y de requisitos de procedimiento/de aplicación, cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección.[1457]

El WP29 ha destacado que para el análisis de cualquier decisión de adecuación[1458] se deberán de reunir las siguientes condiciones mínimas:

Principios de contenido

Se sugiere la inclusión de los siguientes principios básicos:

a) Principio de limitación de objetivos. Los datos deben tratarse con un objetivo especificó y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia.
b) Principio de proporcionalidad y de calidad de los datos. Los datos deben ser exactos y, cuando sea necesario, estar actualizados.
c) Principio de transparencia. Debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal.

1455 Artículo 45
Transferencias basadas en una decisión de adecuación
[...]
9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

1456 Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales. "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la directiva sobre protección de datos de la UE, aprobada por el Grupo de Trabajo del Artículo 29, el 24 de julio de 1998. Fecha de consulta: 30 de agosto de 2018. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_es.pdf

1457 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas por el que se deroga la directiva 95/46/CE (en adelante, RGPD). Esta vez es el turno de los principios relativos al tratamiento.

1458 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas por el que se deroga la directiva 95/46/CE (en adelante, RGPD). Esta vez es el turno de los principios relativos al tratamiento.

d) Principio de seguridad. El responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento.

e) Derechos de acceso, rectificación y oposición. El interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos.

f) Restricciones respecto a transferencias sucesivas a otros terceros países. Únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último garantice asimismo un nivel de protección adecuado, salvo las excepciones previstas en la normatividad.

3. Mecanismos del procedimiento/de aplicación

Con el fin de sentar las bases para evaluar el carácter adecuado de la protección ofrecida, es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimiento judiciales y no judiciales utilizados en terceros países. Los objetivos de un sistema de protección de datos son básicamente tres:

a) Ofrecer un nivel satisfactorio de cumplimiento de las normas. Aun cuando no se puede garantizar un nivel de cumplimiento total a las normas, se destaca la necesidad de que los responsables del tratamiento conozcan muy bien sus obligaciones y los interesados conozcan muy bien sus derechos, y cuenten medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante para garantizar la observancia de las normas, al igual que lo son los sistemas de verificación directa por las autoridades, los auditores o los servicios de la administración encargados específicamente de la protección de datos.

b) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

c) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones.

Derivado de lo anterior, la Comisión ha realizado el análisis de distintos regímenes regulatorios de terceros Estados y ha hecho constar, de conformidad con el procedimiento previsto en el artículo 25[1459] de la Directiva 95/46/CE, que los siguientes países proporcionan un nivel de protección adecuado:

1459 Artículo 25
Principios
1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.
2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

1. Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000
2. Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la Ley Canadiense de Protección de Datos
3. Argentina. Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003
4. Guernesey. Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003
5. Isla de Man. Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004
6. Jersey. Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008
7. Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010
8. Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010
9. Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011
10. Uruguay. Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012
11. Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012
12. Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016

No obstante, debe destacarse que, el hecho de que un país no esté incluido en la lista blanca, ello no significa que dicho país esté incluido implícitamente en una "lista negra", sino que aún no se dispone de una orientación general relativa a dicho país. Con todo, la dificultad principal de este enfoque es que muchos países terceros no tienen una protección uniforme en todos los sectores económicos. Por ejemplo, muchos países tienen legislación sobre protección de datos en el sector público pero no en el privado.

En consecuencia, no debe olvidarse que la frase "nivel adecuado de protección" brinda suficiente flexibilidad a efectos de su aplicación a las diferentes realidades en que dicho estándar es aplicado.

4. Nivel adecuado de protección de datos personales en el Reglamento General de Protección de Datos

El artículo 45 Reglamento General de Protección de Datos (RGDP) dispone las condiciones sobre las cuales se realizarán las transferencias de datos personales basadas en una decisión de adecuación e indica que las mismas podrán llevarse a cabo cuando la CE haya que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado sin que estas queden sujetas a autorización específica.

---

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.
4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.
5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.
6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

De esta forma, el segundo apartado del artículo 45 precisa que al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

- El Estado de derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos.[1460]
- La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la UE y de los Estados miembros.
- Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.[1461]

Derivado de lo anterior, el apartado tres del artículo 45 del RGPD indica que, una vez evaluada la adecuación del nivel de protección podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado. Asimismo, según dispone el apartado tres del artículo 45 del RGPD, el acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control.

1460 En este mismo sentido se encuentra el considerando 104 del RGPD:
En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país respeta el Estado de derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

1461 El Considerando 105 dispone, además:
Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional. La comisión debe consultar al comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales.

Por otro lado, el RGPD dispone que el acto de ejecución establecerá un mecanismo de revisión periódica,[1462] al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. Además del mecanismo de revisión periódica que determine la CE, ésta supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las decisiones adoptadas en términos del RGPD, así como aquellas adoptadas conforme a la Directiva 95/46/CE.

Finalmente, es relevante destacar que, de acuerdo con lo dispuesto por el apartado cinco del ya citado artículo 45 del RGPD, existe la posibilidad de que las decisiones de adecuación sean suspendidas, modificadas o derogadas cuando la información disponible, en particular tras la revisión referida en el párrafo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantice un nivel de protección adecuado.

5. Nivel adecuado de protección de datos en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) disponen reglas específicas para las transferencias de datos personales a terceros Estados, y en relación con éstas últimas se dispone que, tanto el responsable como el encargado podrán realizarlas cuando el país tercero receptor haya sido reconocido con un nivel adecuado de protección por parte del país transferente:

> 36. Reglas generales para las transferencias de datos personales
>
> 36.1. El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:
>
> a. El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de éste que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.
>
> [...]

En consecuencia, se advierte que los Estándares Iberoamericanos remiten a los Estados a facilitar reglas para el flujo transfronterizo de datos personales, siendo el reconocimiento de nivel adecuado de protección una de ellas.

1462 En este sentido, el considerando 106 del RGPD dispone lo siguiente:
La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado seis, o el artículo 26, apartado cuatro de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) número 182/2011 del Parlamento Europeo y del Consejo ([12]), establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

6. Cumplimiento de la normatividad interna para transferencias internacionales de datos personales en México

En la legislación mexicana en materia de protección de datos personales para los sectores público y privado no se alude de forma específica al concepto de nivel adecuado de protección ni a su reconocimiento como decisión oficial de carácter nacional, pero se señala que en el caso de las transferencias internacionales de datos fuera del territorio nacional el tercero receptor deberá asumir las mismas obligaciones de quien transfiere los datos.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en el segundo párrafo del artículo 36 precisa que el tercero receptor de una transferencia de datos personales, sea nacional o extranjero, deberá asumir las mismas obligaciones que correspondan al responsable que transfirió los datos:

> Artículo 36. Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.
>
> El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

En adición a lo anterior, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) dispone como condición específica para las transferencias internacionales que en las mismas el tercero receptor asuma idénticas obligaciones que el responsable que transfiere los datos:

> Condiciones específicas para las transferencias internacionales
>
> Artículo 74. Sin perjuicio de lo dispuesto en el artículo 37 de la Ley, las transferencias internacionales de datos personales serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales.

Reitera lo anterior el artículo 75 del RLFPDPPP que dispone que en el instrumento contractual que firmen las partes deberá plasmarse la asunción de iguales obligaciones para las partes:

> Formalización de las transferencias internacionales
>
> Artículo 75. A tal efecto, el responsable que transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

De forma similar, el artículo 68 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) indica que en el caso de las remisiones y/o transferencias internacionales de datos (fuera del territorio nacional) el tercero receptor se obligará a proteger los datos conforme a los principios y obligaciones de la LGPDPPSO y demás disposiciones aplicables:

> Artículo 68. El responsable solo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.

Asimismo, el artículo 66 de la LGPDPPSO precisa la obligación de formalizar las transferencias internacionales de datos personales para demostrar su alcance y contenido, así como la asunción de obligaciones entre las partes conforme a esta normativa:

> Artículo 66. Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

Los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) en su artículo 116 indican que las transferencias internacionales de datos personales se sujetarán a un nivel de cumplimiento similar o equiparable al de la normatividad nacional:

> Artículo 116. El responsable solo podrá transferir datos personales fuera del territorio nacional, cuando el receptor o destinatarios se obligue a proteger los datos personales conforme a los principios, deberes y demás obligaciones similares o equiparables a las previstas en la Ley General y demás normatividad mexicana en la materia, así como a los términos previstos en el aviso de privacidad que les será comunicado por el responsable transferente.

De esta manera es que la legislación mexicana, si bien no establece la obligación de que el país receptor cuente con un nivel adecuado de protección de datos, sí impone la obligación al receptor de cumplir con los principios, deberes y obligaciones establecidos en la normatividad nacional para el adecuado tratamiento de datos personales.

Notificación de vulneración de seguridad

Christian Paredes González

La notificación de la vulneración de seguridad es una obligación legalmente establecida para los responsables del tratamiento que consiste en informar a los titulares y en determinados casos a las autoridades competentes, en caso de que se produzca una vulneración de seguridad[1463] que afecte los derechos patrimoniales o morales del titular de los datos personales.

De acuerdo con las Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales[1464](Recomendaciones de Manejo de Incidentes), la notificación de vulneraciones de seguridad es un requisito contemplado en la normativa mexicana en materia de protección de datos personales, para que los titulares puedan tomar medidas para la protección de sus derechos morales y patrimoniales.[1465]

1463 El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares considera vulneraciones de seguridad a los siguientes incidentes:
Vulneraciones de seguridad.
Artículo 63. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:
I. La pérdida o destrucción no autorizada.
II. El robo, extravío o copia no autorizada.
III. El uso, acceso o tratamiento no autorizado.
IV. El daño, la alteración o modificación no autorizada.
Por su parte, el artículo 38 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados señala:
Artículo 38. Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:
I. La pérdida o destrucción no autorizada.
II. El robo, extravío o copia no autorizada.
III. El uso, acceso o tratamiento no autorizado.
IV. El daño, la alteración o modificación no autorizada.

1464 INAI. (2018). *Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales.* Disponible en: *http://inicio.ifai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf*

1465 Publicadas el 30 de octubre de 2013 en el *Diario Oficial de la Federación*.

1. Obligación legal

La obligación de notificar las vulneraciones de seguridad en el sector privado aparece regulada en el artículo 20 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que establece lo siguiente:

> Artículo 20. Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

Adicionalmente, el artículo 64 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) establece también la obligación de notificar las vulneraciones de seguridad sobre la misma base lógica prevista en el artículo 20 de la LFPDPPP:

> Notificación de vulneraciones de seguridad
>
> Artículo 64. El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

En el ámbito del derecho público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) señala en su artículo 40 que las vulneraciones de seguridad que comprometan los derechos patrimoniales y/o morales de los titulares deberán ser notificadas tanto al titular de los datos como al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como a los organismos garantes, según corresponda:

> Artículo 40. El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los organismos garantes de las entidades federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

De lo anterior se desprende que la obligación de notificar las vulneraciones de seguridad a las autoridades correspondientes (INAI y órganos garantes) es solamente aplicable al orden público, pues en el orden privado no existe tal requerimiento.

En las Recomendaciones de Manejo de Incidentes, el INAI considera también que en el supuesto de que como resultado de la investigación de un incidente se identifica un posible delito, se debe dar parte al ministerio público.

Las citadas recomendaciones también señalan que en algunos casos puede ser conveniente notificar a aseguradoras, instituciones financieras, autoridades de impartición de justicia o a centros de respuesta a incidentes, para obtener asesoría o proporcionar a los titulares mayor apoyo.

2. Momento para notificar la vulneración

En lo que corresponde al momento de notificar las vulneraciones de seguridad es importante retomar lo establecido en el RLFPDPPP y la LGPDPPSO que establecen las siguientes reglas para determinar el momento de la notificación de la vulneración:

a) LFPDPPP: en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la

afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

b) LGPDPPSO: en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.

Por otro lado, las Recomendaciones de Manejo de Incidentes señalan que se recomienda notificar a los titulares de la siguiente forma: (i) en el menor tiempo posible, (ii) cuando ya se tenga información concreta del incidente y (iii) cuando ya no exista exposición de los activos involucrados en la vulneración. Dentro del proceso de respuesta a incidentes, esto ocurre al final de la etapa de contención, o bien al inicio de la etapa de mitigación.

Las Recomendaciones además sugieren, respecto del sector público, que los notifiquen al titular y al INAI dentro de un plazo máximo de 72 horas, a partir de que se confirme la ocurrencia de éstas y el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de mitigación de la afectación. Se señala, además, que dicho plazo comenzará a correr el mismo día natural en que el responsable confirme la vulneración de seguridad.

3. Procedimiento de notificación de la vulneración

En relación con el procedimiento de notificación de vulneraciones, las Recomendaciones de Manejo de Incidentes establecen que el método recomendado de notificación es el directo con los titulares, es decir por teléfono, correo electrónico, correo postal, o en persona. En caso de que exista urgencia por contactar al titular, puede resultar oportuno utilizar más de un medio de contacto a la vez.

Las Recomendaciones de Manejo de Incidentes también añaden que es posible adoptar la notificación indirecta a través de sitios *web* o medios de comunicación masivos, solamente cuando la notificación directa pueda causar más afectaciones al titular, sea muy costosa o no se tenga información de contacto.

Las Recomendaciones también precisan que la notificación debe ser independiente y personalizada, y no debe incluir material o información no relacionada con el incidente de seguridad, ya que podría causar confusión.

4. Elementos de la notificación de vulneración

Respecto de los elementos de la notificación de la vulneración, en primer lugar, la normatividad del sector privado en el RLFPDPPP contempla lo siguientes elementos:

Información mínima al titular en caso de vulneraciones de seguridad

> Artículo 65. El responsable deberá informar al titular al menos lo siguiente:
>
> I. La naturaleza del incidente;
>
> II. Los datos personales comprometidos;
>
> III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
>
> IV. Las acciones correctivas realizadas de forma inmediata, y
>
> V. Los medios donde puede obtener más información al respecto.

Por su parte, la LGPDPPSO considera como elementos para la notificación de la vulneración los previstos en su artículo 41:

Artículo 41. El responsable deberá informar al titular al menos lo siguiente:

I. la naturaleza del incidente;

II. los datos personales comprometidos;

III. las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;

IV. las acciones correctivas realizadas de forma inmediata, y

V. los medios donde puede obtener más información al respecto.

En este contexto podemos decir que hay dos tipos de notificaciones, la que debe hacerse al titular de los datos y la que deben realizarse a las autoridades de protección de datos personales.

Respecto de la notificación de la vulneración al titular de los datos, en términos de la normatividad aplicable y las Recomendaciones de Manejo de Incidentes, podemos decir que deberán considerar los siguientes elementos informativos:

a) Descripción de la vulneración: se debe explicar de manera muy sencilla y general el incidente ocurrido, en qué consistió, así como el periodo en el que se desarrolló. No se deben dar detalles o incluir información que revele vulnerabilidades o fallas específicas en los sistemas de tratamiento.

b) Datos personales involucrados: una descripción de la información involucrada en el incidente.

c) Recomendaciones a los titulares: el listado de acciones que puede realizar el titular para minimizar los efectos adversos de la vulneración.

d) Acciones correctivas o de mitigación: una descripción general de las acciones llevadas a cabo para evitar que incidentes similares se repitan.

e) Información de contacto: datos de las áreas designadas, mesas de servicio o del personal de la organización que puede atender dudas y proporcionar información adicional del incidente.

f) Fuentes de información adicional: referencias o documentos adicionales de consulta para apoyar a los titulares ante situaciones específicas, como el robo de identidad.

En lo que concierne a la notificación de vulneraciones en el sector público, del contenido dela LGPDPPSO, los Lineamientos de Protección de Datos Personales para el Sector Público y las Recomendaciones de Manejo de Incidentes, se desprende la obligatoriedad de practicar una notificación de vulneración a las autoridades de protección de datos (INAI y/o órganos garantes) mediante un escrito presentado en el domicilio, o bien a través de cualquier otro medio que se habilite para tal efecto, al menos con la siguiente información:

a) la hora y fecha en que se identificó la vulneración;

b) la hora y fecha en que inició la investigación sobre la vulneración;

c) la naturaleza de la vulneración ocurrida;

d) la descripción detallada de cómo ocurrió la vulneración;

e) los tipos de datos personales comprometidos y el número aproximado de titulares afectados;

f) los sistemas de tratamiento comprometidos;

g) las acciones correctivas realizadas de forma inmediata;

h) la descripción de las posibles consecuencias de la vulneración ocurrida;

i) las recomendaciones dirigidas al titular;

j) el medio puesto a disposición del titular para que obtenga mayor información sobre la vulneración y cómo proteger sus datos personales;

k) el nombre completo de la o las personas designadas para proporcionar mayor información al INAI o al órgano garante correspondiente, en caso de requerirse, y

l) cualquier otra información o documentación que considere conveniente hacer del conocimiento del INAI o del órgano garante correspondiente.

5. Registro de la vulneración

Las Recomendaciones de Manejo de Incidentes precisan que se debe generar un archivo histórico o bitácora que permita a los encargados de la respuesta a incidentes contar con una base de conocimiento, que pueda ser utilizada para entrenar a los usuarios, o a nuevos integrantes del equipo de respuesta a incidentes.

De esta manera, se sugiere que el reporte final sobre un incidente que se ha erradicado no sobrepase las dos semanas para su elaboración, a fin de no perder detalles importantes sobre lo aprendido.

Además de lo anterior, debe considerarse que el artículo 39 de la LGPDPPSO[1466] indica que los sujetos obligados deben de contar con una bitácora de registro de las vulneraciones en la que se describa:

a) en qué consistió la vulneración,

b) la fecha en la que ocurrió,

c) el motivo o causa de la vulneración y

d) las acciones correctivas implementadas de forma inmediata y a largo plazo.

Finalmente, se recomienda que una vez cerrado el incidente, el equipo de respuesta debe regresar a la etapa de preparación, a fin de actualizar las medidas de seguridad que permitan mejorar la atención y detección de alertas, así como la respuesta cuando se presenten nuevos incidentes de seguridad.

1466 Artículo 39. El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.

NOTAS

NOTAS

NOTAS

NOTAS

Organismos garantes

Sergio López Ayllón

Los organismos garantes son aquellos previstos en la Constitución Política de los Estados Unidos Mexicanos (CPEUM)[1467] para garantizar el ejercicio de los derechos de acceso a la información y protección de datos personales en sus respectivas competencias (federal y estatal). Los organismos garantes cuentan con autonomía constitucional, la cual les garantiza, normativamente, su independencia, imparcialidad, especialización e integración colegiada.[1468]

Delimitación conceptual y conceptos correlacionados

De acuerdo con el artículo 6 de la CPEUM, la federación debe contar con un organismo de acceso a la información y protección de datos personales que, entre otras características, sea autónomo, especializado, imparcial y colegiado. Por su parte, los artículos 116, fracción VIII, y 122, sección A, fracción VII, de la CPEUM establecen que las constituciones de los estados y de la Ciudad de México tienen que contemplar sus respectivos organismos autónomos que cuenten con las mismas especificidades y que cumplan con el mismo fin de protección y garantía de los derechos anteriormente mencionados. Estos organismos se regirán, en principio, por las constituciones y las leyes locales en materia de transparencia y acceso a la información pública y protección de datos personales.

El organismo de la federación y los organismos estatales y de la ciudad de México tienen distintos ámbitos de competencia donde ejercen sus atribuciones. Es decir, no se encuentran supeditados a una relación de jerarquía, sino que ejercen una competencia propia. Eventuales conflictos de competencia o sustantivos tienen que resolverse determinando cuál es el órgano competente.[1469]

Sin embargo, en la CPEUM se establece una excepción a este principio de validez competencial y es la facultad de resolver recursos de revisión. Según el artículo 6 de la CPEUM, el organismo garante federal "de oficio o a petición fundada del organismo garante equivalente de las enti-

1467 Artículos 6, 116 fracción VIII, y 122, sección A, fracción VII de la CPEUM.

1468 Artículo 3 y 37 de la Ley General de Transparencia y Acceso a la Información Pública.

1469 Legislaciones federal y local. Entre ellas no existe relación jerárquica, sino competencia determinada por la constitución. Tomo I. Materia constitucional. Jurisprudencia. Suprema Corte de Justicia de la Nación, p. 357. Tercera Sala, tesis 299.

dades federativas podrá conocer de los recursos de revisión que por su interés y trascendencia así lo ameriten". Además, este organismo estará facultado para conocer de los recursos que interpongan los particulares respecto de las resoluciones de los organismos especializados de los estados y de la ciudad de México que determinen la reserva, confidencialidad, inexistencia o negativa de la información. Dicho de otro modo, en ciertas hipótesis, el organismo garante federal actúa como autoridad de última instancia, sin perjuicio de que la competencia originaria corresponda a los organismos estatales o de la ciudad de México.

La autonomía constitucional que tiene los organismos garantes implica que carecen de una relación de pertenencia a los poderes tradicionales (Ejecutivo, Legislativo o Judicial) y que por ello son "órganos que ejercen diversas funciones públicas a partir de su propia identidad orgánica y de su propia legitimidad".[1470]

El artículo 37 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) explicita que la autonomía con la que cuentan estos organismos se traduce en su carácter técnico, de gestión, su capacidad de decisión sobre el ejercicio de recursos y su autodeterminación respecto a su organización interna. Esto le dota de la capacidad de decidir en qué gastan el presupuesto y cuál es su estructura orgánica, las funciones y la integración de los organismos, así como sus mecanismos de selección, excusas, suplencias, entre otros.[1471] El artículo 40 del mismo ordenamiento complementa este concepto estableciendo que los organismos garantes tendrán la estructura necesaria para la gestión y el desempeño de sus atribuciones. Además, precisa que se les deberá otorgar un presupuesto adecuado y suficiente para el funcionamiento efectivo y cumplimiento de las leyes en la materia.

Esta autonomía se complementa con un conjunto de principios rectores que establece el artículo 6 constitucional[1472] y son independencia, imparcialidad, certeza, legalidad, eficacia, profesionalismo, transparencia y máxima publicidad. A continuación, haremos una breve explicación de cada uno de ellos.

El principio de independencia se define en el artículo 8, fracción VII, de la LGTAIP, como la capacidad de decidir sin supeditarse a interés, autoridad o persona alguna.

La imparcialidad consiste en el deber que tienen los comisionados y el resto del personal de los órganos de ser ajenos o extraños a intereses[1473] distintos al interés público. Para cumplir con esto, la ley establece, entre otras cosas, procedimientos para la selección de los comisionados y su necesaria especialización.[1474] Lo anterior se complementa con el principio de profesionalismo, definido en el artículo 8, fracción VIII, LGTAIP, que implica que los organismos deberán sujetar su actuación a conocimientos técnicos, teóricos y metodológicos que garanticen un desempeño eficiente y eficaz en el ejercicio de la función pública que tienen encomendada. Finalmente, también se relaciona con el principio de objetividad, es decir, que deben analizar cada caso concreto y resolverlo en todos los hechos, sin consideraciones y criterios personales.[1475]

1470 Roldan, J. (2016). "De la desconcentración administrativa a la autonomía" en María del Carmen Pardo y Guillermo Cejudo, *Trayectorias de reformas administrativas en México: legados y conexiones*. México. El Colegio de México, p. 456.

1471 Artículo 37 de la Ley General de Transparencia y Acceso a la Información Pública.

1472 Por referencia explícita, en el artículo 116, fracción VIII.

1473 Imparcialidad. Contenido del principio previsto en el artículo 17 constitucional. Amparo directo en revisión 944/2005. Distribuidora Malsa, S.A. de C.V. 13 de julio de 2005. Unanimidad de cuatro votos.

1474 Este principio se encuentra relacionado con el de profesionalismo.

1475 Artículo 8, fracción VII de la Ley General de Transparencia y Acceso a la Información Pública.

La certeza y la legalidad están relacionados dado que los organismos tienen la obligación de fundamentar y motivar todas sus acciones, incluyendo todas sus resoluciones en la materia, en normas aplicables y, con esto, les otorgará seguridad y certidumbre a los particulares de saber que actúan conforme a derecho.[1476] Lo anterior, con eficacia, es decir tutelando de manera efectiva el derecho a la información.[1477]

Todo tiene que hacerse de manera transparente y buscando la máxima publicidad, es decir, que la información sea pública, complete, oportuna y accesible, con algunas excepciones.

Con independencia del ámbito espacial de competencia, y de las diferencias que pueden tener en su modelo de organización interna, los organismos garantes de los estados y el organismo garante de la Federación comparten atribuciones y principios que los rigen en común.

Las competencias comunes que les asigna la LGTAIP y la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO) pueden clasificarse de manera genérica en las siguientes categorías: 1) garantizar y resolver las controversias en materia de acceso a la información y protección de datos personales en posesión de sujetos obligados; 2) interpretación, administración, aplicación y supervisión de la aplicación de las leyes de acceso a la información y las de protección de datos personales en posesión de sujetos obligados; 3) capacitación, promoción y difusión de los derechos de acceso a la información y protección de datos personales; 4) establecer políticas y acciones en materia de transparencia proactiva y datos abiertos; 5) promover y garantizar la igualdad sustantiva, en particular en materia de lenguas indígenas, personas con discapacidad y grupos vulnerables; 6) interponer acciones de inconstitucionalidad en contra de leyes que vulneren los derechos de acceso a información pública y protección de datos personales; 7) elaborar y publicar estudios en materia de acceso a la información y protección de datos personales; 8) generar indicadores y criterios para evaluar el desempeño de los responsables en materia de datos personales y 9) participación como integrantes del Sistema Nacional de Transparencia.

1476 Artículo 8 de la Ley General de Transparencia y Acceso a la Información Pública.

1477 Artículo 8, fracciones II, VI y IX de la Ley General de Transparencia y Acceso a la información Pública.

NOTAS

NOTAS

NOTAS

Persona física identificable

Isabel Davara Fernández de Marcos,[1478]
Gregorio Barco Vega y
Alexis Cervantes Padilla

Un dato se considera personal cuando es concerniente a una persona física identificada o identificable. En sentido contrario, cuando la persona física titular de los datos no puede ser identificable, no se considera información personal. Por lo tanto, el concepto de persona física identificable[1479] es trascendental para discernir la aplicación de la normatividad de datos personales, tanto en la normatividad de derecho público como en la de privado. En consecuencia, no basta la sola referencia a una persona o individuo que existe y que tiene capacidad jurídica, es decir, que tiene la cualidad de ser sujeto de derechos y obligaciones, [1480] sino que es menester que dicha información permita identificar a su titular.

El concepto "persona física identificable" aparece regulado por vez primera en la normatividad mexicana en el artículo 2 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP)[1481] que señala que se considera como persona física identificable a "toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información", aclarando a continuación, el mismo artículo 4 del RLFPDPPP que dicho concepto no se actualiza cuando se requieran plazos o actividades desproporcionadas para lograr identificar a la persona.

En el sector público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), si bien no incluye de forma específica el concepto "persona física identificable" en el apartado de sus definiciones, sí precisa, dentro de la definición de dato personal prevista en la fracción IX de su artículo 3 que "se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información".

1478 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

1479 En relación con este concepto, recomendamos también consultar la definición de "titular de los datos personales" que forma parte de este *Diccionario de Protección de Datos Personales*.

1480 *Vid*, tesis, 350119. Tercera Sala. Quinta época. *Semanario Judicial de la Federación*. Tomo LXXXI, p. 4865.

1481 Publicado el 21 de diciembre de 2011 en el *Diario Oficial de la Federación*.

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) en su artículo 2.1 reiteran que una persona física identificable es tal cuando su identidad pueda determinarse directa o indirectamente, siempre y cuando esto no requiera plazos o actividades desproporcionadas.

Como hemos visto, las normatividades y textos citados, al plantearse cuándo una persona física se considera identificable emplean conceptos jurídicos indeterminados que requieren para su concreción la contextualización pertinente, dejando asimismo bastante espacio para la interpretación de la determinación de los medios que permitan la identificación directa o indirecta de la persona.

Sin embargo, en el derecho comparado encontramos algunas precisiones conceptuales para allanar los supuestos en los que la información permite identificar, ya sea de forma directa o indirecta, a una determinada persona.

En España, el Reglamento de la Ley Orgánica de Protección de Datos,[1482] al emplear el término "persona física identificable" establece que se refiere a toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social.[1483]

El Reglamento General de Protección de Datos Personales (RGPD o GDPR por sus siglas en inglés) al definir el concepto "dato personal" aporta una notable claridad para determinar qué se entiende por persona física identificable:

a) En el apartado 1 de su artículo 4 indica que se considera que una persona física es identificable cuando su identidad puede determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

b) En su considerando 26 indica que deben considerarse todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos.

El Grupo de Trabajo del Artículo 29 (GT29 o WP29 por sus siglas en inglés) ha clarificado varios de estos extremos:[1484]

1. Considera que la persona física es "identificable" cuando, aunque no se le haya identificado todavía, sea posible hacerlo (que es el significado del sufijo "ble"). En la práctica señala que tal condición es suficiente para considerar que la información permite identificar a la persona, ya sea de forma directa o indirecta.

1482 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

1483 Artículo 5. Definiciones.
1. A los efectos previstos en este reglamento, se entenderá por: (…)
o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados. (…)

1484 Grupo de Trabajo del Artículo 29, WP 136. Dictamen 4/2007 sobre el concepto de datos personales, Adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

2. Señala, en relación con los medios, que la distinción radica especialmente en "los medios que puedan ser razonablemente utilizados" por el responsable del tratamiento o por cualquier otra persona para identificar al titular.
3. Resalta la importancia del concepto "identificador", al enfatizar que la identificación se logra normalmente a través de datos concretos que podemos llamar identificadores y que tienen una relación privilegiada y muy cercana con una determinada persona, como su altura, el color del cabello, la ropa, etc., o una cualidad de la persona que no puede percibirse inmediatamente, como su profesión, el cargo que ocupa, su nombre, etc.

En resumen, podemos señalar que:

1. la normatividad se aplica a la información concerniente no solo a una persona física identificada, sino a la que puede ser identificable;
2. la cualidad de identificable:
   a. significa que es posible identificar a la persona física, aunque aún no se haya hecho;
   b. es un concepto jurídico indeterminado;
   c. debe evaluarse de manera contextual;
   d. los medios para la identificación pueden ser directos o indirectos, y pueden ser implementados por el responsable del tratamiento o por cualquier otra persona;
   e. cualquier "identificador" o elemento propio de la persona que sirva en el propósito de la identificación debe tenerse en consideración, esto es, cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social que guarda una relación privilegiada y muy cercana con una determinada persona (como por ejemplo su altura, la ropa, la edad, el color de su piel, un nombre, un número de identificación, datos de localización, un identificador en línea, etc.);
   f. no debe requerir plazos o actividades desproporcionadas, teniendo en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, según la tecnología disponible y los avances tecnológicos, y
   g. en definitiva, se puede sostener que una persona física es identificable cuando se dispone de los medios adecuados que permiten determinar la identidad de la persona ya sea a partir de la información de la que dispone de forma directa o bien mediante la aplicación de técnicas o medios de carácter complementario que permiten distinguir a quien pertenecen los datos personales.

Plataforma Nacional de Transparencia

Jorge Islas López

El derecho de acceso a la información pública en México tuvo un nuevo momento cuando la Suprema Corte de Justicia de la Nación (SCJN) revirtió el precedente previo cuando resolvió el caso "Aguas Blancas", en el cual estableció como violación grave el hecho de haber ocultado información relativa al caso de manera reiterada y permanente. A partir de esta nueva interpretación se consideró que la garantía de acceso a la información se encuentra estrechamente vinculada con el respeto de la verdad objetiva de los hechos, de manera que tal derecho es "básico para el mejoramiento de la conciencia ciudadana que contribuirá a que está sea más enterada, lo cual es esencial para el progreso de nuestra sociedad".[1485]

1485 Tesis: P. LXXXIX/96. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo III, junio de 1996, p.513.

Desde ese momento, el derecho a la información pública se ha entendido como una garantía individual que permite a todo gobernado estar informado con la verdad objetiva de los hechos y actos que ejecuta el Estado. Es así que la información se considera un soporte, una base desde la cual los gobernados tienen la posibilidad de ejercer un control social respecto del funcionamiento institucional de los poderes públicos. Esta obligación impuesta a los funcionarios sirve como fundamento para un mejor sistema de pesos y contrapesos, que se traduce en la ejecución de rendición de cuentas. En este sentido, la "publicidad de los actos de gobierno y la transparencia de la administración pública"[1486] son ejes centrales del gobierno republicano. A razón de lo anterior, resulta fundamental contar con un instrumento procedimental que coadyuve al respeto, promoción, protección y garantía del derecho de acceso a la información en México. Este instrumento se ha logrado materializar por medio de la Plataforma Nacional de Transparencia y Acceso a la Información Pública (de aquí en adelante PNT, Plataforma Nacional o Plataforma).

De acuerdo con la exposición de motivos, la PNT es el repositorio electrónico que sirve de apoyo a los sujetos obligados para que pongan a disposición de cualquier persona la información derivada de las obligaciones de transparencia, de manera uniforme, sistematizada y ordenada.[1487] En el mismo sentido, la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) establece, en su artículo 49, que dicho medio es una plataforma electrónica desarrollada, administrada e implementada por los organismos garantes para que estos puedan cumplir con procedimientos, obligaciones y disposiciones señalados en la Ley General para los sujetos obligados y los organismos garantes.

La Plataforma Nacional es una herramienta electrónica que permite un ágil acceso a la información pública gubernamental y administrativa. Este instrumento funciona en coordinación con el Sistema Nacional de Transparencia, Acceso a la Información y Datos Personales (de aquí en adelante, Sistema Nacional o SNT) y facilita la manera de solicitar información al estar en formato electrónico disponible a través de internet. La PNT es sumamente innovadora, toda vez que incorpora nuevos recursos tecnológicos y una sistematización informática de los datos estipulados por ley. De esta manera, se materializa una buena política de transparencia que sienta las bases de lo que se conoce en otras regulaciones de derecho comparado como administración pública virtual.[1488]

1. Características y beneficios

Esta innovación normativa, institucional y tecnológica que está estipulada en la LGTAIP tiene la finalidad de revertir la falta de mecanismos que obstaculizaban una rendición de cuentas pronta, expedita y eficaz, con el fin de garantizar la protección jurídica de las libertades fundamentales de los gobernados y gobernantes. Es decir, la Plataforma Nacional funciona como el medio directo, material y jurídico para el cabal ejercicio del derecho al acceso a la información. De esta forma, el portal http://www.plataformadetransparencia.org.mx/ funciona como un instrumento tecnológico que al registrarse permite que cualquier persona pueda solicitar información sobre los más de ocho mil sujetos obliga-

1486 Tesis: P./J. 54/2008. *Semanario Judicial y su Gaceta*. Novena época. Tomo XXVII, junio de 2008, p. 743.

1487 "Exposición de motivos". Iniciativa con proyecto de decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública, 2014, México, pp. 19.

1488 Al hablar de administración pública virtual, la exposición de motivos hace referencia a un "gobierno (que) se organiza para que toda la información que genera exista en formatos digitales, lo cual permitiría un mejor almacenamiento y también una difusión y consulta más fácil para los propios funcionarios o bien para los gobernados que quieran acceder a ella". Ibídem, pp. 17

dos en todo el territorio nacional.[1489] En este rubro, la PNT permite una interacción ágil y sencilla para el conocimiento de información de interés general. La Plataforma Nacional hace uso de los medios de comunicación electrónicos y la digitalización para la incorporación de solicitudes de información que garanticen el acceso a la información vía remota de manera directa, sencilla, gratuita, así como el ejercicio de la transparencia como eje rector de la rendición de cuentas. La importancia de que la LGTAIP disponga un capítulo completo para la definición, delimitación y reglamentación de la PNT estriba en la producción de una propuesta digital que tenga cobertura nacional y que centralice de forma dinámica y novedosa la búsqueda y recopilación de información relevante.

La PNT nace de un mandato normativo establecido en la LGTAIP en su artículo 31, fracción VI, el cual dispone que el Sistema Nacional debe "establecer los lineamientos para la implementación de la Plataforma Nacional de Transparencia…". De esta forma, es una función primordial del Sistema Nacional crear, impulsar e implementar la normatividad para la Plataforma Nacional, misma que será vinculante para los organismos garantes en su interacción con el medio electrónico. Con ello se busca fortalecer el entramado institucional propuesto por el Sistema Nacional para proteger los derechos de transparencia, así como de acceso a la información y protección de datos personales. Mediante el presente modelo se pretende acercar el funcionamiento del SNT a todo peticionario de una manera ágil, sencilla y sin costo alguno, para que realicen solicitudes de información o consulten información pública y ser informados acerca de las cuestiones que consideren de especial interés.

Para asegurar el funcionamiento y puesta en marcha de la Plataforma, la Ley estipula que los organismos garantes tendrán la responsabilidad del desarrollo, administración e implementación de la misma.[1490] La obligación del Estado para garantizar el derecho de acceso a la información no solo involucra su autorrestricción de respeto, o de no interferencia, sino que involucra que se tomen las medidas necesarias para que las personas puedan ejercerlo plenamente. Esta obligación es también de carácter internacional, en cuanto a que todos los Estados que formen parte de la Convención Americana sobre Derechos Humanos (México ratificó en 1981 la Convención y aceptó la competencia en 1998) tienen el deber jurídico de adoptar disposiciones, ya sean legislativas o administrativas, encaminadas a que todas las personas puedan ejercer de la mejor manera sus derechos humanos.

La Plataforma Nacional, como señala la Dra. Jacqueline Peschard, tiene como una de sus bondades que "al colocar en un solo sitio de internet la información de todos los sujetos obligados le da cohesión e integralidad, sin embargo, el enorme volumen de información puede resultar poco funcional para la Plataforma".[1491] La transparencia en México solo se puede dar a través de incentivos y procedimientos institucionales que obren a favor de nuestro derecho a saber la verdad objetiva de la esfera pública. Sin embargo, una crítica importante hecha desde el derecho administrativo es que el exceso de información también puede ser una forma de obstaculizar la transparencia. Por eso, la Plataforma Nacional, si bien es de suma utilidad, debe cuidar, por medio del uso de cierta ingeniería institucional, que los ciudadanos pueden acceder a esta de una forma fácil, sin mayores obstáculos.

1489 Con este nuevo modelo constitucional y legal se elevó el número de sujetos obligados a más del doble, aumentando además el número de obligaciones de transparencia que deben cumplir.

1490 Artículo 49. Los organismos garantes desarrollarán, administrarán, implementarán y pondrán en funcionamiento la plataforma electrónica que permita cumplir con los procedimientos, obligaciones y disposiciones señaladas en la presente Ley para los sujetos obligados y organismos garantes, de conformidad con la normatividad que establezca el Sistema Nacional, atendiendo a las necesidades de accesibilidad de los usuarios.

1491 Islas, J. (coord.). (2016). Ley General de Transparencia y Acceso a la Información Pública, comentada. INAI. México, p. 186.

En un país como México, con desigualdades sociales y económicas transversales, el uso y aprovechamiento de la Plataforma lamentablemente está restringida a aquellos sectores de la sociedad que no cuentan con acceso a medios electrónicos.[1492] La realidad es que la Plataforma, aún y cuando tiene una natural generosidad para universalizar el derecho a saber, nació con algunas limitaciones inherentes a la situación económica del país. Al respecto, es de suma trascendencia proyectar medidas y políticas que contemplen la heterogeneidad y desigualdades de nuestro país. Buscando de esta forma que el acceso a la información sea un derecho del que todos los gobernados puedan ser partícipes.

2. Interpretación literal de la Ley

A. Integración

Al concentrar en un único sitio de internet todos los procedimientos que se llevan a cabo por los organismos garantes, ya sea por medio de consultas de información o solicitudes de información, así como de recursos de revisión, el legislador pensó necesario que la Plataforma se constituyera por al menos cuatro grandes subsistemas en materia de transparencia y acceso a la información. El artículo 50 de la Ley General establece que la Plataforma Nacional se integra por:

a) el sistema de solicitudes de acceso a la información;

b) el sistema de gestión de medios de impugnación;

c) el sistema de portales de obligaciones de transparencia, y

d) el sistema de comunicación entre organismos garantes y sujetos obligados.

De esta forma, la PNT logra integrar en un medio a cuatro subsistemas. A la luz de lo anterior, este medio electrónico, que permite un eficaz acceso a la información pública, tiene por objeto convertirse en una pieza central de la transparencia en México.

Si bien, es por medio del sistema de solicitudes que el derecho de acceso a la información se ejerce de forma directa, el sistema de gestión de medios de impugnación permite a los usuarios defender sus derechos. Por otro lado, el sistema de portales de obligaciones permite comparar la información entre los diferentes sujetos obligados. Asimismo, a diferencia de años previos, el Sistema de comunicación entre organismos garantes ha permitido que el público tenga mejores herramientas para observar la información pública, así como sus recursos de revisión. Estos subsistemas son de carácter nacional, lo que significa que la idea detrás de ellos es centralizar los procedimientos requeridos por ley para la concertación e integración de los datos comprendidos. La compilación de los subsistemas enunciados con antelación permite utilizar medidas uniformes que sienten las bases procedimentales e institucionales para la obtención de datos o información pública que pueda ser de interés general.

El objetivo de la Plataforma es para garantizar la consecución del fin último de la LGTAIP: asegurar la aplicación fáctica y procedimental del derecho a la transparencia,[1493] acceso a la

1492 De conformidad con lo observado por la OCDE, México cuenta con una cobertura de banda ancha fija de 48 líneas por cada 100 hogares y 13.3 líneas por cada 100 habitantes; mientras la cobertura de banda ancha fija promedio en los países de la OCDE es de 30.1 líneas por cada 100 habitantes.
Marco Internacional y recomendaciones de la banda ancha en el escenario mexicano: Disponible en: http://www.ift.org.mx/sites/default/files/industria/temasrelevantes/11337/documentos/marcoreferenciabandaancha23nov17.pdf

1493 En referencia a los sujetos obligados que asignan recursos públicos a los distintos sindicatos, estos también tienen el deber de habilitar un espacio en sus páginas de internet para así cumplir con sus obligaciones de transparencias, lo cual involucra que tengan la infraestructura tecnológica necesaria para el uso y acceso a la Plataforma Nacional.

información y protección de datos personales. En consecuencia, esta herramienta técnica permite integrar las normas y el desarrollo de las tareas institucionales de acceso a la información y protección de datos personales como una acción que garantiza el derecho humano a saber de la cosa pública.

La transición hacia una sociedad más informada es una práctica que los organismos garantes de transparencia deben fomentar (LGTAIP, art. 51), por lo que se considera una obligación fundamental en una democracia. No hay duda que la transparencia y el acceso a la información son rubros que forman parte de la agenda de cambio institucional que propició parte de nuestra transición a la democracia vertical, el espacio en donde se ejerce el poder público, el llamado cuarto de máquinas en donde los engranajes institucionales funcionan de tal forma que garantizan este derecho. En este sentido, la Corte Interamericana de Derechos Humanos (CIDH) ha reiterado que estas materias son una parte esencial de toda democracia. De esta forma se pronunció en diferentes casos al resaltar que "en una sociedad democrática es indispensable que las autoridades estatales se rijan por el principio de máxima divulgación, el cual establece la presunción de que toda información es accesible, sujeto a un sistema restringido de excepciones" y que estas se encuentren "orientadas a satisfacer un interés público imperativo".[1494] De esta manera, con el establecimiento de la Plataforma Nacional se cumple satisfactoriamente con el mandato constitucional establecido en su artículo sexto.

B. Procedimientos y solicitudes

Los procedimientos de acceso a la información pública se materializan través de la Plataforma Nacional al ampliar por medio de la LGTAIP, artículo 122, las diferentes formas en las que las personas pueden presentar una solicitud para acceder a la información que desean. En este sentido, en un principio se determinó que cualquier persona por sí misma o a través de su representante puede generar una solicitud de acceso a la información pública.

Asimismo, la Ley estableció que esta solicitud debe realizarse ante la unidad de transparencia, ya sea a través de la Plataforma Nacional, en las oficinas designadas para ello, por vía correo electrónico, correo postal, mensajería, telégrafo y verbalmente. Es de resaltar la cláusula abierta que el legislador decidió establecer en este artículo, ya que ante el hecho contingente de que surgieran otros medios en el futuro, decidió otorgarle la facultad al Sistema Nacional para la aprobación de cualquier otro medio que estime necesario para ejercer este derecho. El legislador puso especial atención al procedimiento de acceso a la información, ya que este es un elemento imprescindible para que los ciudadanos ejerzan sin obstáculos su debido derecho.

En la exposición de motivos resalta que uno de los aspectos novedosos del procedimiento de acceso a la información es que "se amplía la forma de solicitar información, pues anteriormente no se contemplaba la forma verbal, ni la vía telefónica".[1495] Asimismo, es de reconocerse el hecho de que todo el proceso de solicitud de información es gratuito, lo cual garantiza el acceso universal de todas las personas. Sin embargo, las condiciones fácticas no siempre son favorables a lo anterior, por lo que también existen los meca-

1494 Criterio recogido en diversos pronunciamientos de la Corte Interamericana de Derechos Humanos, como son los casos "Herrera Ulloa vs. Costa Rica", 2004, párrafos 121 y 122; "Ricardo Canese vs. Paraguay", 2004, párrafo 96; "Palamara Iribarne vs. Chile", 2005, párrafo 85; y la opinión consultiva OC-5/85, la colegiación obligatoria de periodistas, 1985, párrafo 45. Los presentes criterios serán analizados con mayor profundidad cuando se haga referencia a jurisprudencia y convencionalidad aplicable a la materia.

1495 "Exposición de motivos". Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. 2014. México, p. 36.

nismos que regulan en qué momento y bajo qué circunstancias se cobrará una cuota de recuperación por entregar la información que se solicite.

El derecho de acceso a la información, como todo derecho humano, universal e inherente por naturaleza, se ejerce en igualdad de condiciones para todas las personas. Por ello, su ejercicio no debe estar restringido más que por las causas que la misma ley prevé, las cuales deben ser objetivas y estar encaminadas a la preservación del interés público superior, o la salvaguarda nacional, tal como señala la Constitución, la LGTAIP en su artículo 113 y los tratados internacionales aplicables. Por lo anterior, en el caso de que una solicitud de información ponga en peligro los intereses establecidos en la Ley General, la Plataforma Nacional podrá establecer estas razones para justificar la reserva de la información.

En referencia a las solicitudes de información formuladas ante la Plataforma Nacional, se les asigna de forma automática un número de folio por medio del cual los solicitantes pueden dar seguimiento a sus requerimientos (LGTAIP, artículo 123). De esta manera, se garantiza la sistematización de las solicitudes de acceso a la información. En los demás casos, la unidad de transparencia es la encargada de registrar y capturar la solicitud de acceso en la Plataforma Nacional y es la que debe enviar el acuse de recibo al solicitante, el cual debe tener la fecha de recepción, el folio correspondiente y los plazos de respuesta aplicables. En este rubro, la LGTAIP sigue lo establecido en el párrafo 21 de la Ley Modelo Interamericana sobre Acceso a la Información Pública, la cual establece que "salvo que la información pueda ser entregada de manera inmediata, toda solicitud de información deberá ser registrada y se le deberá asignar un número para su debido seguimiento, el cual deberá ser proporcionado al solicitante junto con la información de contacto del oficial de información encargado de procesar la solicitud".[1496]

3. Jurisprudencia y convencionalidad

En razón de la novedad que supone la Plataforma Nacional, el Poder Judicial de la Federación no ha emitido, por el momento, criterio alguno respecto al funcionamiento que deba tener la misma. Sin embargo, es posible remitirse a la CIDH, la cual en diferentes casos ha sostenido criterios que precisan que en una sociedad democrática toda información debe ser accesible y sujeta a escrutinio público.[1497]

La CIDH, a su vez, considera que el Estado debe realizar, en un plazo razonable, la capacitación a los órganos, autoridades y agentes públicos encargados de atender las solicitudes de acceso a información bajo control del Estado sobre la normativa que rige este derecho, que incorpore los parámetros convencionales que deben respetarse en materia de restricciones al acceso a dicha información.[1498] En el mismo sentido, en el caso "Gomes Lund y otros (Guerrilha do Araguaia) vs. Brasil"[1499] se destaca la obligación del Estado de garantizar la efectividad de un procedimiento adecuado para la tramitación y resolución de las solicitudes de información, de tal forma que se fijen los plazos para resolver y entregar la información, y que se encuentre bajo la responsabilidad de los funcionarios debidamente capacitados.

1496 Ley Modelo Interamericana sobre Acceso a la Información. 2010. Disponible en: https://www.oas.org/dil/esp/CP-CAJP-2840-10_Corr1_esp.pdf

1497 Corte IDH. "Claude Reyes y otros vs. Chile". Fondo, reparaciones y costas. Sentencia de 19 de septiembre de 2006. Serie C, No., 151, párr. 92; Corte IDH. "Gomes Lund y otros (Guerrilha do Araguaia) vs. Brasil". Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 24 de noviembre de 2010. Serie C, No. 219, párrafo 197

1498 Corte IDH. "Caso Claude Reyes y otros vs. Chile". Fondo, reparaciones y costas. Sentencia de 19 de septiembre de 2006. Serie C No. 151, párrafo 165, Chile.

1499 Corte IDH. "Caso Gomes Lund y otros (Guerrilha do Araguaia) vs. Brasil". Excepciones preliminares. Fondo, reparaciones y costas. Sentencia de 24 de noviembre de 2010. Serie C No.219, párrafo 231.

Por lo anteriormente expuesto, para considerar si la Plataforma Nacional ha logrado cumplir con los criterios expuestos en la jurisprudencia interamericana es necesario expresar algunas conclusiones del Diagnóstico del Programa Nacional de Transparencia y Acceso a la Información, 2017-2021.[1500] Esta reflexión es importante para identificar los retos institucionales que deben ser atendidos en el futuro. Es por ello que una de las conclusiones más importantes de dicho informe tiene que ver con los inicios del proyecto de la Plataforma Nacional se tuvieron retos significativos para la integración, interconexión, y desarrollo de soluciones informáticas en algunas entidades federativas. Asimismo, se identificaron sujetos obligados que no contaron con el sistema Infomex,[1501] ni refirieron la Plataforma Nacional, en cambio indicaron que tenían otro tipo de sistema informático para la atención de solicitudes.

4. Derecho comparado

Respecto a cómo se han incorporado los medios electrónicos en la promoción y garantía del derecho a la información en otros países, han sido una referencia ejemplar las buenas prácticas que organismos internacionales han observado en la materia. El Banco Mundial, mediante su investigación en los medios electrónicos y transparencia titulada *Open Government Impact y Outcomes, Mapping the Landscape of Ongoing Research,* encontró que en los países en vías de desarrollo, en los cuales la desigualdad es considerable en términos reales, no existen sondeos y estudios de investigación que determinen el impacto que tienen fácticamente la normatividad y políticas públicas respecto al acceso a la información. "De esta forma, (una de las principales) implicaciones es el desarrollo de herramientas tecnológicas insuficientes y desarticuladas en la práctica".[1502] Derivado de lo anterior, el Banco Mundial estipula y recomienda la creación de evaluaciones y estimaciones a nivel nacional, que analicen el impacto fáctico de las plataformas y las políticas públicas en la materia. Se aconseja al respecto "que se realicen investigaciones que tengan una relevancia de política pública clara, a través de un enfoque más impulsado por la demanda, es decir, que permita emparejar el resultado esperado por los gobiernos y por la población en general que quiere ejercer su derecho".[1503]

Asimismo, diversos países han desarrollado sistemas y medios digitales análogos a la Plataforma Nacional. Uno de los sistemas más completos y complejos es el europeo. Según el artículo 15 del Tratado de Funcionamiento de la Unión Europea, "los ciudadanos y residentes de los países de la UE tienen derecho de acceso a los documentos del Parlamento Europeo, el Consejo y la Comisión Europea. Esto significa que los ciudadanos pueden obtener documentos en poder de la Comisión y otras instituciones, incluida información legislativa, documentos oficiales, archivos históricos y actas y agendas de reuniones". Todo ello se ve reflejado en el Registro de Documentos de la Comisión Europea, donde se encuentran sistematizados documentos legislativos, documentos elaborados por la Comisión y datos de interés general. Asimismo, se pueden realizar solicitudes de información que no se encuentre publicada al momento de la consulta, todo lo anterior por vía electrónica.

1500 Sistema nacional de Transparencia, Acceso a la información y Protección de Datos Personales. Diagnóstico del Programa Nacional de Transparencia y Acceso a la Información (Protai), 2017-2021, pp. 89-106. Disponible en: http://snt.org.mx/images/Doctos/170613_Documento_diagnostico_PROTAI_combinado.pdf

1501 El sistema de solicitudes de información anterior a la Plataforma Nacional.

1502 Diagnóstico del 2017-2021. Recuperado de: http://snt.org.mx/images/Doctos/170613_Documento_diagnostico_PROTAI_combinado.pdf, p. 90.

1503 Diagnóstico del PROTA, 2017-2021, p. 91.

5.Conclusión

La Plataforma Nacional de Transparencia es la expresión material del cumplimiento de las obligaciones de transparencia establecidos en la Constitución y en la LGTAIP. El modelo electrónico propuesto permite que los ciudadanos se conviertan en verdaderos guardianes de la democracia por medio de un escrutinio asiduo y permanente de los recursos y de las decisiones públicas. Con la misma idea se expresó Federico Reyes Heroles cuando dijo, en referencia a los países que no tienen una legislación sobre la transparencia y su relación negativa con la corrupción: "Allí donde existe una ley de acceso a la información pública la corrupción no campea a sus anchas. Se trata sin duda de una de las medidas más eficaces para combatir la corrupción".[1504] Por ello, la Ley General si bien es un instrumento que por sí mismo establece ciertos derechos, lo importante es su instrumentalización objetiva, es decir necesita un medio por el cual se hagan valer y se garanticen estos derechos. La Plataforma Nacional es la respuesta que por el momento ha resuelto el problema de la universalización del derecho a saber.

Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Pedro Salazar Ugarte y
Jesús Eulises González

Es el órgano colegiado de máxima decisión del organismo garante y en el que residen originariamente las facultades y atribuciones para promover, respetar, proteger y garantizar los derechos de acceso a la información pública y protección de datos personales respecto de los sujetos obligados y, en sus modalidades, de los particulares.

1. Ubicación dentro de las garantías institucionales de los derechos

De acuerdo con la teoría de Luigi Ferrajoli, los derechos fundamentales requieren de los mecanismos normativos, procedimentales e institucionales para hacerse efectivos y tener los elementos necesarios para su garantía.[1505] En este contexto, el sistema jurídico mexicano cuenta con los elementos necesarios para que los derechos de acceso a la información y protección de datos se encuentran debidamente garantizados.

Lo anterior se materializa en la existencia de la garantía primaria, al encontrarse reconocidos los derechos en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en tratados internacionales y desarrollados a detalle los alcances y límites de estos derechos en multiplicidad de leyes, reglamentos y demás normas especializadas. De la misma manera, ambos derechos cuentan con las garantías secundarias procedimentales e institucionales para hacerlos efectivos. El constituyente primero, y después el legislador, diseñaron los procedimientos para la presentación de solicitudes de información, el ejercicio de derechos de acceso, rectificación, cancelación y oposición (ARCO), las denuncias ante violaciones y los correspondientes recursos de revisión. Todas estas son garantías segundarias de los derechos en cuestión. Además, se cuenta con otros mecanismos de protección constitucional como el juicio de amparo.

1504 Reyes, H.F. (2010). *Corrupción: de los ángeles a los índices*. Cuaderno de transparencia 01. México IFAI.

1505 Ferrajoli, L. (2009). "Los fundamentos de los derechos fundamentales", en De Cabo, Antonio y Pisarello, Gerardo (editores). *Los fundamentos de los derechos fundamentales*. Cuarta edición. Madrid. Trotta.

De hecho, si nos atenemos al esquema de garantías institucionales, los derechos de acceso a la información (DAI) y protección de datos personales (DPDP) son de los más desarrollados en el sistema normativo nacional. Para los DAI, la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) delinea el sistema nacional de protección. De ésta se desprenden 33 leyes, 32 de las entidades federativas y otra más correspondiente a la Federación.

Por lo que hace al DPDP, existen dos regímenes de protección, uno para el sector privado y otro para el sector público. El sector privado se encuentra regulado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), su Reglamento (LFPDPPP) y lineamientos especializados en materias como la autorregulación, aviso de privacidad, etc. Por lo que hace al sector público, la norma general es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), al igual que la LGTAIP, de la que se desprenden 32 leyes locales y una más de carácter federal.

Como autoridades encargadas de la protección de los derechos se designó a los organismos garantes, que son el Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales (INAI), así como 32 organismos garantes locales para los ámbitos de los estados y la Ciudad de México.

Conforme al texto constitucional, el INAI es el "organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley".[1506] Como podemos, ver se trata de un organismo con plena autonomía constitucional que tiene el objetivo de garantizar el cumplimiento del DAI y el DPDP. La norma fundamental lo determina como un ente colegiado, es decir que será constituido por más de una persona, en las que recaen sus facultades y atribuciones. La misión de garantizar los derechos es destinada a los integrantes (comisionados) del organismo garante federal y en su actuación colectiva conforman el Pleno que nos ocupa en esta voz.

La Ley Federal de Transparencia y Acceso a la Información Pública define al Pleno como "la instancia del INAI en la que los comisionados del mismo ejercen de manera colegiada las facultades conferidas a ellos en términos de la presente Ley y demás disposiciones constitucionales y legales aplicables".[1507] Por su parte, el estatuto orgánico del INAI[1508] plantea que el Pleno es "el órgano máximo de dirección y decisión del Instituto, integrado por los siete comisionados con voz y voto, incluido su presidente".[1509]

2. Integración

El texto constitucional desarrolla las bases y principios de los derechos de acceso a la información y protección de datos personales únicamente en los elementos básicos de la garantía de éstos. Junto a los mecanismos para hacer efectivos estos derechos, el artículo 6 constitucional estableció que el organismo garante federal debe ser integrado por siete comisionados.

1506 CPEUM, articulo 6, apartado A, fracción VIII.

1507 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 4, fracción VIII.

1508 Acuerdo mediante el cual se aprueba el estatuto orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado en el *Diario Oficial de la Federación* el 17 de enero de 2017.

1509 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 3, fracción XII.

Para ser elegible como comisionado del organismo garante federal se requiere cumplir con los siguientes requisitos:

- ser ciudadano mexicano por nacimiento, en pleno ejercicio de sus derechos políticos y civiles;
- tener cuando menos 35 años cumplidos el día de la designación;
- gozar de buena reputación y no haber sido condenado por delito que amerite pena corporal de más de un año de prisión; pero si se tratare de robo, fraude, falsificación, abuso de confianza y otro que lastime seriamente la buena fama en el concepto público, inhabilitará para el cargo, cualquiera que haya sido la pena;
- haber residido en el país durante los dos años anteriores al día de la designación, y
- no haber sido secretario de Estado, fiscal general de la República, senador, diputado federal, ni titular del poder ejecutivo de alguna entidad federativa, durante el año previo al día de su nombramiento.[1510]

Para la formalización del procedimiento de integración del Pleno del INAI se facultó al Senado de la República para realizar la designación, mientras que al Ejecutivo Federal se le otorgó la facultad para objetar la decisión. El procedimiento, además, permite la participación de la sociedad civil en la selección de los aspirantes a ser integrantes del organismo garante.

El mecanismo para la selección de los comisionados tiene como primer paso "una amplia consulta en la sociedad". De hecho, en nombramientos recientes, el Senado de la República emitió una convocatoria para la recepción de candidaturas a universidades públicas y privadas; institutos de investigación, asociaciones y organizaciones no gubernamentales, así como a la ciudadanía en general.

El segundo paso es la aprobación de la Cámara de Senadores. Hasta ahora la recepción de candidaturas está a cargo de la Junta de Coordinación Política (en adelante Jucopo). Esta instancia, posteriormente, informa de las candidaturas a las comisiones de Anticorrupción y Participación Ciudadana; y de Justicia del Senado de la República. Estas comisiones parlamentarias tienen a su cargo la evaluación de las candidaturas para emitir un listado de elegibles. Para llegar a este listado las comisiones mencionadas analizan los documentos seleccionados y convocan a comparecencias públicas a los candidatos. Posteriormente, la lista de elegibles regresa a la Jucopo para que se haga la selección de los candidatos que se someterán al Pleno del Senado.[1511]

Vale la pena hacer una reflexión sobre la distribución interna de atribuciones del órgano garante. Si bien el Pleno es la máxima autoridad dentro del Instituto, las titularidades de las facultades para ejecutar las decisiones de este órgano son delegadas al comisionado presidente, quien —con el auxilio de las áreas operativas— lleva a cabo las acciones destinadas para cumplimentar las decisiones plenarias. Al comisionado presidente le corresponde la representación legal del organismo garante y constituye el eje de coordinación y dirección institucional.[1512]

1510 El artículo 6 constitucional refiere a los requisitos de elegibilidad para ser designado como ministro o ministra de la Suprema Corte de Justicia de la Nación. Se exime de la fracción III del artículo 95 constitucional que hace referencia al título de licenciado en derecho con antigüedad mínima de 10 años.

1511 Es importante advertir que este procedimiento podría variar si así lo decide el Senado de la República porque se encuentra contemplado en una convocatoria con vigencia acotada al proceso de que se trate.

1512 Acuerdo mediante el cual se aprueba el Estatuto Orgánico..., cit., artículo 3, fracción III.

Los siete comisionados eligen de entre sus integrantes al comisionado presidente. Para el procedimiento de elección es suficiente colmar la mayoría simple y el periodo de duración del encargo es de tres años. El comisionado presidente, al mismo tiempo de fungir como ponente de asuntos y proyectos, tiene a cargo un conjunto de facultades de elección a través de las secretarías y direcciones generales del Instituto para llevar a cabo la ejecución de las decisiones plenarias y cumplir con las funciones que, por su naturaleza, corresponden a una instancia de decisión unipersonal.[1513]

3. Análisis a partir de las facultades y funciones del pleno del INAI

La naturaleza de un organismo constitucional autónomo (OCA) es entendible a través de sus características. Estos organismos son entidades establecidas directa e inmediatamente en la Constitución, tienen una función especializada, participan directamente en la dirección política del Estado (a través de la emisión de actos ejecutivos, legislativos o jurisdiccionales), mantienen una paridad en el máximo rango con los poderes tradicionales y otros OCA y son plenamente autónomos en su administración.[1514]

Las primeras de estas características han quedado asentadas en el apartado anterior porque sabemos que el INAI y su Pleno se encuentran establecidos directamente en la CPEUM y tiene como objetivo garantizar el cumplimiento del DAI y el DPDP en el ámbito nacional. Para entender las otras características conviene analizar de manera sucinta las principales facultades y atribuciones del Pleno del INAI.

La función de este cuerpo colegiado se encuentra desarrollada a profundidad en el estatuto[1515] que recoge y desarrolla las facultades que la norma constitucional y las normas secundarias establecen para su organización. Al momento de escribir esta voz, la figura del Pleno se encuentra desarrollada en el capítulo segundo, en los artículos 6 al 12 del estatuto antes mencionado.

3.1. Como instancia de decisión jurisdiccional

Quizá la función más conocida del INAI es la sustanciación de las inconformidades de los particulares frente a las respuestas de los sujetos obligados, ya sean estas de acceso a la información o para el ejercicio de los llamados derechos ARCO. Lo cierto es que la función jurisdiccional del INAI, en los denominados recursos de revisión, es sustancial y ocupa el grueso de las órdenes del día de las sesiones plenarias.[1516] Sin embargo, las actividades jurisdiccionales de este órgano son más amplias.

La actividad jurisdiccional ha sido comentada y definida por el Poder Judicial de la Federación. Una reciente interpretación jurisprudencial ayuda a dimensionarlas en autoridades que se encuentran fuera de los poderes judiciales: "Si bien son autoridades formalmente administrativas […], entre sus funciones se encuentran las de conocer, calificar y sancionar las infracciones a dichos ordenamientos; supuestos en los que se erigen como autoridades materialmente jurisdiccionales, pues dilucidan una cuestión de derecho, al

1513 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículos 30 y 31 y Acuerdo mediante el cual se aprueba el estatuto orgánico artículos 13, 15 y 16. del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicado en el *Diario Oficial de la Federación* el 17 de enero de 2017.

1514 Salazar, P. (2017). *El Poder Ejecutivo en la Constitución mexicana. Del metaconstitucionalismo a la constelación de autonomías.* México. Fondo de Cultura Económica, pp. 106 y 107.

1515 Cfr. Acuerdo mediante el cual se aprueba el estatuto orgánico…, cit.

1516 En el último Informe de labores presentado al Congreso de la Unión, el INAI reportó haber resuelto más de 8 mil recursos en estas materias. Cfr. INAI. (2017). *Informe de Labores 2017*. Disponible en: http://inicio.ifai.org.mx/Publicaciones/Informelabores2017.pdf.

imponer sanciones a través del procedimiento previsto en dichos ordenamientos en ejercicio de una función pública, con un carácter supra partes, con imparcialidad, autonomía y aplicando las normas contenidas en los referidos ordenamientos administrativos para determinar si existió su incumplimiento por los particulares".[1517]

Lo anterior no se reduce al poder sancionador, sino que alcanza la capacidad de resolver controversias: "Ese tercero (la autoridad no jurisdiccional) se convierte en rector del procedimiento y juez de esa controversia específica, por lo que realiza una actividad materialmente jurisdiccional y, en ese tenor, el laudo que dicta también es un acto materialmente jurisdiccional, lo que de suyo equipara a dicha autoridad arbitral a una jurisdiccional".[1518]

En este sentido, el INAI se configura como una institución que cuenta con facultades materialmente jurisdiccionales. De hecho, es el Pleno la autoridad dentro del organismo garante que delibera, discute y vota las resoluciones que ponen fin a los siguientes procedimientos: recurso de revisión en materia de acceso a la información,[1519] recurso de revisión en materia de protección de datos personales,[1520] recurso de inconformidad (en este supuesto el INAI actúa como segunda instancia frente a las resoluciones de los organismos garantes de las entidades federativas),[1521] los recursos de revisión atraídos de los organismos garantes de las entidades federativas.[1522]

Cabe advertir que también en el ámbito del sector público, pero con la finalidad de investigar e imponer sanciones, el Pleno resuelve los siguientes procedimientos: procedimiento de verificación de las obligaciones de transparencia, procedimiento de denuncia por incumplimiento a las obligaciones de transparencia y el procedimiento sancionatorio previsto en el título sexto, capítulo III de la Ley Federal.

En el ámbito del sector privado y en materia de protección de datos personales, el Pleno resuelve los procedimientos de protección de derechos,[1523] de imposición de sanciones[1524] y de verificación.[1525] Todos estos se encuentran desarrollados en la LFPDPPP y el RLFPDPPP.

3.2. Como instancia legislativa y ejecutiva

Para lograr el fin encomendado por la Constitución, el Pleno del INAI tiene asignadas facultades para la emisión de normas generales y para la ejecución de leyes a través de actos de naturaleza administrativa.

En efecto, el diseño constitucional de protección del DAI y el DPDP en nuestro país asigna al organismo garante facultades ejecutivas que hasta 2014 correspondían a un ente desconcentrado de la administración pública federal. Al INAI también le fueron otorgadas

1517 Tesis PC.VI.A. J/10 A (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo II, enero de 2018, p. 1036.

1518 Tesis I.11o.C.26 K (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo IV, marzo de 2018, p. 3479.

1519 Cfr. Ley General de Transparencia y Acceso a la Información Pública, articulo 41, fracción II, y Ley Federal de Transparencia y Acceso a la Información Pública, artículo 21, fracción II.

1520 Cfr. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 103.

1521 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 21 fracción III.

1522 Cfr. Acuerdo mediante el cual se aprueban los nuevos Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción, articulo 19. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5472060&fecha=16/02/2017.

1523 Cfr. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículo 45 y Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículos 122 y 125.

1524 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 59 y Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículo 143.

1525 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 61, y Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículo 137.

facultades para la creación de normas reglamentarias especializadas, así como para ejecución de programas y políticas públicas para la garantía del DAI y el DPDP.

En este sentido, el INAI puede emitir lineamientos, criterios, códigos de buenas prácticas que determinan cómo se dará cumplimiento a las leyes a su cargo. Un ejemplo son las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales, cuyo objetivo es ponderar los impactos que puede tener un tratamiento de datos personales para identificar y mitigar riesgos en la materia.

La ejecución de las decisiones plenarias, como habíamos señalado, corresponde al comisionado presidente y a la estructura administrativa que depende del mismo, en los términos del estatuto.[1526]

3.3. Como un organismo dotado de autonomía plena

La principal característica de los OCA es el amplio rango de autonomía que se les otorga frente a los poderes tradicionales. En este sentido, se constituyen como elementos sustanciales aquellas atribuciones que desarrollan este ámbito. De este conjunto de facultades destacan las atribuciones legislativas internas, de gestión y presupuestarias.

La autonomía implica la facultad un sujeto de emitir las normas que lo rigen. En este sentido el Pleno del INAI puede establecer las normas y estructura administrativa interna mediante la adopción del estatuto[1527] y elegir a los servidores públicos que conforman a la organización.[1528] No debemos olvidar que todos los otros actores estatales se encuentran sujetos a las leyes que desarrollan los DAI y los DPD y estas facultades buscan que ninguna otra institución estatal interfiera en la misión del INAI imponiendo reglas o personas que menoscaben la protección de los derechos a garantizar.

Además, se facultó al INAI para decidir sobre sus planes de trabajo, las propuestas de políticas y programas de trabajo y proyectos especiales.[1529]

Otros conjuntos de atribuciones relevantes son aquellos que se refieren al presupuesto y su gestión. La autonomía requiere capacidad de decisión y gestión de los recursos institucionales. En esta materia destacan las facultades para realizar la propuesta de presupuesto anual, establecer los mecanismos de racionalidad, austeridad y disciplina en materia presupuestaria y para ejercer, sin intermediarios, los recursos que le son asignados.[1530]

3.4. Como un actor en procedimientos de justicia constitucional

El último conjunto de facultades otorgadas al organismo garante y ejercidas por el Pleno se refieren a su capacidad para iniciar controversias constitucionales y acciones de inconstitucionalidad en los términos del artículo 105 de la Constitución Federal.

1526 Ley Federal de Transparencia y Acceso a la Información Pública., artículo 31, fracción VI y acuerdo mediante el cual se aprueba el estatuto orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, artículo 16, publicado en el *Diario Oficial de la Federación* el 17 de enero de 2017. En este punto no se observan a detalle las facultades de cada una de las unidades administrativa, lo anterior representa un ejercicio mucho más amplio que el requerido para una voz de diccionario.

1527 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 35, fracciones I y XV.

1528 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 35, fracción II y III.

1529 Cfr. Acuerdo mediante el cual se aprueba el estatuto orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, artículo 12, fracción XXIII.

1530 Cfr. Acuerdo mediante el cual se aprueba el estatuto orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, artículo 12, fracciones XIV y XV, y Ley Federal de Transparencia, artículo 31, fracción XI.

Para ejercer estas potestades, se autorizó al Pleno la posibilidad para someterlo a discusión y votación.[1531] Si un proyecto es respaldado por la mayoría, éste se turna a las instancias internas que presentarán las acciones correspondientes ante la Suprema Corte de Justicia de la Nación.

Prestador de servicios de certificación

Jonathan Gabriel Garzón Galván

Con el nacimiento de las firmas electrónicas avanzadas en las que se utiliza el cifrado asimétrico, se creó la figura de las entidades certificadoras o prestadores de servicios de certificación, quienes aportan los sistemas de cómputo e infraestructura tecnológica necesaria para brindar certeza al manejo de las llaves o claves utilizadas en ese método de firma. En la legislación encontramos las siguientes definiciones:

a) Artículo 2 de Ley Modelo de la CNUDMI sobre las firmas electrónicas (2001).[1532] Se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas.

b) Artículo 89 del Código de Comercio.[1533] La persona o institución pública que preste servicios relacionados con firmas electrónicas expide los certificados o presta servicios relacionados como la conservación de mensajes de datos, el sellado digital de tiempo y la digitalización de documentos impresos, en los términos que se establezca en la norma oficial mexicana sobre digitalización y conservación de mensajes de datos que para tal efecto emita la Secretaría de Economía.

c) Artículo 2 de la Ley de Firma Electrónica Avanzada.[1534] Las instituciones públicas conforme a las leyes que les son aplicables, así como los notarios y corredores públicos y las personas morales de carácter privado que de acuerdo con lo establecido en el Código de Comercio sean reconocidas con tal carácter para prestar servicios relacionados con la firma electrónica avanzada y, en su caso, expedir certificados digitales.

Como se mencionó previamente, la vinculación entre las claves públicas y privadas utilizadas en el cifrado asimétrico de la firma electrónica avanzada se realiza bajo un esquema de confianza, donde la llave pública es validada e introducida en un certificado digital,[1535] este proceso es llevado a cabo por entidades responsables de mantener un proceso confiable de acreditación de la identidad de los solicitantes, y el mantenimiento de una in-

1531 Cfr. Ley Federal de Transparencia y Acceso a la Información Pública, artículo 35, fracción VIII.

1532 Ley Modelo de la CNUDMI sobre firmas electrónicas y su guía para su incorporación al derecho interno, disponible en: http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf, fue examinada y dictaminada durante la sesión 38 ° del Grupo IV de Trabajo, celebrada del 12 al 23 de marzo de 2001; teniendo como objetivos permitir o facilitar el empleo, entendimiento y marco regulatorio armonizado y equitativo de firmas electrónicas.

1533 El 13 de junio de 2003, se publicó en el *Diario Oficial de la Federación* (DOF), la reforma al Código de Comercio que adiciona el título tercero, al que denomina "Del Comercio Electrónico", con el que se otorga facultades a la Secretaría de Economía para acreditar a las personas físicas y jurídicas que deseen ofrecer servicios de firma electrónica de uso exclusivo para la materia mercantil. Código de Comercio, última reforma DOF 28/03/2018. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf /3_280318.pdf

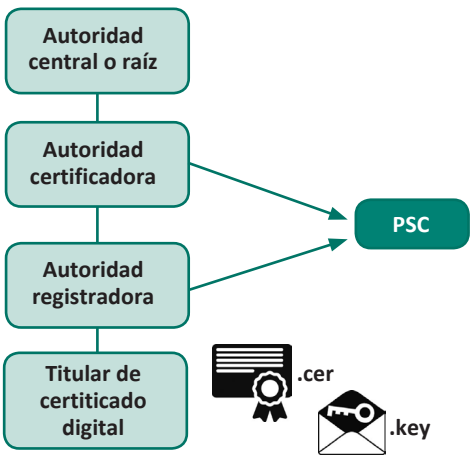
1534 Ley Federal de Firma Electrónica Avanzada, última reforma DOF 11/01/2012. Disponible en: http://www. diputados.gob.mx/LeyesBiblio/pdf/LFEA.pdf

1535 Un certificado digital es definido por la regulación como todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de firma electrónica, artículo 89 de Código de Comercio, última reforma DOF 28/03/2018. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf /3_280318.pdf, y artículo 2 de la Ley Modelo de la CNUDMI sobre firmas electrónicas y su guía para su incorporación al derecho interno. Disponible en: http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf.

fraestructura de clave pública[1536] (mejor conocida como PKI por sus siglas en inglés *Public Key Infraestructure*).

Julio Téllez precisa que "sacar a la luz una clave y asociarla a un nombre es un ejercicio sencillo, pero ¿Cómo puede hacerse para demostrar dicha relación? La práctica actual invita a introducir la clave pública de un individuo en un certificado digital junto con información relativa a la clave (por ejemplo, la fecha de vencimiento) y al propietario de dicha clave (nombre, etc.,). Luego, una tercera parte de confianza firma este certificado, lo que significa que aprueba la reivindicación de identidad implícita en el certificado".[1537]

Estos terceros de confianza son comúnmente llamados o identificados por la regulación como prestadores de servicios de certificación (PSC), lo cuales pertenecen a una estructura jerárquica dentro de la infraestructura de llave pública, esta estructura mantiene diferentes entidades con diferentes roles y responsabilidades:



La autoridad raíz o central es aquella institución que certifica y otorga certificados digitales a las autoridades certificadoras, y supervisa el funcionamiento de la infraestructura en general, registrando todos los certificados digitales (claves públicas) que las autoridades certificadoras emiten.

La autoridad certificadora es quien recibe de la autoridad registradora las solicitudes para emitir certificados digitales e introduce la clave pública en un certificado, firmándolo electrónicamente de conformidad.

La autoridad registradora es el contacto entre la autoridad certificadora y los solicitantes de certificados digitales, es la responsable de acreditar la personalidad y verificar que los datos de identificación contenidos en la llave pública sean válidos y verídicos. Los certificados tienen un periodo de validez y expedirse con ciertos límites de uso, incluso,

1536 La infraestructura de clave pública debe ser entendida como un conjunto de políticas, procesos, servidores, *software* y centros de servicios utilizados con el propósito de administrar certificados y pares de claves públicas y privadas. PricewaterhouseCoppers. (2010). *Estudio Santander Universidades, Firma Electrónica en las Universidades*, p. 13.

1537 Tellez, J. (2004). *Derecho Informático*. 3ra Edición. Mc Graw Hill. México, p. 200.

limitando también el valor de las transacciones en que pueden usarse.[1538] Toda esta información acompañará a la solicitud que envíe la autoridad registradora a la autoridad certificadora para que lo introduzca al certificado digital.

Es importante mencionar que para cumplir sus funciones, la autoridad registradora puede apoyarse en personas físicas a las que se les conoce como agentes certificadores. Asimismo, la autoridad registradora deberá llevar el registro de las claves públicas certificadas por su correspondiente autoridad certificadora, ambos roles, tanto de autoridad certificadora, como de autoridad registradora son generalmente realizados por un mismo prestador.

Los PSC, en sus roles de autoridades registradoras y certificadoras, deben publicar sus prácticas, políticas, responsabilidades y alcances en documentos denominados: Declaración de Prácticas de Certificación y Políticas de Certificación, en ellos se encontrará toda la información necesaria para que las personas que reciben un documento electrónico firmado y respaldado por un certificado digital emitido por ese PSC, decida si ha de confiar en la relación entre el firmante y el par de claves.

Entre las obligaciones que tienen los PSC destacan las de poner a disposición de los titulares los sistemas para generar su par de claves de manera secreta y exclusivamente bajo su control, controlar la fiabilidad del certificado —antes de otorgarlo—, identificar perfectamente a la persona a la que se le va a otorgar el certificado, mantener un registro de los certificados emitidos, permitir la consulta en línea del estatus de los certificados emitidos y la revocación de los certificados, no almacenar o copiar bajo ninguna circunstancia las claves privadas y disponer de los recursos económicos para afrontar el riesgo de la responsabilidad por daños y perjuicios.[1539]

Queda pendiente la cuestión del profesionalismo general y de la confiabilidad del PSC. Podría ocurrir que un PSC señale que cuenta con un procedimiento detallado de certificación de la identidad, pero que no siga ese procedimiento.[1540] En este caso, el grado de confiabilidad y seguridad de la firma electrónica avanzada dependerá de la solidez procedimental, jurídica y tecnológica de la infraestructura de clave pública.[1541]

La estructura de confianza sólida del PSC permite cumplir dos de los elementos requeridos para que una firma electrónica sea avanzada, mismos que se enuncian en el artículo 97 del Código de Comercio:

I. Los datos de creación de firma (clave privada) corresponden exclusivamente al firmante.	El PSC acredita la identidad y verifica los datos contenidos en la clave pública, la cual está matemáticamente relacionada con la clave privada y, por lo tanto, si todo es correcto en el proceso, se garantiza que ambas claves corresponden exclusivamente al firmante.
II. Los datos de creación de la firma (clave privada) estaban, en el momento de la firma, bajo el control exclusivo del firmante.	La generación del par de claves se hace bajo el control exclusivo de su titular a través de un *software* basado en estándares internacionales que es proporcionado por el PSC. Asimismo, los datos de creación de firma (clave privada) están protegidos por una contraseña de acceso, la cual es establecida por su titular al momento de la generación del par de claves a través del *software* antes mencionado.

1538 Davara, M. (2008). *Manual de Derecho Informático*. Thomson Aranzadi. Décima edición. España, p. 470.

1539 Davara, M. (2008). *Manual de Derecho Informático*. Thomson Aranzadi. Décima edición. España, p. 469.

1540 Tellez, J. (2004). *Derecho Informático*. Tercera edición. Mc Graw Hill. México, p. 201.

1541 PwC. (2010). *Estudio Santander Universidades, Firma Electrónica en las Universidades*, p. 5.

En materia comercial, la principal función de los PSC es llevar a cabo los servicios adicionales de firma electrónica avanzada, como son: a) la emisión de certificados digitales de firma electrónica avanzada, b) emisión de constancias de conservación conforme a la NOM151-SCFI-2016, c) emisión de sellos digital de tiempo y d) digitalización de documentos de conformidad con la NOM151-SCFI-2016[1542] en los términos y con los requisitos que establece el Código de Comercio.

La Secretaría de Economía funge como autoridad registradora raíz y es responsable de la aplicación del marco normativo en materia de comercio electrónico, acredita a las personas jurídicas como prestador de servicios de certificación cuando cumplen con los requisitos establecidos en la Ley y supervisa las funciones de los PSC. El propio Código de Comercio y su regulación secundaria[1543] establecen requisitos específicos para los PSC en esta materia.

En el ámbito financiero, el Banco de México funge como autoridad raíz para autorizar como agencia registradora (AR) y/o agencia certificadora (AC) a las instituciones de crédito (bancos) y empresas que les presten servicios relacionados con transferencia de fondos o valores.

En el ámbito fiscal, el Servicio de Administración Tributaria (SAT) funge como un PSC con los roles de autoridad certificadora y registradora, bajo la autoridad raíz del Banco de México, lo cual se encuentra formalizado a través de un convenio de coordinación. En un segundo caso, para la emisión de certificados a personas jurídicas o morales, el propio SAT funge como autoridad raíz, autoridad certificadora y autoridad registradora.[1544]

En el ámbito de la Administración Pública Federal, la Ley Federal del Procedimiento Administrativo[1545] contempla lo siguiente:

> Artículo 69-C.
>
> La certificación de los medios de identificación electrónica del promovente, así como la verificación de la fecha y hora de recepción de las promociones o solicitudes y de la autenticidad de las manifestaciones vertidas en las mismas, deberán hacerse por las dependencias u organismo descentralizados, bajo su responsabilidad y de conformidad con las disposiciones generales que al efecto emita la Secretaría de la Función Pública.

Lo anterior es complementado con la Ley Federal de Firma Electrónica Avanzada donde se establece que cualquier institución pública conforme a las leyes que le son aplicables puede ser PSC o autoridad certificadora.

1542 Esta norma fue publicada en el DOF el 30 de marzo de 2017 y cancela la NOM-151-SCFI-2002.

1543 Artículo 102 inciso A. Código de Comercio, artículos 7, 8 y 9, Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación (DOF de 19 de julio de 2004); 2 bis, 2 bis.1. Reforma a las reglas generales a las que deberán sujetarse los prestadores de servicios de certificación (DOF de 1 de marzo de 2007. Para más referencias ver: http://www.firmadigital.gob.mx/

1544 Esta precisión es importante porque ni el Código de Comercio, la Ley Federal de Firma Electrónica Avanzada o la regulación del Banco de México permiten la emisión de certificados digitales directamente a personas morales, esto es, si se pueden emitir a representantes legales de las personas morales, pero no directamente a personas morales. Debido a que se vuelve complejo imputar la responsabilidad del uso de la clave privada a una persona física en particular, que no es titular de un certificado, como aquella materialmente realizadora del acto, lo cual afecta la teoría de la representación del ordenamiento jurídico mexicano. Para salvaguardar lo anterior el artículo 19-A del Código Fiscal estableció que: "Se presumirá sin que se admita prueba en contrario, que los documentos digitales que contengan firma electrónica avanzada de las personas morales, fueron presentados por el administrador único, el presidente del consejo de administración o la persona o personas, cualquiera que sea el nombre con el que se les designe, que tengan conferida la dirección general, la gerencia general o la administración de la persona moral de que se trate, en el momento en el que se presentaron los documentos digitales". Lo anterior, puede generar serios conflictos legales por dos cuestiones: la primera de ellas debido a que se le podrían imputar acciones a una persona diferente a aquella que solicito el certificado y/o a aquella que materialmente utilizó el par de claves y segundo porque se establece una presunción que no admite prueba en contrario, lo cual también podría interpretarse como contrario a las garantías de legalidad y seguridad jurídica, bajo las cuales se sustenta el marco jurídico mexicano.

1545 Ley Federal del Procedimiento Administrativo, última reforma DOF 18/05/2018. Disponible en: http://www. diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf

Otros esfuerzos que permite el uso de la firma electrónica avanzada y por tanto hacen referencia a las entidades certificadoras o PSC, pueden ser localizados en otros ámbitos, como el educativo,[1546] el judicial,[1547] de seguridad social,[1548] y en varias administraciones locales como la de la Ciudad de México, Baja California, Chiapas, Colima, Guanajuato, Guerrero, Hidalgo, Jalisco, Morelos, Sonora y Yucatán. En todos ellos se establecen diferentes prestadores de servicios de certificación, autoridades raíz, certificadoras y registradoras exclusivas para sus distintos ámbitos de aplicación.

Presunto infractor

Gabriel López López

Es aquella persona física o moral de carácter privado que presumiblemente dio o ha dado tratamiento a los datos personales en contravención a las disposiciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y que se encuentra sujeta a la sustanciación del Procedimiento de Imposición de Sanciones (Pisan) ante la unidad administrativa competente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Para efectos de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación y de Imposición de Sanciones (Lineamientos de Procedimiento), la fracción XIII, del artículo 3 dispone que se entiende como tal a la persona física o moral de carácter privado a la que se le inicia un procedimiento de imposición de sanciones por presuntas conductas infractoras señaladas en las resoluciones del procedimiento de protección de derechos o el de verificación, violatorias de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

1. Antecedentes

Hasta la reforma constitucional publicada en el DOF el 18 de junio de 2008, nuestra Carta Magna no reconocía expresamente el principio de presunción de inocencia, no obstante, el Pleno de la Suprema Corte de Justicia de la Nación (SCJN) sostenía que el mismo se consagraba de manera implícita en los artículos 14, párrafo segundo, 16, párrafo primero, 19, párrafo primero, 21, párrafo primero y 102, apartado A, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), pues el mismo deriva de los principios de debido proceso legal y acusatorio.

Ello reconoce el derecho de todo inculpado a su libertad y, que para privarlo de éste, es necesario cumplir con una serie de garantías mínimas otorgándole una defensa adecuada. Por su parte, el principio acusatorio implica que es a la autoridad investigadora a la que corresponde la función persecutoria de los delitos, por lo cual, consideraba que ambos

1546 La Universidad Nacional Autónoma de México mediante el acuerdo del rector, de octubre de 2005, permite el uso de la firma electrónica avanzada para docentes, escuela y facultades.

1547 El Consejo de la Judicatura del poder Judicial de la Federación, a través del acuerdo general 21/2007, establece el uso de la firma electrónica para el seguimiento de expedientes judiciales.

1548 La Ley del Seguro Social (artículos 40, 111 y 286) contempla la notificación de cédulas de liquidación a través de medios magnéticos, el uso de la firma electrónica simple en el expediente clínico electrónico y la presentación de promociones o solicitudes a través de medios de comunicación electrónicos. El Acuerdo 43/2004 que contiene los Lineamientos para la Asignación de Número Patronal de Identificación Electrónica y Certificado Digital regulan el uso de certificados electrónicos y la firma electrónica avanzada para la realización de trámites ante el Instituto Mexicano del Seguro Social (IMSS). Esta regulación no especifica quien fungirá como autoridad raíz, pero en la práctica, de nueva cuenta la autoridad, en este caso el IMSS, funge en este rol y en el de autoridad certificadora y registradora, sin admitir certificados digitales de otras autoridades.

resguardaban el principio de presunción de inocencia, pues el gobernado no tendrá la obligación de probar la licitud de su conducta, reconociendo así, *a priori*, el estado o condición de inocencia de los hombres.

Tal criterio se contiene en la tesis XXXV/2002, conforme a la cual, los principios constitucionales del debido proceso legal y el acusatorio resguardan en forma implícita el diverso principio de presunción de inocencia, dando lugar a que el gobernado no esté obligado a probar la licitud de su conducta cuando se le imputa la comisión de un delito, en tanto que el acusado no tiene la carga de probar su inocencia, puesto que el sistema previsto por la CPEUM le reconoce, *a priori*, tal estado al disponer expresamente que es al ministerio público a quien incumbe probar los elementos constitutivos del delito y de la culpabilidad del imputado.[1549]

> PRESUNCIÓN DE INOCENCIA. EL PRINCIPIO RELATIVO SE CONTIENE DE MANERA IMPLÍCITA EN LA CONSTITUCIÓN FEDERAL. De la interpretación armónica y sistemática de los artículos 14, párrafo segundo, 16, párrafo primero, 19, párrafo primero, 21, párrafo primero, y 102, apartado A, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos se desprenden, por una parte, el principio del debido proceso legal que implica que al inculpado se le reconozca el derecho a su libertad, y que el Estado solo podrá privarlo del mismo cuando, existiendo suficientes elementos incriminatorios, y seguido un proceso penal en su contra en el que se respeten las formalidades esenciales del procedimiento, las garantías de audiencia y la de ofrecer pruebas para desvirtuar la imputación correspondiente, el juez pronuncie sentencia definitiva declarándolo culpable; y por otra, el principio acusatorio, mediante el cual corresponde al ministerio público la función persecutoria de los delitos y la obligación (carga) de buscar y presentar las pruebas que acrediten la existencia de éstos, tal y como se desprende de lo dispuesto en el artículo 19, párrafo primero, particularmente cuando previene que el auto de formal prisión deberá expresar "los datos que arroje la averiguación previa, los que deben ser bastantes para comprobar el cuerpo del delito y hacer probable la responsabilidad del acusado"; en el artículo 21, al disponer que "la investigación y persecución de los delitos incumbe al ministerio público"; así como en el artículo 102, al disponer que corresponde al ministerio público de la Federación la persecución de todos los delitos del orden federal, correspondiéndole "buscar y presentar las pruebas que acrediten la responsabilidad de éstos". En ese tenor, debe estimarse que los principios constitucionales del debido proceso legal y el acusatorio resguardan en forma implícita el diverso principio de presunción de inocencia, dando lugar a que el gobernado no esté obligado a probar la licitud de su conducta cuando se le imputa la comisión de un delito, en tanto que el acusado no tiene la carga de probar su inocencia, puesto que el sistema previsto por la Constitución Política de los Estados Unidos Mexicanos le reconoce, a priori, tal estado, al disponer expresamente que es al ministerio público a quien incumbe probar los elementos constitutivos del delito y de la culpabilidad del imputado (XXXV/2002).[1550]

A partir de la referida reforma constitucional, el principio de presunción de inocencia se encuentra expresamente tutelado en la fracción I, del apartado B, del artículo 20 de la CPEUM.[1551]

En relación con lo anterior, el principio de presunción de inocencia también se encuentra reconocido por diversos instrumentos internacionales de los que México es parte, como lo son el artículo 8 de la Convención Americana sobre Derechos Humanos (CADH),[1552]

1549 Tesis P. XXXV/2002. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XVI, agosto de 2002, p. 14.

1550 Tesis P. XXXV/2002. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XVI, agosto de 2002, p. 14.

1551 Artículo 20. El proceso penal será acusatorio y oral. Se regirá por los principios de publicidad, contradicción, concentración, continuidad e inmediación.
B. De los derechos de toda persona imputada:
I. A que se presuma su inocencia mientras no se declare su responsabilidad mediante sentencia emitida por el juez de la causa.

1552 Artículo 8. Garantías Judiciales

el artículo 11 de la Declaración Universal de los Derechos Humanos y el artículo 14 del Pacto Internacional de Derechos Civiles y Políticos.[1553]

2. Delimitación conceptual y conceptos relacionados

Como se mencionó anteriormente, la CPEUM reconoce el estado o condición de inocencia de los gobernados, razón por la cual los protege a través del derecho de toda persona a que se presuma su inocencia, lo que significa que todo hombre debe ser tratado con tal calidad, inocente, hasta en tanto no se demuestre lo contrario. Esto implica que corresponde a la autoridad desvirtuar la inocencia probando la ilicitud de la conducta, así opera desde que se inicia la investigación hasta la resolución final que la destruya.

Derivado de lo anterior, el principio de presunción de inocencia exige que para imponer una sanción resulta indispensable la certeza de la comisión de la infracción, ya que si lo que motiva la imposición de la sanción es una determinada conducta, ante la duda de su comisión o su inexistencia misma, no existe justificación para imponer la sanción.

En síntesis, el principio de presunción de inocencia constituye el derecho a recibir la consideración y el trato de no partícipe en conductas infractoras y determina, el derecho a que no se apliquen las consecuencias o los efectos jurídicos que acarrea la inexistencia en la comisión de la conducta atípica sancionable, aunado al hecho de que exige la existencia de elementos probatorios que la destruyan de forma clara y contundente.

Al resolver el amparo en revisión 89/2007, la Segunda Sala de la SCJN emitió el criterio que a continuación se inserta:

> PRESUNCIÓN DE INOCENCIA. ALCANCES DE ESE PRINCIPIO CONSTITUCIONAL. El principio de presunción de inocencia que en materia procesal penal impone la obligación de arrojar la carga de la prueba al acusador, es un derecho fundamental que la Constitución Política de los Estados Unidos Mexicanos reconoce y garantiza en general, cuyo alcance trasciende la órbita del debido proceso, pues con su aplicación se garantiza la protección de otros derechos fundamentales como son la dignidad humana, la libertad, la honra y el buen nombre, que podrían resultar vulnerados por actuaciones penales o disciplinarias irregulares. En consecuencia, este principio opera también en las situaciones extraprocesales y constituye el derecho a recibir la consideración y el trato de "no autor o no partícipe" en un hecho de carácter delictivo o en otro tipo de infracciones mientras no se demuestre la culpabilidad; por ende, otorga el derecho a que no se apliquen las consecuencias a los efectos jurídicos privativos vinculados a tales hechos, en cualquier materia (2a. XXXV/2007).[1554]

De lo anterior se advierte que dicho principio opera fundamentalmente en el campo procesal, en tanto que produce un influjo decisivo en el régimen jurídico de la prueba. De este punto de vista se infieren tres cuestiones:

a) que toda condena debe ir precedida siempre de una actividad probatoria impidiendo la condena sin pruebas;

---

2. Toda persona inculpada de delito tiene derecho a que se presuma su inocencia mientras no se establezca legalmente su culpabilidad. Durante el proceso, toda persona tiene derecho, en plena igualdad, a las siguientes garantías mínimas: Artículo 11

1. Toda persona acusada de delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad, conforme a la ley y en juicio público en el que se le hayan asegurado todas las garantías necesarias para su defensa.

1553 Artículo 14

2. Toda persona acusada de un delito tiene derecho a que se presuma su inocencia mientras no se pruebe su culpabilidad conforme a la ley.

1554 Tesis 2a. XXXV/2007. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XXV, mayo de 2007, p. 1186.

b) que las pruebas para fundar la decisión de condena merecen tal concepto jurídico y ser constitucionalmente legítimas y

c) que la carga de la actividad probatoria pesa sobre los acusadores, y que no existe nunca carga del acusado sobre la prueba de su inocencia o de su participación en los hechos.

Por tanto, en virtud de la presunción de inocencia, ninguna persona podrá ser considerada culpable sino hasta la sentencia condenatoria que la desvirtúe plenamente, acreditando la infracción al ordenamiento jurídico, y en cuyo proceso se hayan observado todas las garantías necesarias para su adecuada defensa.

Es así que, el principio en estudio es aplicable, no únicamente a la materia penal, sino como se ha expuesto en la presente obra, también al derecho administrativo sancionador, en tanto que éste es una manifestación de la potestad punitiva del Estado, dado que implica la imposición de una sanción en virtud de una conducta humana que infrinja el ordenamiento jurídico.

Al respecto, resulta ilustrativa la tesis de la segunda sección de la Sala Superior del TFJA en la tesis (VIII-P-2aS-157), que determinó que el procedimiento administrativo sancionador deriva de la competencia de las autoridades administrativas para imponer sanciones a las acciones y omisiones antijurídicas desplegadas por el sujeto infractor, de modo que, la pena administrativa es una función jurídica que tiene lugar como reacción a lo antijurídico, frente a la lesión del derecho administrativo, por ello es dable afirmar que la sanción administrativa guarda una similitud fundamental con la penal, toda vez que, como parte de la potestad punitiva del Estado, ambas tienen lugar como reacción frente a lo antijurídico, ya que en uno y otro supuestos la conducta humana es ordenada o prohibida bajo la sanción de una pena, la cual se aplica dependiendo de la naturaleza del caso tanto por el tribunal, como por la autoridad administrativa, cuyo rubro y textos son:

> PRESUNCIÓN DE INOCENCIA. EL TRIBUNAL FEDERAL DE JUSTICIA FISCAL Y ADMINISTRATIVA DEBE PROCURAR SU APLICACIÓN, AL SER UN PRINCIPIO QUE OPERA EN EL DERECHO PENAL PERO TAMBIÉN PARA EL DERECHO ADMINISTRATIVO SANCIONADOR. En la tesis P.XXXV/2002, del Pleno de la Suprema Corte, publicada en el *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XVI, agosto de 2002, página 14, de rubro: "PRESUNCIÓN DE INOCENCIA. EL PRINCIPIO RELATIVO SE CONTIENE DE MANERA IMPLÍCITA EN LA CONSTITUCIÓN FEDERAL.", se advierte que los artículos 14, párrafo segundo, 16, párrafo primero, 19, párrafo primero, 21, párrafo primero y 102, apartado A, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, en su texto anterior a la reforma publicada en el *Diario Oficial de la Federación* el 18 de junio de 2008, consagran los principios del debido proceso legal y acusatorio, los cuales resguardan en forma implícita el diverso principio de presunción de inocencia, que consiste en que el gobernado no está obligado a probar la licitud de su conducta cuando se le imputa la comisión de un delito, en tanto que el acusado no tiene la carga de probar su inocencia. Si se parte de esa premisa, la presunción de inocencia es un derecho que surge para disciplinar distintos aspectos del proceso penal, empero, debe trasladarse al ámbito administrativo sancionador, en tanto ambos son manifestaciones de la potestad punitiva del Estado. De tal suerte que dicho principio es un derecho que podría calificarse de "poliédrico", en el sentido de que tiene múltiples manifestaciones o vertientes cuyo contenido se encuentra asociado con derechos encaminados a disciplinar distintos aspectos del proceso penal y administrativo sancionador. Así, en la dimensión procesal de la presunción de inocencia pueden identificarse al menos tres vertientes: 1. como regla de trato procesal; 2. como regla probatoria; y 3. como estándar probatorio o regla de juicio, lo que significa que el procedimiento administrativo sancionador se define como disciplinario al desahogarse en diversas fases con el objetivo de obtener una resolución sancionatoria de una conducta antijurídica que genera que se atribuya la carga de

la prueba a la parte que acusa. De esa forma, la sanción administrativa cumple en la ley y en la práctica distintos fines preventivos o represivos, correctivos o disciplinarios o de castigo. Así, el procedimiento administrativo sancionador deriva de la competencia de las autorida- des administrativas para imponer sanciones a las acciones y omisiones antijurídicas desplegadas por el sujeto infractor, de modo que, la pena administrativa es una función jurídica que tiene lugar como reacción frente a lo antijurídico, frente a la lesión del derecho administrativo, por ello es dable afirmar que la sanción administrativa guarda una similitud fundamental con la penal, toda vez que, como parte de la potestad punitiva del Estado, ambas tienen lugar como reacción frente a lo antijurídico, ya que en uno y otro supuestos la conducta humana es ordenada o prohibida bajo la sanción de una pena, la cual se aplica dependiendo de la naturaleza del caso tanto por el tribunal, como por la autoridad administrativa. De tal suerte que, dadas las similitudes del procedimiento penal y del administrativo sancionador, es que los principios que rigen al primero, como el de presunción de inocencia, también aplican al segundo. En esos términos, las Salas del Tribunal Federal de Justicia Fiscal y Administrativa deben utilizar un método al valorar los elementos de convicción que obran en autos, para verificar que por sus características reúnen las condiciones para considerarlos una prueba de cargo válida, además de que arrojen indicios suficientes para desvanecer la presunción de inocencia, así como cerciorarse de que estén desvirtuadas las hipótesis de inocencia y, al mismo tiempo, descartar la existencia de contraindicios que den lugar a una duda razonable sobre la que se atribuye al infractor sustentada por la parte acusadora (VIII-P-2aS-157).[1555]

Principio de calidad

Isabel Davara Fernández de Marcos,[1556]
Gregorio Barco Vega y
Alexis Cervantes Padilla

El principio de calidad del tratamiento es obligatorio para todo aquel que interviene en el tratamiento, ya sea en el sector público o privado, y se divide en dos vertientes diferenciadas:

a) el responsable del tratamiento debe adoptar las medidas necesarias a su alcance para mantener los datos personales en su posesión exactos, completos, correctos y actualizados a fin de que no se altere su veracidad, y
b) el responsable debe proceder a la cancelación de los datos personales cuando han dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables.

En cuanto a su regulación en México podemos distinguir:

a) en el sector privado, el principio de calidad aparece regulado de forma general en el artículo 11 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que establece la obligación del responsable de procurar que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados, así como la de proceder a su cancelación cuando ya no sean requeridos para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, y
b) En el sector público, el principio de calidad se reconoce, en el artículo 23 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO),

1555 Tesis VIII-P-2aS-157. *Revista del Tribunal Federal de Justicia Fiscal y Administrativa*. Octava época, no. 14, septiembre de 2017, p. 525

1556 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

que consigna la obligación del responsable del tratamiento de adoptar las medidas para cumplir con la calidad de los datos a fin de que no se altere su veracidad y ordena su supresión (previo bloqueo) una vez que concluya el plazo de conservación.[1557]

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) coinciden con las previsiones de la normatividad nacional y señalan que es obligación del responsable adoptar las medidas necesarias para mantener exactos, completos y actualizados los datos personales en su posesión, de tal manera que no se altere la veracidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento. [1558]

En el ámbito internacional, el Reglamento General de Protección de Datos Europeo (RGPD o GDPR por sus siglas en inglés) también reconoce el principio de calidad y precisa que, con base en esta máxima, los datos personales serán exactos y, si fuera necesario, actualizados, además de que se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que son tratados.[1559]

El principio de calidad está estrechamente relacionado con el principio de finalidad, proporcionalidad y minimización, puesto que se materializa cuando los datos personales tratados son exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la que se tratan.[1560] En relación con la concreción práctica de estos elementos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[1561] precisa que los mismos tienen el siguiente alcance:

a) Exactos: se considera que los datos personales son exactos cuando reflejan la realidad de la situación de su titular, es decir, son verdaderos o fieles. Sobre este particular, los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en adelante Lineamientos Generales) añaden que los datos personales son exactos y correctos cuando los mismos no presentan errores que pudieran afectar su veracidad.[1562]
b) Completos: se considera que los datos personales están completos cuando no falta ninguno de los que se requieran para las finalidades para las cuales se obtuvieron y son tratados, de forma tal que no se cause un daño o perjuicio al titular. Los Lineamientos Generales añaden que los datos se consideran completos cuando su integridad permite el cumplimiento de las finalidades que motivaron su tratamiento y de las atribuciones del responsable.[1563]
c) Pertinentes: se considera que los datos personales son pertinentes cuando corresponden efectivamente al titular.

1557 Artículo 23. El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.
Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.
Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.

1558 Artículo 19.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1559 Artículo 4, apartado 1del Reglamento General de Protección de Datos.

1560 Artículo 36 del Reglamento de la LFPDPPP.

1561 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 56. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

1562 Artículo 21, fracción I de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1563 Artículo 21, fracción II de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

d) Actualizados: se considera que los datos personales están actualizados cuando están al día y corresponden a la situación real del titular. De forma análoga, vale la pena señalar que los aludidos lineamientos para la administración pública precisan que este elemento se cumple cuando los datos responden fielmente a la situación actual del titular.

e) Correctos: se considera que los datos personales son correctos cuando cumplen con todas las características anteriores. Asimismo, los Lineamientos Generales señalan que los datos son correctos cuando no presentan errores que pudieran afectar su veracidad.[1564]

Podemos mencionar, además, dos importantes consecuencias en relación con la fuente de obtención de los datos personales:

a) Cuando los datos son proporcionados directamente por el titular: tanto el Reglamento de la LFPDPPP y la LGPDPPSO coinciden en que existe la presunción legal de que se cumple con el principio de calidad cuando los datos personales son proporcionados directamente por su titular y hasta que éste no manifieste y acredite lo contrario.[1565] Es decir, siempre que la persona a la que corresponden los datos personales los proporcione directa o personalmente se entiende que se cumple con la calidad de los datos.

b) Cuando los datos se obtengan de forma indirecta, por otro lado, el responsable deberá adoptar medidas de cualquier naturaleza (medidas razonables según el RLFPDPPP)[1566] dirigidas a garantizar que los datos responden al principio de calidad, de acuerdo con la categoría de datos personales y las condiciones y medios de tratamiento.[1567] La normatividad no precisa qué tipo de medidas deberán ser adoptadas para cumplir con lo anterior, por lo que puede presumirse que existe una versatilidad en la admisión de métodos y procedimientos para cumplir con este principio.

En este orden de ideas, el INAI[1568] señala que el responsable podrá adoptar medidas como las siguientes:

a) establecer procedimientos para corregir y actualizar los datos personales no solo en atención a solicitudes de ejercicio del derecho de rectificación, sino también de oficio, cuando el responsable cuente con evidencia de que los datos en su posesión están incorrectos;

b) realizar campañas de actualización dirigidas a los titulares;

c) informar a los encargados a los que se haya comunicados datos personales sobre las correcciones o actualizaciones de los datos personales que tengan lugar, a fin de que realicen lo conducente en la base de datos que manejen e

d) incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

En la práctica, como decíamos, el principio de calidad entraña distintas obligaciones:

a) conservar los datos personales exclusivamente por el tiempo que sea necesario para llevar a cabo las finalidades que justificaron el tratamiento y para cumplir con aspectos legales, administrativos, contables, fiscales, jurídicos e históricos, y el periodo de bloqueo;

1564 Artículo 21, fracción I de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1565 *Vid,* segundo párrafo del artículo 36 del RLFPDPPP y párrafo segundo, artículo 23 de la LGPDPPSO.

1566 Tercer párrafo del artículo 36 del RLFPDPPP.

1567 Artículo 22, fracción I de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1568 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 56. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

b) cancelar[1569] los datos personales una vez cumplida la finalidad del tratamiento, entendiendo que la cancelación da lugar al bloqueo, y a éste luego le seguirá la supresión. En este punto existe una obligación concreta en la LFPDPPP respecto del incumplimiento de obligaciones contractuales, al señalarse que los datos referentes a éstas deberán ser eliminados en un plazo de 72 meses, contados a partir de la fecha en que se presente el mencionado incumplimiento;
c) fijar y documentar los plazos de conservación y
d) acreditar que dichos plazos de conservación[1570] sean cumplidos por el responsable.

En cuanto al establecimiento de los plazos de conservación, el RLFPDPPP y la LGPDPPSO[1571] concretan que éstos deberán considerar con lo siguiente:

a) no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento;
b) deberán atender las disposiciones aplicables a la materia de que se trate;
c) deberán tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información y
d) el período de bloqueo de éstos.

En consecuencia, para determinar el plazo de conservación de los datos personales, el responsable deberá tomar en cuenta lo siguiente:

a) plazo de conservación;
b) tiempo requerido para levar a cabo las finalidades del tratamiento;
c) plazos legales, administrativos, contables, fiscales, jurídicos e históricos aplicables y
d) periodo de bloqueo

De acuerdo con el INAI, para cumplir con la obligación de conservación adecuada de los datos personales, los responsables podrán adoptar medidas como:

a) identificar las disposiciones normativas que regulan la actividad en la que se tratan los datos personales, a fin de conocer si imponen obligaciones de conservación de los datos personales por periodos específicos;
b) verificar los plazos administrativos, contables, fiscales, jurídicos e históricos que resulten aplicables;
c) verificar los plazos de prescripción legales y/o contractuales para fijar el periodo de bloqueo y definir el plazo de conservación a partir de lo anterior, y
d) establecer procedimientos para suprimir[1572] los datos personales concluido dicho periodo.[1573]

1569 Segundo párrafo del artículo 11 de la LFPDPPP y tercer párrafo del artículo 23 de la LGPDPPSO.

1570 Recomendamos al lector consultar la definición de "conservación de datos personales" que forma parte este *Diccionario de Protección de Datos Personales*.

1571 Artículo 37 del RLFPDPPP y último párrafo del artículo 23 de la LGPDPPSO.

1572 El INAI cuenta con la *Guía para el Borrado Seguro de Datos Personales*. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf, la cual establece recomendaciones precisas para realizar la eliminación de datos personales, ya sea que estos obren en soportes físicos o electrónicos.

1573 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 56. Fecha de consulta: 30 de noviembre de 2018.

En la práctica,[1574] para establecer y documentar[1575] los procedimientos de cancelación y supresión,[1576] el INAI[1577] recomienda a las organizaciones:

a) especificar por escrito los procedimientos para la conservación, bloqueo y supresión de los datos personales;
b) incluir en los procedimientos los plazos de conservación, distinguiendo con claridad cuándo deberá empezar el periodo de bloqueo;
c) detallar los pasos o fases para llevar a cabo el bloqueo y supresión total[1578] de los datos personales, y
d) acreditar que los datos personales están siendo cancelados, bloqueados y suprimidos de acuerdo con los plazos de conservación originalmente definidos por el responsable o por la normatividad que le resulte de aplicación.[1579] Para dicho fin será esencial que el responsable cuente con el documento que establezca la política de cancelación, bloqueo y supresión de datos personales y elabore bitácoras o cualquier otro documento en el que se acredite la fecha de bloqueo o supresión de los datos personales, y la información relevante en relación con dichas acciones.

Principio de consentimiento

Isabel Davara Fernández de Marcos,[1580]
Alexis Cervantes Padilla y
Gregorio Barco Vega

El principio de consentimiento[1581] establece la obligación del responsable de obtener el consentimiento del titular de los datos personales de manera libre, específica, inequívoca e informada para la realización del tratamiento de los datos personales, salvo que no sea requerido en virtud de la actualización de las causales de excepción previstas en la normatividad.

El principio de consentimiento obliga a los responsables del tratamiento, en caso de no estar dentro a alguna de las excepciones previstas en la normatividad, a solicitar el consentimiento del titular para el tratamiento de sus datos personales.

En el sector privado, el artículo 8 de la Ley Federal de Protección de Datos personales en Posesión de los Particulares (LFPDPPP) regula el principio de consentimiento y señala que: "Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley".[1582]

1574 Artículo 38 del RLFPDPPP y artículo 24 de la LGPDPPSO.

1575 Segundo párrafo del artículo 11 de la LFPDPPP y tercer párrafo del artículo 23 de la LGPDPPSO.

1576 Segundo párrafo del artículo 11 de la LFPDPPP y tercer párrafo del artículo 23 de la LGPDPPSO.

1577 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 56. Fecha de consulta: 30 de noviembre de 2018.

1578 En relación con la supresión, es necesario tener en cuenta que los Lineamientos Generales en su artículo 23 indican que las políticas, métodos y técnicas deberán considerar la irreversibilidad, seguridad y confidencialidad y que los métodos empleados sean favorables para el medio ambiente.

1579 Artículo 39 del RLFPDPPP.

1580 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

1581 En relación con esta definición se recomienda consultar las definiciones de consentimiento, consentimiento tácito, consentimiento expreso y consentimiento expreso y por escrito que forman parte de este *Diccionario de Protección de Datos Personales*.

1582 Artículo 8 de la Ley Federal de Protección de Datos personales en Posesión de los Particulares.

Asimismo, dicho artículo establece las modalidades de consentimiento aplicables, las cuales son: el tácito, el expreso y el expreso y por escrito, estableciendo reglas específicas para cada una.

En el sector público, este principio se regula en el artículo 20 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que obliga a los sujetos obligados del orden público a contar con el consentimiento previo del titular para el tratamiento de los datos personales cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 del citado ordenamiento.

De acuerdo con las disposiciones legales vigentes, es posible discernir distintas modalidades de consentimiento: el tácito, el expreso y el expreso y por escrito.[1583] Si bien en esta obra se encuentran definiciones específicas sobre cada uno de ellos, podemos mencionar de manera general que dichas modalidades se distinguen por lo siguiente:

a) Consentimiento tácito: se actualiza cuando, habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su oposición al tratamiento de sus datos.[1584] Es válido para dar tratamiento a cualquier tipo de dato personal con excepción de aquellos datos que revistan el carácter de datos personales patrimoniales, financieros o sensibles.

b) Consentimiento expreso: se actualiza cuando el titular de los datos personales manifiesta su voluntad verbalmente, ya sea por escrito, por medios electrónicos, ópticos, por cualquier otra tecnología, o por signos inequívocos.[1585] Dicho consentimiento es requerido cuando así lo exija una ley o reglamento, se trate de datos financieros o patrimoniales, datos sensibles, lo solicite el responsable para acreditar el mismo, o lo acuerden así el titular y el responsable.

c) Consentimiento expreso y por escrito: es obligatorio cuando se tratan datos personales sensibles. Se debe obtener a través de firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación equivalente.[1586]

Cualquiera que sea la modalidad bajo la cual se otorgó el consentimiento, debe revestir las siguientes características específicas:

a) Libre: cuando el consentimiento debe ser obtenido sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular.

b) Específico: el consentimiento debe referirse de forma concreta, explícita y lícita a una o varias finalidades determinadas que justifiquen el tratamiento de los datos personales. Es decir, como lo indica el INAI en la *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, la solicitud del consentimiento deberá ir siempre ligada a las finalidades concretas del tratamiento que se informen en el aviso de privacidad, esto es, el consentimiento se deberá solicitar para tratar los datos personales para finalidades específicas y no en lo general.[1587]

1583 Se recomienda consultar las definiciones de consentimiento tácito, consentimiento expreso y consentimiento expreso y por escrito que forman parte de este *Diccionario de Protección de Datos Personales* para mayor detalle sobre los elementos de cada una de las modalidades del consentimiento.

1584 *Vid*, artículo 8, segundo párrafo de la LFPDPPP y artículo 21 de la LGPDPPSO.

1585 *Vid*, artículo 8, segundo párrafo de la LFPDPPP y artículo 21 de la LGPDPPSO.

1586 Artículo 9 de la LFPDPPP y último párrafo del artículo 21 de la LGPDPPSO.

1587 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 18. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

c) Informado: de forma previa al otorgamiento del consentimiento, se debe hacer del conocimiento del titular el aviso de privacidad en virtud del cual se informa a este último sobre el tratamiento al que serán sometidos los datos personales y las consecuencias de su otorgamiento.

d) Inequívoco: este requisito se cumple cuando existen elementos que, de manera indubitable, demuestran que el consentimiento ha sido lícitamente otorgado por el titular.

e) Revocable: El titular tiene la posibilidad de revocar el consentimiento[1588] en cualquier momento, y el responsable la correlativa obligación de establecer mecanismos sencillos y gratuitos que permitan al titular ejercer dicho derecho al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.[1589]

En ausencia de dichas características el consentimiento no puede considerarse como lícitamente otorgado.

Como decíamos, la regla general indica que en todo tratamiento debe obtenerse el consentimiento del titular para el uso de sus datos personales, salvo que existan excepciones que la normatividad aplicable precisa también en los artículos 10 y 37 de la LFPDPPP y 22 y 70 de la LGPDPPSO.

Para pronta referencia, se presenta la siguiente tabla que contienen las disposiciones aludidas:

LFPDPPP		LGPDPPPSP	
Excepción al consentimiento para el tratamiento	**Excepción al consentimiento para las transferencias**	**Excepción al consentimiento para el tratamiento**	**Excepción al consentimiento para las transferencias**
Artículo 10. No será necesario el consentimiento para el tratamiento de los datos personales cuando: I. Esté previsto en una Ley; II. Los datos figuren en fuentes de acceso público; III. Los datos personales se sometan a un procedimiento previo de disociación; IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;	Artículo 37. Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos: I. Cuando la transferencia esté prevista en una ley o tratado en los que México sea parte; II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;	Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos: I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;	Artículo 70. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos: I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o tratados internacionales suscritos y ratificados por México;

1588 Artículo 21 del RLFPPP y artículo 20 de los Lineamientos Generales.

1589 Los Estándares de Protección de Protección de Datos Personales para los Estados Iberoamericanos coinciden al señalar: 12.2. Siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos.
Asimismo, el Reglamento General de Protección de Datos Personales señala en el apartado 3 de su artículo 7:
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria,tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o VII. Se dicte resolución de autoridad competente.	III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas; IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero; V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia; VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.	II. Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente; IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente; V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable; VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes; VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria; VIII. Cuando los datos personales figuren en fuentes de acceso público; IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.	II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales; III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia; IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última; V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados; VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular; VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero; VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente Ley, o IX. Cuando la transferencia sea necesaria por razones de seguridad nacional. […]

No obstante, el hecho de que no se requiera el consentimiento para el tratamiento o la transferencia de los datos personales, no implica que no se deban cumplir los otros principios (licitud, calidad, lealtad, finalidad, información, proporcionalidad y responsabilidad), y muy especialmente la obligación de poner a disposición del titular el aviso de privacidad.[1590]

1590 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 20. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Otro aspecto que conviene considerar es el de la carga de la prueba[1591] de la obtención del consentimiento, pues la obligación de demostrar su lícita obtención recae, en todos los casos, en el responsable del tratamiento[1592] por lo que, dependiendo de la modalidad del consentimiento que se involucre, el responsable deberá generar las pruebas válidas en derecho que le permitan acreditar ante la autoridad, en caso de ser requerido, la lícita obtención del consentimiento.[1593] En relación con esta carga probatoria, es fundamental tener presente que el responsable podrá valerse de pruebas electrónicas, ya éstas tienen plena validez en términos de la legislación civil,[1594] misma que es supletoria a la normatividad de protección de datos personales.

Principio de finalidad

Isabel Davara Fernández de Marcos,[1595]
Alexis Cervantes Padilla y
Gregorio Barco Vega

El principio de finalidad se traduce en la obligación legal a cargo del responsable de tratar los datos personales del titular exclusivamente para dar cumplimiento a las finalidades que le fueron informadas al titular a mediante el aviso de privacidad del responsable.

Este principio es toral porque va a definir la eficiencia y eficacia del resto de los principios, pues su especificación determinará la viabilidad del tratamiento en su conjunto. Es decir, si la finalidad no está legítimamente determinada, el consentimiento se verá viciado, pues se presta respecto de ésta. La calidad también estará cuestionada, puesto que solo que se podrá definir si los datos cumplen con la calidad respecto de la finalidad del tratamiento, ya que no hay datos correctos, actualizados o pertinentes en abstracto, sino respecto de una finalidad, lo mismo podemos decir del principio de proporcionalidad o de minimización. Por lo tanto, la finalidad define el tratamiento y con ello su licitud, lealtad y la responsabilidad de quien lo lleva a cabo.

En el sector privado, el principio de finalidad aparece regulado de forma general en el artículo 12 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que establece las siguientes obligaciones para el responsable:

1591 Los Estándares de Protección de Protección de Datos Personales para los Estados Iberoamericanos coinciden al señalar:
12. Condiciones para el consentimiento
12.1. Cuando sea necesario obtener el consentimiento del titular, el responsable demostrará de manera indubitable que el titular otorgó su consentimiento, ya sea a través de una declaración o una acción afirmativa clara.

De la misma forma, el Reglamento General de Protección de Datos en el apartado 1 de su artículo 7 indica lo siguiente:
1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

1592 Artículo 20 del RLFPDPPP y último párrafo del artículo 16 de los Lineamientos Generales.

1593 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 23. Fecha de consulta: 30 de noviembre de 2018.

1594 Artículo 210-A. Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

1595 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

a) solo realizar el tratamiento que sea necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad, y

b) obtener el consentimiento del titular en caso de querer tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad.[1596] De este modo, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) solo autoriza el tratamiento de los datos para finalidades distintas cuando así lo permita de forma explícita una ley o reglamento o cuando el responsable haya obtenido el consentimiento para el nuevo tratamiento.[1597]

En el sector público, el principio de finalidad se reconoce en el primer párrafo del artículo 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), que establece:

a) Todo tratamiento debe estar justificado por finalidades concretas, lícitas, explícitas y legítimas.

b) Las finalidades deben estar relacionadas con las atribuciones que la normatividad aplicable le confiera.

c) Si el responsable desea tratar los datos para finalidades distintas, los Lineamientos Generales de Protección de Datos Personales para el Sector Público (en adelante Lineamientos Generales)[1598] indican que deberá considerar factores como la expectativa razonable de privacidad del titular, la naturaleza de los datos personales, las consecuencias del tratamiento posterior y las medidas adoptadas para que el tratamiento cumpla con la normatividad aplicable.[1599]

En el entorno internacional, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) coinciden con las previsiones de la normatividad nacional e indican que todo tratamiento de datos personales se limitará al cumplimiento de finalidades determinadas, explícitas y legítimas.[1600] Además, añaden que "el tratamiento ulterior de datos personales con fines archivísticos, de investigación científica e histórica o con fines estadísticos, todos ellos, en favor del interés público, no se considerará incompatible con las finalidades iniciales".[1601]

El Reglamento General de Protección de Datos europeo (RGDP o GDPR por sus siglas en inglés) también reconoce el principio de finalidad al precisar que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados de forma incompatible con esos fines.[1602]

Como vemos, existe una multitud de conceptos jurídicos indeterminados en la definición de este principio. Lo anterior no es una deficiencia en la técnica legislativa, sino que precisamente expresa la gran dificultad que existe para definir este principio y su concreción. Los Lineamientos Generales explican qué se entiende por finalidades concretas, lícitas, explícitas y legítimas:

1596 Coinciden en este sentido los Estándares de Protección de Datos Personales:
17.2. El responsable no podrá tratar los datos personales en su posesión para finalidades distintas a aquellas que motivaron el tratamiento original de éstos, a menos que concurra alguna de las causales que habiliten un nuevo tratamiento de datos conforme al principio de legitimación.

1597 Artículo 43 del RLFPDPPP.

1598 Artículo 9 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1599 Artículo 10 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1600 Artículo 17.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1601 Artículo 17.3 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1602 Artículo 4, apartado 1 del Reglamento General de Protección de Datos.

a) Concretas: cuando el tratamiento de los datos personales atiende a la consecución de fines específicos o determinados sin que admitan errores, distintas interpretaciones o provoquen incertidumbre, dudas o confusión con el titular. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) recomienda establecer controles para evitar que los datos personales se traten para finalidades no previstas en el aviso de privacidad o que no hayan sido consentidas por el titular e incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.[1603]

b) Explícitas: se deberán especificar de manera clara para qué objeto se tratarán los datos personales, sin lugar a confusión y con objetividad.[1604] El responsable se encuentra obligado a evitar que las finalidades que describa en el aviso de privacidad sean inexactas, ambiguas o vagas e incluyan redacciones como "de manera enunciativa más no limitativa", "entre otras finalidades", "otros fines análogos", "por ejemplo" o "entre otros".[1605]

c) Lícitas: cuando las finalidades que justifican el tratamiento de los datos personales son acordes con las atribuciones o facultades del responsable, conforme a lo previsto en la legislación y el derecho internacional que le resulte aplicable. Como decíamos, el principio de calidad influye irremediablemente en los demás principios, de manera que muchos de ellos —si no es que todos— se ven directamente imposibilitados de cumplir si se incumple con el principio de finalidad.

d) Legítimas: cuando las finalidades que motivan el tratamiento de los datos personales se encuentran habilitadas por el consentimiento del titular, salvo que se actualice alguna de las causales de excepción previstas en el artículo 22 de la LGPDPPSO.[1606]

Por otro lado, la finalidad o finalidades del tratamiento se distinguen en dos tipos:[1607]

1603 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 52. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

1604 Con fundamento en lo previsto por el artículo 40 del RLFPDPPP.

1605 Lineamiento 24 de los Lineamientos del Aviso de Privacidad.

1606 Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla.
II. Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.
III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente.
IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente.
V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.
VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria.
VIII. Cuando los datos personales figuren en fuentes de acceso público.
IX. Cuando los datos personales se sometan a un procedimiento previo de disociación.
X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

1607 En este sentido, los Lineamientos del Aviso de Privacidad establecen que la definición de las finalidades tiene que cumplir con los siguientes criterios:

a) en el listado de finalidades se deberán incluir las relativas al tratamiento con fines de mercadotecnia, publicidad o prospección comercial, en caso de que el responsable trate los datos personales para dichos fines y
b) se deberá identificar y distinguir entre las finalidades que dieron origen y son necesarias para la existencia, mantenimiento y cumplimiento de la relación jurídica entre el responsable y titular, de aquéllas que no lo son.

a) primarias: las que dan origen a la relación jurídica entre el responsable y el titular y
b) secundarias: las que no dan origen a la relación jurídica y están sometidas al consentimiento[1608] del titular, sin que la negativa de éste tenga como consecuencia la conclusión del tratamiento.[1609] En este contexto, los Lineamientos del Aviso de Privacidad[1610] indican que en el aviso de privacidad se deberá informar al titular sobre el mecanismo implementado para que pueda manifestar su negativa[1611] para el tratamiento de sus datos personales en relación con las finalidades que no son necesarias para la relación jurídica entre el responsable y titular.[1612]

Principio de lealtad

Isabel Davara Fernández de Marcos,[1613]
Alexis Cervantes Padilla y
Gregorio Barco Vega

El tratamiento de los datos personales no solo debe ser legal, sino también leal. El principio de lealtad consiste en:

a) la obligación de los responsables del tratamiento de respetar la confianza depositada por el titular de los datos al proporcionar sus datos personales para un determinado tratamiento, esto es, la expectativa razonable[1614] del titular de los datos, de forma tal que los datos sean exclusivamente tratados de conformidad con las condiciones previamente acordadas por las partes en el aviso de privacidad, así como en términos de lo dispuesto por la normatividad aplicable.[1615]

1608 Con fundamento en lo previsto por el artículo 41 del RLFPDPPP.

1609 Con fundamento en lo previsto por el artículo 42 del RLFPDPPP.

1610 Fracción V del lineamiento vigésimo cuarto de los Lineamientos del Aviso de Privacidad.

1611 En los casos en que el aviso de privacidad no se haga del conocimiento del titular de manera personal o directa, por ejemplo, cuando se haga por envío postal, el aviso de privacidad debe indicar que el titular tiene un plazo de cinco días hábiles para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades secundarias. Ver definición de "consentimiento tácito" en este diccionario.

1612 De acuerdo con los Lineamientos del Aviso de Privacidad, el mecanismo para que el titular manifieste su negativa para el tratamiento de sus datos personales para finalidades secundarias deberá cumplir con lo siguiente:
Mecanismo para manifestar la negativa
25. El mecanismo al que refiere la fracción V del lineamiento anterior, podrá ser implementado a través de la inclusión de casillas u opciones de marcado en el propio aviso de privacidad, o bien fuera de éste, por el medio que el responsable determine, el cual deberá estar disponible al momento en que el titular consulta el aviso de privacidad. En todos los casos, este mecanismo debe permitir que el titular manifieste su negativa previa al tratamiento de sus datos personales o al aprovechamiento de los mismos.
En términos del párrafo segundo del artículo 14 del Reglamento de la Ley, cuando el aviso de privacidad no se haga del conocimiento del titular de manera directa o personal, se deberá incluir en éste una declaración o advertencia que informe al titular que tiene un plazo de cinco días hábiles para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales con respecto a las finalidades que no son necesarias, ni dieron origen a la relación jurídica con el responsable.
Quedan a salvo los derechos del titular para ejercer sus derechos a la revocación del consentimiento u oposición, en caso de que no manifieste la negativa para el tratamiento de sus datos personales previo a la entrega de los mismos o de su aprovechamiento.

1613 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

1614 Según el artículo 7 de la LFPDPPP y artículo 19 de la LGPDPPSO, la expectativa razonable de privacidad del titular se entiende como "la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por la Ley".

1615 INAI. (s. f.). *Guía para Titulares de los Datos Personales. Volumen 2. Principios rectores de la Protección de Datos Personales*, p. 7. Disponible en: http://inicio.ifai.org.mx/Guias/Guia%20Titulares-02_PDF.pdf

b) La garantía para el titular de que nadie puede obtener sus datos personales a través de medios engañosos o fraudulentos. Esto incluye:
   1. no recabar los datos personales con dolo, mala fe o negligencia,
   2. no vulnerar la confianza del titular en relación con que sus datos personales serán tratados conforme a lo acordado por las partes e
   3. informar a este último sobre todas las finalidades del tratamiento de sus datos a través del aviso de privacidad.[1616]

El principio de lealtad tiene dos dimensiones, una positiva que se traduce en la facultad del titular de autorizar el tratamiento de sus datos siempre que el responsable respete los intereses del titular y evite hace uso de mecanismos ilícitos para su obtención. En su dimensión negativa, este principio se concreta en la prohibición para el responsable de tratar los datos en contravención de los intereses del titular[1617] y mediante el uso de medios engañosos o fraudulentos.

El sustento normativo del principio de lealtad está en el artículo 7 de la Ley Federal de Protección de Datos personales en Posesión de los Particulares (LFPDPPP) y en el artículo 19 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que disponen lo siguiente:

Artículo 7 de la LFPDPPP	Artículo 19 de la LGPDPPSO
Artículo 7 La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. En todo tratamiento de datos personales se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.	Artículo 19 El responsable no deberá obtener y tratar datos personales a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.

En el ámbito regional es importante mencionar que los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) consagran el principio de lealtad y previenen que en virtud de dicho principio el responsable deberá tratar los datos personales en su posesión privilegiando la protección de los intereses del titular y absteniéndose de tratarlos a través de medios engañosos o fraudulentos. Asimismo, dicho instrumento detalla que se considera que un tratamiento de datos es desleal cuando se da lugar a una discriminación injusta o arbitraria contra los titulares.[1618]

1616 El Reglamento de la LFPDPPP (RLFPDPPP) señala, en su artículo 44, que dicho principio establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, y añade la prohibición de hacer uso de medios engañosos o fraudulentos para recabar y tratar datos personales, e indica que se considera que existe una actuación fraudulenta o engañosa por parte del responsable cuando se presente cualquiera de los siguientes supuestos:
   1. exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento,
   2. se vulnere la expectativa razonable de privacidad del titular a la que se refiere el artículo 7 de la LFPDPPP y
   3. las finalidades no sean las informadas en el aviso de privacidad.

1617 En el sector público, el artículo 11 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público es coincidente con lo señalado en el RLFPDPPP y añade, en su fracción II, que se considera que el responsable privilegia los intereses del titular cuando el tratamiento de datos personales que efectúa no da lugar a una discriminación o trato injusto o arbitrario contra éste.

1618 Artículos 15.1 y 15.2 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

Dicha redacción se traduce en la obligación de los Estados iberoamericanos de introducir en su normatividad interna disposiciones que garanticen la protección de la expectativa razonable de privacidad y que prohíban tratamientos de datos que se consideren desleales frente a los titulares de los datos personales.

Por otro lado, es importante mencionar que el Reglamento General de Protección de Datos europeo (RGPD o GDPR por sus siglas en inglés) señala que los responsables del tratamiento se encuentran compelidos a dar tratamiento a los datos de forma lícita, leal y transparente en relación con el interesado.[1619]

En la faceta práctica, en su *Guía para cumplir con los principios y deberes de la LFPDPPP*,[1620] el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) recomienda a los responsables que para tratar los datos personales respetando la protección de intereses y confianza del titular de los datos, prescindiendo del uso de cualquier práctica ilícita en el tratamiento, implementen lo siguiente:

a) Revisar los procedimientos y formatos utilizados por la organización o por los encargados contratados para recabar datos personales, para verificar que en no se utilicen prácticas que lleven a la obtención de los datos de manera dolosa, de mala fe o con negligencia. En este punto, el INAI sugiere que se realicen acciones de capacitación y concientización del personal, y prohibir cláusulas contractuales o mecanismos de otro tipo que conduzcan a la obtención de datos personales por medios engañosos o fraudulentos.

b) Prever sanciones para el personal o encargados en caso del uso de prácticas dolosas, de mala fe o negligentes para la obtención de los datos personales.

c) Tratar los datos conforme lo acordado e informado al titular, en los términos de la normatividad aplicable y el aviso de privacidad.

Principio de licitud

Isabel Davara Fernández de Marcos,[1621]
Alexis Cervantes Padilla y
Gregorio Barco Vega

El principio de licitud se traduce como la obligación del responsable del tratamiento de recabar y dar tratamiento a los datos personales de forma lícita conforme a las disposiciones establecidas en la normatividad de datos personales aplicable.[1622] Es decir, este principio implica el mandato de que el responsable del tratamiento de los datos personales lleve a cabo el tratamiento con apego y cumplimiento a lo dispuesto por la legislación mexicana y por el derecho internacional.[1623]

Sin embargo, en el ámbito del derecho público, este principio se concreta más y establece la obligación de que el responsable del tratamiento sujete su actuar a las facultades o atri-

1619 Artículo 5 del Reglamento General de Protección de Datos.

1620 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 14-15. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

1621 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

1622 Artículo 7 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

1623 Artículo 10 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

buciones que la normatividad aplicable le confieran[1624] y con estricto apego y cumplimiento de lo dispuesto en la normatividad aplicable, y en su caso, el derecho internacional, respetando los derechos y libertades de los titulares.[1625]

En este contexto, el principio de licitud, según indica el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), conmina al responsable a dar tratamiento a los datos personales de forma lícita y leal actuando con apego a las leyes en general y en lo particular a la normatividad de protección de datos personales. Es decir, sobre dicha base explicativa, el responsable solo podrá hacer con los datos personales aquello que le esté legalmente permitido.[1626]

Derivado de lo anterior, los responsables del tratamiento, tanto en el ámbito privado como en el público, se encuentran jurídicamente compelidos a dar cumplimiento a los principios (consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad) y deberes (seguridad y confidencialidad)[1627] de protección de datos personales, por lo que la violación de cualquiera de los principios y deberes referidos se traduce en una violación al principio de licitud, y por en ende puede afirmarse que existe una vulneración al derecho humano de protección de datos personales.

Otra vertiente del principio de licitud regulado en la normatividad mexicana es la que obliga al responsable a abstenerse de obtener datos personales a través de medios engañosos o fraudulentos. Si bien es cierto que de la definición legal del principio de licitud únicamente pueden advertirse las dos vertientes antes señaladas, en la práctica la autoridad ha señalado que incumplir con alguno de sus apercibimientos implica también una violación al principio de licitud.

En el entorno internacional, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos establecen, en su artículo 14.1, la obligación del responsable de tratar los datos personales en su posesión con estricto apego y cumplimiento de lo dispuesto por el derecho interno del Estado iberoamericano que resulte aplicable, el derecho internacional y los derechos y libertades de las personas. Asimismo, el artículo 14.2 del citado ordenamiento previene que el tratamiento de datos personales que realicen las autoridades públicas debe sujetarse a las facultades o atribuciones que el derecho interno del Estado iberoamericano les confiera expresamente, además de lo previsto en el numeral 14.1 antes referido.

Por su parte, el Reglamento General de Protección de Datos Europeo (RGPD o GDPR por sus siglas en inglés) señala que los responsables del tratamiento se encuentran compelidos a dar tratamiento a los datos de forma lícita, leal y transparente en relación con el interesado.[1628]

Cabe resaltar que el RGPD establece una serie de bases de legitimación para considerar lícito el tratamiento de los datos personales: el consentimiento del titular para fines específicos, la ejecución de un contrato en el que el interesado es parte o para la aplicación de medidas precontractuales, el cumplimiento de una obligación legal aplicable al responsable, la protección de intereses vitales del interesado o de otra persona física, el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos y la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero.[1629]

1624 Artículo 17 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1625 Artículo 8 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1626 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 14. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

1627 Artículo 6 de la LFPDPPP y artículos 16 de la LGPDPPSO y 7 de los Lineamientos Generales.

1628 Artículo 5 del Reglamento General de Protección de Datos.

1629 Artículo 6 del Reglamento General de Protección de Datos.

Como podemos ver, en la regulación europea el principio de licitud está vinculado exclusivamente a la necesidad de que el responsable que lleve a cabo un tratamiento cuente con una base de legitimación, y no así, a la obligación del responsable del tratamiento de cumplir con la totalidad de las obligaciones impuestas en la normatividad.

En cuanto a su cumplimiento práctico, el INAI recomienda en su *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*[1630] y así evitar contravenir lo dispuesto por la mencionada Ley. Por su parte, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), ni ninguna otra ley o normatividad aplicable en nuestro país, o convenio o acuerdo internacional del cual México sea parte,[1631] puede realizar las siguientes acciones:

a) Revisar que los datos se traten conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) y demás normativa aplicable.
b) Conocer la normativa que en lo particular regule la actividad en la que se tratan los datos personales, como por ejemplo las disposiciones en materia de salud o bancarias e identificar si dicha normativa incluye disposiciones que se vinculen, de manera directa o indirecta, con la protección o el tratamiento de datos personales.
c) Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

Principio de proporcionalidad

Isabel Davara Fernández de Marcos,[1632]
Alexis Cervantes Padilla y
Gregorio Barco Vega

El responsable puede tratar exclusivamente aquellos datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las cuales se obtuvieron del titular. El principio de proporcionalidad se encuentra intrínsecamente relacionado con los principios de calidad y finalidad.

En la práctica, el principio de proporcionalidad impone al responsable del tratamiento un límite en la recolección de datos personales, de forma tal que el responsable no recabe datos personales a su arbitrio y, sin que sean necesarios para el cumplimiento de un fin concreto, explícito y legítimo.

En el sector privado, el principio de proporcionalidad aparece regulado de la siguiente manera:

1. De forma general, en el artículo 13 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) se establecen las siguientes obligaciones:

1630 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* pp. 14-15. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

1631 INAI (s.f.). *Guía para Titulares de los Datos Personales. Volumen 2. Principios rectores de la Protección de Datos Personales*, p. 6. Disponible en: http://inicio.ifai.org.mx/Guias/Guia%20Titulares-02_PDF.pdf

1632 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

a) Cuidar que solo sean objeto de tratamiento los datos personales necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.[1633]

b) Realizar esfuerzos razonables para limitar el periodo de tratamiento de datos personales sensibles a efecto de que sea el mínimo indispensable. Sobre este particular, el párrafo segundo del artículo 9 de la LFPDPPP prohíbe crear bases de datos que contengan datos personales sensibles, sin que medie una justificación para finalidades legítimas, concretas y acordes con las actividades del responsable, haciendo además especial hincapié el INAI en que el responsable verifique el periodo que se requiere para conservar los datos personales sensibles, y una vez transcurrido, se proceda a su eliminación.

2. En el artículo 45 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) se señala que solo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.

En el sector público, el principio de proporcionalidad se reconoce en el primer párrafo del artículo 25 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), donde se obliga al responsable a tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.[1634] Por su parte, los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) indican[1635] que se considera que los datos son adecuados, relevantes y estrictamente necesarios cuando son apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención, de acuerdo con las atribuciones conferidas al responsable por la normatividad aplicable.[1636]

En el entorno internacional, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) coinciden con las previsiones de la normatividad nacional y convienen en que este principio obliga al responsable a tratar únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario en relación con las finalidades que justifican su tratamiento.[1637]

El Reglamento General de Protección de Datos Europeo (RGPD o GDPR por sus siglas en inglés) concreta este principio al establecer el mandato de que los datos personales sean adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.[1638]

Finalmente, cabe mencionar que el principio de proporcionalidad se escinde en un subprincipio conocido como criterio de minimización.[1639] Con base en este criterio, el responsable se

1633 En este sentido el

1634 Con fundamento en el artículo 45 del RLFPDPPP.

1635 Artículo 24 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1636 Para cumplir con el principio de proporcionalidad en la práctica, el INAI recomienda a los responsables realizar lo siguiente:
- Identificar las finalidades del tratamiento de los datos personales y hacerse la pregunta ¿qué datos personales necesito para cumplir con esta finalidad?
- Revisar los datos personales que se están tratando en cada una de las finalidades y, a partir de la respuesta dada en la pregunta anterior, hacerse la pregunta ¿son necesarios para cumplir con la finalidad?
- Incluir previsiones sobre la obligación de cumplir con este principio en las cláusulas, contratos u otros instrumentos jurídicos que se firmen con terceros.

INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 48. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

1637 Artículo 18.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1638 Artículo 4, apartado 1 del Reglamento General de Protección de Datos.

1639 El RGPD señala en el apartado 1 de su artículo 4 que los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos).

encuentra legalmente compelido a realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del que ha motivado su tratamiento.[1640] Para esto, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) recomienda que a partir del análisis que el responsable realice para determinar que solo hayan sido objeto de tratamiento los datos necesarios, adecuados y relevante, realice un nuevo esfuerzo y trate de reducir al mínimo indispensable los datos personales que requiere para cumplir con las finalidades para las cuales se obtuvieron y elimine, tras el requerido bloqueo como se explica en el principio de calidad, de sus bases de datos aquellos que no son indispensables para cumplir con las finalidades.[1641]

Principio de responsabilidad

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La palabra "responsabilidad" hace referencia a la cualidad de ser responsable[1642] y jurídicamente es la capacidad existente en todo sujeto activo de derecho para reconocer y aceptar las consecuencias de un hecho realizado libremente.[1643] Es decir, se trata de una palabra empleada para denotar la capacidad de ser responsable por los propios actos y asumir las consecuencias que de ello se deriven.

Desde la perspectiva del derecho de protección de datos personales se ha empleado con frecuencia este término para referirse a la persona (física o moral) que decide sobre el tratamiento (denominado responsable) de datos personales, y que, por detentar esa capacidad de decisión, está obligado a adoptar medidas, estrategias, políticas, procedimientos y prácticas concretos para dar cumplimiento a los principios (licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad) y deberes (confidencialidad y seguridad) de protección de datos personales.[1644]

Como señala el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[1645] "a este principio se le conoce también como el principio de rendición de cuentas, ya que establece la obligación de los responsables de velar[1646] por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación y demostrar ante los titulares y la autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales".[1647]

1640 Con fundamento en el artículo 45 del RLFPDPPP y el artículo 25 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1641 El RGPD señala en el apartado 1 de su artículo 4 que los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos).

1642 RAE. (2017). Responsabilidad, en *Diccionario de la Lengua Española.* Disponible en: http://dle.rae.es/?id=WCqQQlf

1643 RAE. (2017). Responsabilidad, en *Diccionario de la Lengua Española.*

1644 Para un mayor estudio sobre este tema recomendamos la lectura de las definiciones de los principios y deberes mencionados y que forman parte de este *Diccionario de Protección de Datos Personales*.

1645 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 63. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

1646 De acuerdo con el *Diccionario de la Lengua Española*, la palabra "velar" tiene diversas acepciones entre las que podemos encontrar dos de utilidad: 1) observar atentamente algo y 2) cuidar solícitamente de algo. Consultado en: *Diccionario de la Real Academia Española*, el 30 de noviembre de 2018. Disponible en: http://dle.rae.es/?id=bTFZNAf|bTJiBaz|bTJnxpM

1647 En el entorno anglosajón este principio (llamado "accountability" en inglés) es de reconocida y cada vez mayor relevancia y significación. *Vid*. Grupo de Trabajo del Artículo 29, Dictamen 3/2010 sobre el principio de responsabilidad,

En la normatividad nacional, este principio se recoge de forma independiente en las leyes de protección de datos personales aplicables para los sectores privado y público.

En el sector privado, el principio de responsabilidad se reconoce de forma general en el artículo 14 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que señala que es obligación del responsable velar por el cumplimiento de los principios de protección de datos personales establecidos por la LFPDPPP debiendo adoptar las medidas necesarias para su aplicación incluso cuando los datos fueren tratados por un tercero a solicitud del responsable.

En el sector público, el principio de responsabilidad se reconoce en el primer párrafo del artículo 29 de la LGPDPPSO, que obliga al responsable a implementar específicos mecanismos legales para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la LGPDPPSO y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular, al Instituto o a los organismos garantes, según corresponda. En este contexto, los Lineamientos Generales señalan que el responsable deberá adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la normatividad aplicable, así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y el INAI.[1648]

Por su parte, los Estándares coinciden con las previsiones de la normatividad nacional y convienen en que este principio obliga al responsable a implementar los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones, así como a rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

En el Reglamento General de Protección de Datos Europeo (RGPD o GDPR por sus siglas en inglés) el principio de "responsabilidad proactiva" es uno de los cambios más significativos del RGPD, que nuestra legislación ya incorpora, de modo más tácito en el sector privado y con más contundencia en el sector público. Algunos de los puntos más importantes en el RGPD en este principio son los siguientes:

a) El cambio esencial está en la rendición de cuentas, en la obligación demostrable que el responsable ha velado por el respeto a los principios y a la normatividad de una manera proactiva.
b) Emplea la expresión "responsabilidad proactiva" y establece que con base en dicha máxima el responsable del tratamiento es responsable del cumplimiento de los principios de protección previstos en su artículo 5 y deberá ser capaz de demostrarlo,[1649] señalando específicamente la adhesión a códigos de conducta o a un mecanismo de certificación aprobados, como elementos para demostrar dicho cumplimiento.
c) Es necesario que la responsabilidad del responsable del tratamiento quede establecida frente a cualquier tratamiento de datos personales que éste realice (por sí mismo o a través de un tercero), estando obligado, en consecuencia, a aplicar medidas opor-

adoptado el 13 de julio de 2010. Fecha de consulta: 30 de octubre de 2018. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_es.pdf

1648 Primer párrafo del artículo 46 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

1649 Artículo 4, apartado 1 del Reglamento General de Protección de Datos.

tunas y eficaces para demostrar[1650] la conformidad de sus actividades con el RGPD, incluyendo la eficacia de las medidas.[1651]

d) Para medir la eficacia y eficiencia de dichas medidas, el RGPD señala que deberá tenerse en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, uniendo el principio de la responsabilidad proactiva a otro concepto esencial en el RGPD, el de análisis de riesgo.

Como vemos, el alcance del principio de responsabilidad es imponer una serie de obligaciones prácticas y demostrables que requiere acciones concretas y actividades específicas. El Grupo de Trabajo del Artículo 29 (GT29 o WP29 por sus siglas en inglés)[1652] ha insistido en que la "arquitectura jurídica" de los mecanismos de responsabilidad podría plantear dos niveles:

a) Primer nivel: consistiría en un requisito reglamentario básico vinculante para todos los responsables del tratamiento de datos. El contenido del requisito incluiría dos elementos, la aplicación de medidas/procedimientos y el mantenimiento de pruebas de dicho extremo. Este primer nivel podría complementarse con requisitos particulares.

b) Segundo nivel: incluiría sistemas discrecionales de responsabilidad que superaran los requisitos jurídicos mínimos de los principios subyacentes de protección de datos (proporcionando garantías más estrictas que las exigidas por la normativa aplicable) y las modalidades de aplicación o de garantía de la eficacia de las medidas (requisitos de aplicación que sobrepasen el nivel mínimo).

En el caso de la normatividad nacional, podemos exponer la siguiente comparativa de los mecanismos del primer nivel:

Artículo 48 del RLFPDPPP	Artículo 30 de la LGPDPPSO
I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable.	I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales.
II. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.	II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable.
III. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad.	III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales.
IV. Destinar recursos para la instrumentación de los programas y políticas de privacidad.	IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.

continúa...

1650 Responsabilidad del responsable del tratamiento.

1651 El RGPD señala en el apartado 1 de su artículo 4 que los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos).

1652 *Vid*. Grupo de Trabajo del Artículo 29, Dictamen 3/2010 sobre el principio de responsabilidad, adoptado el 13 de julio de 2010. Fecha de consulta: 30 de octubre de 2018. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_es.pdf

V. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos.	V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
VI. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran.	VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares.
VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales.	VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia.
VIII. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento.	VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.
IX. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento.	
X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.	

Según el alcance del principio de responsabilidad, la anterior lista puede entenderse como ilustrativa[1653] ya que en la práctica el responsable puede adoptar medidas adicionales y complementarias[1654] para acreditar el cumplimiento de este principio. Es decir, las me-

1653 Como sustento de lo anterior se puede mencionar que el segundo párrafo del artículo 46 de los Lineamientos Generales señala que en adición a los elementos previstos en el artículo 30 de la LGPDPPSO, en la adopción de las políticas e implementación de mecanismos a que se refiere el citado artículo 46, el responsable deberá considerar, de manera enunciativa más no limitativa, el desarrollo tecnológico y las técnicas existentes, la naturaleza, contexto, alcance y finalidades del tratamiento de los datos personales, las atribuciones y facultades y demás cuestiones que considere convenientes pudiendo valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de mejores prácticas o cualquier otro mecanismos que determine adecuado para tales fines.

1654 En el mismo sentido, los Estándares Iberoamericanos en su artículo 20.3 exponen una serie de medidas enunciativas y no limitativas
20.3. Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa más no limitativa, los siguientes:
a) Destinar recursos para la instrumentación de programas y políticas de protección de datos personales.
b) Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales.
c) Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable.
d) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales.

didas previstas en la normatividad pueden considerarse componentes fijos que deberán aplicarse en la mayoría de las operaciones de tratamiento de datos, mientras que, las soluciones particularizadas serán aplicables al resto de medidas que el responsable adopte en función de los hechos y circunstancias de cada caso particular, con atención especial al nivel de riesgo identificado en cada tratamiento.[1655]

En síntesis, de acuerdo con la normatividad vigente en materia de protección de datos personales, el principio de responsabilidad implica la asunción de las siguientes obligaciones por parte del responsable:

a) Velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales (incluso en casos en que los datos sean tratados por encargados).
b) Adoptar las medidas y mecanismos necesarios para garantizar el debido tratamiento de los datos personales privilegiando los intereses del titular y la expectativa razonable de privacidad.
c) Adoptar medidas específicas para que los terceros con los que se sostiene una relación jurídica que implique el tratamiento de los datos personales, respeten el aviso de privacidad del responsable.

Como vemos, la magnitud, extensión e importancia del principio de responsabilidad es mucha, y en este orden de ideas, para concretar la explicación, hemos considerado prudente y necesario sintetizar las siguientes recomendaciones emitidas por el INAI[1656] para determinar si una organización sujeta a la LFPDPPP cumple con el principio de responsabilidad:

Cumplimiento al principio de responsabilidad	
Obligación	Acciones recomendadas para el cumplimiento
Velar por el cumplimiento de los principios y responder por el tratamiento de los datos personales, aún por aquéllos comunicados a encargados.	Incluir en los contratos u otro instrumento jurídico que celebre con sus empleados, encargados y/o terceros, cláusulas en las que se comprometan a garantizar el adecuado tratamiento de los datos personales.

continúa...

e) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran.
f) Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales.
g) Establecer procedimientos para recibir y responder dudas y quejas de los titulares.

1655 En el mismo sentido, los Estándares Iberoamericanos en su artículo 20.3 exponen una serie de medidas enunciativas y no limitativas.

1656 INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* p. 63. Fecha de consulta: 30 de noviembre de 2018. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

Adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.	Establecer acciones técnicas y administrativas para la protección de los datos personales, tales como considerar el impacto a la privacidad en el diseño de sistemas de información, bases de datos y tratamiento.
	Adoptar políticas de privacidad, adherirse a esquemas de autorregulación, hacer uso de estándares, mejores prácticas internacionales o mecanismos similares.
	Establecer programas de capacitación y actualización, así como desarrollar contenidos que permitan concientizar a quienes tienen acceso a datos personales para el desarrollo de sus funciones.
	Adoptar medidas que permitan supervisar, vigilar y verificar el grado de cumplimiento de la organización en materia de protección de datos personales, estableciendo también sanciones en caso de incumplimiento.
	Analizar los riesgos que implica todo tratamiento de datos personales para el derecho fundamental a la protección de datos y la privacidad de sus titulares.
Tomar medidas para que los terceros con quienes mantiene una relación jurídica que implique el tratamiento de los datos personales, respeten el aviso de privacidad en el que se establezcan las condiciones de dicho tratamiento.	Incluir en los contratos u otros instrumentos jurídicos que celebre con terceros, cláusulas en las que se establezca la obligación de realizar el tratamiento de los datos de conformidad con los términos señalados en el aviso de privacidad.
	Documentar la comunicación del aviso de privacidad a terceros.

En definitiva, el principio de responsabilidad:

a) es una obligación proactiva del responsable del tratamiento, y
b) debe estar orientada a poder demostrar de forma continua que cumple con los principios, deberes y obligaciones previstos en la normatividad ante la autoridad garante y ante el propio titular de los datos personales.

Principios de autorregulación vinculante

Rosa María Franco Velázquez

Los principios que deben observarse y regir a los esquemas de autorregulación, según los parámetros de autorregulación vinculante,[1657] son los de: voluntariedad, obligatoriedad, transparencia, responsabilidad e imparcialidad. Así, cada uno de dichos principios se traduce en lo siguiente:[1658]

1. "Voluntariedad: La adhesión o adopción de los esquemas de autorregulación vinculante será de manera libre sin que medie vicio alguno en el consentimiento". Esto es que,

1657 Parámetros de Autorregulación en materia de Protección de Datos Personales, publicados en el *Diario Oficial de la Federación* el 29 de mayo de 2014. (Los Parámetros).

1658 Numeral 8 de los Parámetros.

aquellas personas físicas o morales que traten datos personales decidirán de manera libre y manifestarán su voluntad respecto a si se adhieren o no a un determinado esquema de autorregulación. Sin embargo, una vez que se toma la decisión de adherirse a un determinado esquema de autorregulación, será obligatorio para dicha persona física o moral y podrá ser sancionada de acuerdo con las reglas del esquema.

2. "Obligatoriedad: El esquema de autorregulación vinculante constriñe a quien se adhiere al mismo o lo adopta". Toda vez que los esquemas de autorregulación vinculante complementan la legislación en materia de protección de datos y buscan que se cumpla con ella de manera más sencilla con reglas acordes con la realidad de un determinado sector, es necesario que sean obligatorios para todos aquellos que se adhieren. En concreto, un esquema de autorregulación no será la excepción para cumplir con determinada regulación, sino para cumplir con ella de forma más eficiente y adecuada.
3. "Transparencia: Las prácticas en materia de protección de datos personales serán transparentes, salvo aquella información que se especifique como confidencial o reservada, siempre que exista el derecho a clasificarla de conformidad con las disposiciones aplicables". El derecho humano de acceso a la información establece que en principio los individuos pueden solicitar, investigar, difundir, buscar y recibir toda la información de los órganos de gobierno y aquella que se refiera a ellos mismos, con las únicas limitantes que se establezcan en las leyes aplicables, por ejemplo, por razones de interés público y seguridad nacional.[1659] Es así que toda la información en materia de datos personales, incluyendo aquella que se refiera a las características de esquemas de autorregulación vinculante, debe estar disponible y abierta al público salvo que se haya clasificado como confidencial o reservada.
4. "Responsabilidad: El responsable tiene la obligación de velar por el cumplimiento de los principios de protección de datos personales previstos por la Ley, en relación con los datos personales que posee o que haya comunicado a un tercero o encargado, ya sea que éste se encuentre o no en territorio nacional, para lo cual deberá adoptar las medidas necesarias". La Ley dispone que los responsables del tratamiento deberán observar, durante el ciclo de vida de los datos, los principios de protección de datos personales como licitud, consentimiento, información, calidad, finalidad, lealtad, responsabilidad y proporcionalidad.[1660] Es así que, aunque el tratamiento de datos personales se lleve a cabo por un tercero o encargado, el responsable deberá tomar las medidas necesarias, como la adopción de cláusulas de protección de datos, convenios de remisión y transferencia, etc. para que dicho tercero o encargado cumpla también con los principios de protección de datos personales y demás obligaciones establecidas en la Ley, el Reglamento y otra normatividad que resulte aplicable.
5. "Imparcialidad: los esquemas de autorregulación vinculante deben organizarse e implementarse de forma que se salvaguarden la objetividad e imparcialidad de sus actividades". Teniendo en cuenta que los esquemas de autorregulación en ocasiones son supervisados y aplicados por los mismos adheridos, deben contar con reglas claras respecto al cumplimiento y aplicación de sus principios y estándares, a fin de que siempre sean observados de manera imparcial y objetiva.

1659 Artículo 4 de la Ley General de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 4 de mayo de 2015.

1660 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010. (La Ley).

Privacidad

Olivia Andrea Mendoza Enríquez

La privacidad se puede entender como el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.[1661]

Por su parte, el derecho a la privacidad es el derecho de las personas para separar aspectos de su vida privada del escrutinio público, es decir, el derecho de las personas para desarrollar en un espacio reservado ciertos aspectos de la vida personal.

Este derecho tiene dos componentes esenciales: el derecho de aislarse y el derecho de controlar la información de carácter personal.

1. Delimitación conceptual y conceptos correlacionados

Lo primero que se debe decir es que el concepto "privacidad" no es un concepto terminado y que dependerá del contexto y circunstancias de los casos particulares, para acotarlo. Es decir, lo que en un país puede considerarse como ámbito privado en otro no.

En virtud de lo anterior, el término "privacidad" no es fácil de definir, ya que hasta el momento no se tiene una idea clara de sus alcances. Esto se confirma con lo dicho por el Tribunal Europeo de Derechos Humanos, que considera la privacidad como un concepto amplío, no susceptible de una definición exhaustiva.[1662]

La Suprema Corte de Justicia de la Nación (SCJN) ha establecido que las afirmaciones contenidas en las resoluciones nacionales e internacionales relacionadas a la privacidad o vida privada son útiles en la medida en que no se tomen de manera descontextualizada, emerjan de un análisis cuidadoso de los diferentes escenarios jurídicos en los que la idea de privacidad entra en juego y no se pretenda derivar de ellas un concepto mecánico de vida privada, de referentes fijos e inmutables. Lo único que estas resoluciones permiten reconstruir, en términos abstractos, es la imagen general que evoca la idea de privacidad en nuestro contexto cultural.[1663]

Aunado a lo anterior, el vertiginoso desarrollo tecnológico plantea nuevos desafíos hacía las nuevas manifestaciones de ámbitos privados en la vida de las personas, como el caso de los correos electrónicos, las plataformas digitales de mensajería instantánea, o en su caso, los dispositivos electrónicos que reportan información de los ámbitos más privados e íntimos de las personas.

Dicho lo anterior, resulta conveniente también establecer que los términos privacidad y derecho a la privacidad no necesariamente refieren a lo mismo: la privacidad es un elemento consustancial a la dignidad humana y por ende debe ser protegido por el derecho y el derecho a la privacidad es aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público.[1664]

1661 Información consultada en el *Diccionario de la Lengua Española*. Disponible en: http://dle.rae.es/?id=UD4g0KW. Fecha de consulta: 12 de septiembre de 2018.

1662 Véase Piñar, J. (2010). "¿Existe privacidad?, Lección magistral impartida en la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid", en *Protección de Datos Personales. Compendio de lecturas y legislación*. México. Editorial Tiro Corto, p. 16.

1663 165823. 1a. CCXIV/2009. Primera Sala. Novena época. *Semanario Judicial de la Federación y su Gaceta.* Tomo XXX, diciembre de 2009, p. 277. Derecho a la Vida Privada. Su contenido general y la importancia de no descontextualizar las referencias a la misma. Disponible en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/165/165823.pdf. Fecha de consulta: 20 de agosto de 2018.

1664 Ricci, D. (2013). "Artículo 16 Constitucional. Derecho a la privacidad", en Ferrer Mac-Gregor, *et al* (coord.). *Derechos Hu-*

Vincular el concepto de privacidad a elementos tan importantes como la dignidad humana no es cosa menor, ya que esto ha permitido establecer la obligación de los Estados para su efectiva garantía, a partir de la teoría de los derechos humanos y de la articulación, en este caso, desde el Sistema Interamericano de Derechos Humanos, del cual México forma parte.

Iniciando desde la conceptualización del derecho a la privacidad, éste tiene su origen en la doctrina estadounidense de finales del siglo XIX, cuando Warren y Brandeis publicaron su ensayo *The Right to Privacy*, el cual manifestaba el necesario reconocimiento del derecho a no ser molestados (*right to be alone*), y posteriormente Westin amplió este concepto e incluyó dentro del derecho a la privacidad, el derecho de todo individuo para determinar cómo, cuándo y hasta qué punto su información personal es comunicada a los demás.[1665]

A pesar de que el concepto surge en un sistema de derecho perteneciente al *common law*, esta doctrina ha tenido un impacto provechoso en sistemas jurídicos del derecho continental, como en el caso de México, particularmente para la construcción del derecho a la protección de datos personales.

A partir del ensayo *The Right to Privacy*, el concepto de privacidad se define casi de la misma manera y se mantiene el elemento constante de que la privacidad se describe como un derecho a ser dejado en paz y un derecho de cada uno individuo para determinar, en circunstancias normales, cuáles son sus pensamientos, los sentimientos y las emociones comunicadas con otros.[1666]

Dicho lo anterior, podemos afirmar que el derecho a la privacidad tiene dos componentes principales:

a) el derecho de aislarse y
b) el derecho a controlar la información personal, incluso después de haberla difundido.

Como se ha dicho, es en este segundo componente del derecho a la privacidad en el que se configura y manifiesta el derecho a la protección de datos personales. En este sentido, si bien la garantía del derecho a la protección de datos personales no significa por sí misma una garantía efectiva del derecho a la privacidad, sí supone un componente primordial para dicha salvaguarda, es decir, el derecho a la protección de datos personales no significa por sí mismo privacidad, pero no puede haber privacidad sin la garantía del derecho a la protección de datos personales.

A partir del derecho a la privacidad, convergen algunos conceptos relacionados a éste, entre los que destacan:

a) Vida privada: es la esfera de la vida que se decide dejar en el ámbito de lo privado o de lo íntimo y que no puede ser invadida por persona o entidad alguna. Aquello que se decide dejar fuera del conocimiento de lo público.

   La protección constitucional de la vida privada implica poder conducir parte de la vida protegida de la mirada y las injerencias de los demás, y guarda conexiones de variado tipo con pretensiones más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos: el derecho de poder tomar libremente

manos en la Constitución: comentarios de jurisprudencia constitucional Interamericana II. Instituto de Investigaciones Jurídicas. UNAM, p. 1045. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf. Fecha de consulta: 20 de agosto de 2018.

1665 Westin, A. (1967). *Privacy and Freedom*. Nueva York. Ateneum, p. 7.

1666 Holvast, J. (2007). *History of Privacy*. Disponible en: http://opendl.ifip-tc6.org/db/conf/ifip9-6/fidis2008/Holvast08.pdf. Fecha de consulta: 20 de agosto de 2018.

ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular.[1667]

b) Intimidad: es la zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.[1668] Existe un debate en relación a si intimidad y privacidad son conceptos que se pueden utilizar como sinónimos. Algunos tribunales han determinado que sí, y otros doctrinarios, como Garzón Valdés, han estimado ambos conceptos refieren a situaciones distintas.[1669]

   La SCJN hace una diferencia entre vida privada e intimidad en el Amparo Directo en Revisión 402/2007,[1670] en el que establece que la intimidad se constituye con los extremos más personales de la vida y del entorno familiar, cuyo conocimiento está restringido a los integrantes de la unidad familiar.

   Con las reservas y posturas de los tribunales respecto del debate, podemos decir que la intimidad es un elemento manifestado dentro del ámbito privado, cuya afectación requeriría un nivel más alto de protección jurídica.

c) Autodeterminación informativa: el derecho a la autodeterminación informativa fue reconocido en el sistema jurídico anglosajón bajo los vocablos *privacy* o *right of privacy*.

   No obstante, para el derecho continental, esta acepción llega cuando el Tribunal Constitucional Federal Alemán en la sentencia de 15 de diciembre de 1983 sobre el censo completó los derechos constitucionales de la personalidad, sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad, lo cual garantizó la continuidad de las libertades básicas reconocidas anteriormente, a través de la formulación de un nuevo derecho denominado "autodeterminación informativa".

   Este derecho reconoce la facultad de las personas para decidir sobre el tratamiento de sus datos personales y así garantizar derechos conexos como el derecho a la no discriminación y al libre desarrollo de la personalidad.[1671]

d) Derecho de protección de datos personales: este derecho le confiere a las personas control sobre su información personal. Se manifiesta a través de los denominados derechos de acceso, rectificación, cancelación y oposición (ARCO) frente al tratamiento de datos personales. El titular del dato personal tiene el poder para decidir quién, cuándo, cómo y hasta qué punto utilizan su información personal. Al igual que los demás dere-

1667 165823. 1a. CCXIV/2009. Primera Sala. Novena época. *Semanario Judicial de la Federación y su Gaceta.* Tomo XXX, diciembre de 2009, p. 277. Derecho a la Vida Privada. Su contenido general y la importancia de no descontextualizar las referencias a la misma.

1668 *Diccionario de la Lengua Española*. Disponible en: http://dle.rae.es/?id=LyCn6I9. Fecha de consulta: 10 de agosto de 2018.

1669 Garzón, E. (2008). "Lo íntimo, lo privado y lo público", en *Cuadernos de Transparencia.* México. Núm. 6. IFAI. Disponible en: http://biblio.upmx.mx/textos/15588.pdf. Fecha de consulta 20 de agosto de 2018.

1670 Amparo Directo en Revisión 402/2007. Disponible en: http://207.249.17.176/Transparencia/Epocas/Primera%20sala/Novena%20%C3%A9poca/2007/133.pdf. Fecha de consulta: 13 de agosto de 2018.

1671 Sentencia de 15 de diciembre de 1983 emitida por el Tribunal Constitucional Federal Alemán. Disponible en: http://www.informatica-juridica.com/jurisprudencia/alemania.asp. Fecha de consulta: 13 de agosto de 2018.
El principio de consentimiento se analiza en esta sentencia, anulando la Ley del Censo de Población de 1982 y que dio lugar a una revisión sustancial de la ley federal de 1977, así como de las leyes del ejército y del servicio secreto.

chos humanos, no es un derecho absoluto y su ejercicio solo puede estar limitado a aquellas restricciones prescritas en ley que resulten razonables en una sociedad democrática, por ejemplo: seguridad nacional, seguridad pública, preservación de la salud, prevención del delito y la protección de los derechos y libertades de los demás.

Para el caso de México, el derecho a la protección de datos personales tiene un reconocimiento constitucional, desarrollado en el marco de los postulados de la doctrina europea y los esquemas de autorregulación y sectorización del sistema anglosajón.[1672]

e) Inviolabilidad de las comunicaciones: con la denominación "secreto de las comunicaciones" u otras como "inviolabilidad de la correspondencia" se ha constituido una de las dimensiones o garantías clásicas de los derechos fundamentales que protegen la vida privada de la persona, aunque es, en definitiva, un derecho fundamental autónomo.[1673]

El Código Nacional de Procedimientos Penales, publicado en el *Diario Oficial de la Federación* el 5 de marzo de 2014, proporciona una definición de la intervención de comunicaciones privadas, al prever en el párrafo segundo del artículo 291[1674] lo siguiente: "La intervención de comunicaciones privadas abarca todo un sistema de comunicación, o programas, que sean fruto de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo".[1675]

El derecho reconocido constitucionalmente en México de la inviolabilidad de las comunicaciones dispone que las comunicaciones privadas son inviolables y que únicamente la autoridad judicial federal, a petición del ministerio público federal o su homólogo en las entidades federativas, pueden solicitar la intervención de comunicaciones privadas. En su momento existió un debate interesante entorno a facultades reservadas para las mismas autoridades antes citadas, respecto de solicitudes de geolocalización en tiempo real. Este derecho protege a la persona frente a intromisiones no solo de terceros particulares, sino del Estado, siempre que no se encuentre en alguna de las excepciones de ley.[1676]

2. Contenido esencial y características del derecho a la privacidad

Es conveniente decir que, si bien no existe un reconocimiento expreso del derecho a la privacidad en instrumentos jurídicos internacionales, sí se encuentra un importante antecedente en el reconocimiento del derecho a la no injerencia en la vida de las personas, lo

1672 Mendoza, O. (2018). "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", en *Revista IUS*. México. Vol. 12. Núm. 41, p. 273. Disponible en: https://www.revistaius.com/index.php/ius/article/view/355. Fecha de consulta: 20 de agosto de 2018.

1673 Díaz, J. (2006). "El derecho fundamental al secreto de las comunicaciones: una visión desde la jurisprudencia europea y su influencia en el Tribunal Constitucional español", en *Derechos Humanos México, Revista del Centro Nacional de Derechos Humanos*. Año 1, núm. 2. Disponible en: http://www.corteidh.or.cr/tablas/R21770.pdf. Fecha de consulta: 10 de agosto de 2018.

1674 En este ordenamiento se desarrolla un concepto acorde a la evolución tecnológica en México, al prever que podría ser materia de intervención, tanto las comunicaciones en tiempo real como aquellas realizadas de manera previa a la intervención.

1675 Código Nacional de Procedimientos Penales. Disponible en: http://dof.gob.mx/nota_detalle.php?codigo=5334903&fecha=05/03/2014. Fecha de consulta: 20 de agosto de 2018.

1676 Mendoza, A. (2016). "El Secreto de las comunicaciones en el ámbito de internet", en Recio Gayo, Miguel, (coord.), *La Constitución en la sociedad y economía digitales. Temas selectos de derecho digital mexicano*, Suprema Corte de Justicia de la Nación, p. 135. Disponible en: https://www.sitios.scjn.gob.mx/cec/sites/default/files/archivos/calendario_actividades/00_La%20constitucion%20en%20la%20sociedad%20y%20economia%20digitales%20%28entero%29.pdf

cual ha contribuido para el desarrollo de doctrina en torno a los derechos de privacidad y el de protección de datos personales.

Los instrumentos internacionales más relevantes en la materia son el artículo 12[1677] de la Declaración Universal de los Derechos Humanos de 1948,[1678]el artículo 11 de la Convención Americana sobre Derechos Humanos, el V de la Declaración Americana de los Derechos y Deberes del Hombre y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, los cuales reconocen el derecho a la no injerencia en la vida privada de las personas.

Por otro lado, el derecho a la privacidad no es un derecho reconocido expresamente por la Constitución Política de los Estados Unidos Mexicanos (CPEUM), no obstante, a partir de criterios jurisprudenciales, se ha establecido su reconocimiento y límites para la garantía de dicho derecho.

En este sentido, la SCJN, al resolver el Amparo en Revisión[1679] 134/2008, determinó que el fundamento del derecho a la privacidad en México es el primer párrafo del artículo 16 constitucional, al establecer la garantía de seguridad jurídica de todo gobernado a no ser molestado en la privacidad de su persona, de su intimidad familiar o de sus posesiones, sino mediante mandamiento escrito. La privacidad no se acota al espacio físico del domicilio, lugar donde normalmente se manifiesta la intimidad, sino que se incluyó también aquellas intromisiones o molestias que por cualquier medio puedan realizarse en el ámbito de la vida privada.[1680]

Existen algunos otros reconocimientos constitucionales implícitos en relación con la salvaguarda del derecho a la privacidad, entre los que se encuentran:

a) Información confidencial en términos del derecho de acceso a la información: la fracción segunda del artículo 6 de la CPEUM establece límites en el ejercicio del derecho de acceso a la información, lo cual hace necesario que las autoridades federales, estatales y municipales protejan cuando concedan el ejercicio del derecho de acceso a la información pública, lo referente a la vida privada y datos personales de las personas, en los términos y con las excepciones que fijen las leyes.[1681]
b) Límites de la libertad de imprenta: el artículo 7 constitucional establece como límite a la libertad de imprenta, el respeto a la vida privada de las personas.[1682]

1677 Artículo 12 DUDH: nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. Disponible en: http://unesdoc.unesco.org/images/0017/001790/179018m.pdf. Fecha de consulta: 20 de agosto de 2018.

1678 En el contexto de posguerra, se debe recordar que acciones cometidas por el Estado alemán, como el censo de los judíos, llevó a reflexiones sobre los límites en las intromisiones de la vida privada de las personas por parte de los Estados.

1679 Este juicio de amparo dio origen a la tesis 2ª. LXIII/2008. El derecho a la privacidad o intimidad está protegido por el artículo 16, primer párrafo de la CPEUM.

1680 Amparo en Revisión 134/2008: el primer párrafo del artículo 16 constitucional, la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a un ámbito de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. En un sentido amplio, la referida garantía puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida. Disponible en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/169/169700.pdf. Fecha de consulta: 20 de agosto de 2018.

1681 Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_270818.pdf. Fecha de consulta: 13 de agosto de 2018.

1682 Artículo 7 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_270818.pdf. Fecha de consulta: 13 de agosto de 2018.

c) La inviolabilidad de las comunicaciones: el artículo 16 constitucional establece que las comunicaciones privadas son inviolables, y que únicamente la autoridad judicial federal, a petición del ministerio público federal o de su homólogo en las entidades federativas, puede solicitar la intervención de las comunicaciones privadas. Existe la posibilidad de realizar intervenciones de comunicaciones privadas en cualquier materia, siempre y cuando la comunicación grabada fuera aportada por alguna de las partes que participaran en ella. También se estableció la obligación de instaurar juzgados de control que dieran trámite a las solicitudes de intervención de comunicaciones, y llevar a cabo un registro de todas las comunicaciones sostenidas por jueces y autoridades de investigación para estos fines.[1683]

d) El derecho a la protección de datos personales: el mismo artículo 16 constitucional garantiza este derecho y, como vimos en líneas previas, se trata de un articulador natural del derecho a la privacidad. En 2009 se reformó el artículo 16 mencionado, a fin de reconocer el derecho a la protección de datos personales y las acciones inherentes al ejercicio de este derecho, los denominados derechos de acceso, rectificación, cancelación y oposición frente al tratamiento de datos personales (ARCO).[1684]

e) Resguardo de identidad y datos personales de víctimas: otra disposición constitucional que abona a la garantía del derecho a la privacidad es la establecida en el artículo 20, apartado C, fracción V de la CPEUM, que reconoce el derecho que tienen las víctimas del delito a que sea resguardada su identidad y sus datos personales en los casos relacionados con menores de edad, delitos de violación, secuestro, delincuencia organizada, o bien cuando a juico del juzgador, ello sea necesario para la protección de la víctima.[1685]

A manera de resumen podemos decir que, si bien el derecho a la privacidad no se encuentra expresamente reconocido en el texto constitucional, sí se puede lograr su efectiva salvaguarda a través de derechos habilitadores como los mencionados en líneas previas.

Por otro lado, la Corte Interamericana de Derechos Humanos[1686] (CIDH) ha reconocido que el derecho a la privacidad tiene como objeto:

a) proteger la vida privada y domicilio de injerencias arbitrarias o abusivas, es decir, el derecho de quedar exento de las invasiones por parte de particulares o de las autoridades estatales y

b) controlar la información de carácter personal, incluso después de haberla proporcionado a un particular o entidad del Estado.

En el mismo sentido, reconoce que los aspectos de la vida sexual de las personas están protegidos dentro del derecho a la privacidad.

En las siguientes líneas analizaremos algunos elementos que la CIDH ha incorporado al derecho a la privacidad:

1683 Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_270818.pdf. Fecha de consulta: 13 de agosto de 2018.

1684 Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_270818.pdf.

1685 Artículo 20 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_270818.pdf. Fecha de consulta 13 de agosto de 2018.

1686 La reforma constitucional de 2011, en materia de derechos humanos en México, obliga que las autoridades en cualquier ámbito respeten los instrumentos jurídicos internacionales y la jurisprudencia de tribunales especializados en la protección de derechos humanos, como la Corte Interamericana de Derechos Humanos.

a) "Caso de las Masacres de Ituango vs. Colombia": el domicilio y la vida privada se encuentran intrínsecamente ligados ya que el domicilio se convierte en un espacio en el cual se puede desarrollar libremente la vida privada, por lo que el domicilio se encuentra dentro del ámbito de protección del derecho a la privacidad.[1687]

b) En el caso "Fontevecchia y D´Amico vs. Argentina", aunado al reconocimiento del domicilio como elemento de la vida privada, determina que el ámbito de la privacidad comprende entre otras dimensiones, tomar decisiones libremente relacionadas con diversas áreas de la propia vida, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público. En este caso, la CIDH reconoce expresamente el derecho de controlar la información de carácter personal, lo cual se traduce en el derecho a la protección de datos personales.[1688]

c) Caso "Fernández Ortega y otros vs. México"[1689] y "Rosendo Cantú y otra vs. México":[1690] la CIDH incorpora la vida sexual dentro del concepto de vida privada, al señalar que es un término amplio no susceptible de definiciones exhaustivas, pero que comprende, entre otros ámbitos protegidos, la vida sexual y el derecho de establecer y desarrollar relaciones con otros seres humanos. En estos casos, la CIDH establece que ante la violación sexual que sufrieron las víctimas, se vulneraron valores y aspectos esenciales de su vida privada, y supuso una intromisión en su vida sexual y anuló su derecho a tomar libremente decisiones respecto de con quien tener relaciones sexuales, perdiendo de forma completa el control sobre sus decisiones más personales e íntimas y sobre las funciones corporales básicas.

d) Caso "Tristán Donoso vs. Panamá", la CIDH reconoció que aunque las conversaciones telefónicas no se encuentren expresamente previstas en el artículo 11 de la Convención Americana sobre Derechos Humanos, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección de la vida privada.[1691] En este mismo caso, la CIDH reconoce dos elementos primordiales relacionados al derecho a la privacidad: la honra y la reputación, al señalar que el primero se relaciona con la estima y valía propia, mientras que la reputación se refiere a la opinión que otros tienen de una persona.[1692]

Podemos concluir que la CIDH reconoce como elementos inherentes al derecho a la privacidad al derecho a la vida privada, la inviolabilidad del domicilio, de las conversaciones telefónicas y de cualquier comunicación, el derecho a la honra y la reputación.

1687 Sentencia de 1 de julio de 2006. "Caso de las masacres de Ituango vs. Colombia", numeral 7 del apartado de Declaraciones, p. 146. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf. Fecha de consulta: 20 de agosto de 2018.

1688 Caso "Fontevecchia y D´Amico vs. Argentina". Fondo, reparaciones y costas. Sentencia 29 de noviembre de 2011. numeral 48. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf. Fecha de consulta: 13 de agosto de 2018.

1689 Caso "Fernández Ortega y otros vs. México". Sentencia de 30 de agosto de 2010. Disponible en: http://www.ordenjuridico.gob.mx/JurInt/STCIDHM2.pdf. Fecha de consulta 13 de agosto de 2018.

1690 Caso "Rosendo Cantú y otra vs. México". Sentencia de 31 de agosto de 2010. Disponible en: http://www.ordenjuridico.gob.mx/JurInt/STCIDHM5.pdf. Fecha de consulta: 13 de agosto de 2018.

1691 Caso "Tristán Donoso vs. Panamá", numeral 55. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf. Fecha de consulta 20 de agosto de 2018.

1692 Caso "Tristán Donoso vs. Panamá", numeral 55.

3. Límites al derecho a la privacidad

Cuando afirmamos que el derecho a la privacidad es un derecho humano reconocido implícitamente en instrumentos internacionales y nacionales, debemos considerar que en esta lógica no existen derechos absolutos, por lo que estará sujeto a una serie de limitantes, entre ellos, otros derechos humanos, como la libertad de expresión y el derecho de acceso a la información.

En este sentido, en los casos "Tristán vs. Panamá" y "Escher vs Brasil", la CIDH manifestó que el derecho a la vida privada no es absoluto, por lo que los Estados pueden restringirlo, sin embargo, para que una injerencia no sea abusiva o arbitraria, debe:

a) estar prevista en una ley en sentido formal y material;

b) seguir un fin legítimo, y

c) ser necesaria en una sociedad democrática, es decir, que se cumplan los principios de idoneidad, necesidad y proporcionalidad.[1693]

A continuación desarrollamos algunos de los límites más comunes del derecho a la privacidad:

a) Libertad de expresión. El derecho a la privacidad es una de las limitantes naturales del derecho de libertad de expresión. En el caso "Ulloa vs. Costa Rica", la CIDH reconoció expresamente que la libertad de expresión no es un derecho absoluto según lo dispone el artículo 12.3 de la CADH.[1694] Uno de los límites a la libertad de expresión en el respeto a los derechos o a la reputación de los demás. No obstante, lo anterior, es importante decir que el derecho a la libertad de expresión no puede estar sujeto a la previa censura, sino a responsabilidades ulteriores, las cuales deben estar fijadas por ley. Esto se traduce en el deber de los Estados de garantizar mecanismos legales para, por ejemplo, reclamar el derecho al honor, pero que esto no se puede traducir en el establecimiento de mecanismos sistemáticos de censura (responsabilidad ulterior).

   En el caso "Kimel vs. Argentina", la CIDH reconoce que para determinar la prevalencia entre el derecho de libertad de expresión y el derecho a la honra, requiere necesariamente de una ponderación a través de un juicio de proporcionalidad y de un estudio caso por caso, conforme a las características y circunstancias propias.[1695]

   En estos planteamientos, y ante conflictos entre derechos como la privacidad vs. La libertad de expresión, existen consideraciones importantes a tener en cuenta, como las características de la persona que invoca un daño al honor, si ésta, por ejemplo, funge como servidor público o si en su caso, existe un interés público para la divulgación de la información.

   En este sentido, se debe considerar que las personas que ocupan cargos públicos o políticos o los propios particulares que desarrollan actividades sometidas al escrutinio público han decidido voluntariamente exponerse a dicho escrutinio y, por tanto, ceden un peldaño de derecho a la privacidad frente a la divulgación de información que, por ejemplo, abone a la transparencia, la rendición de cuentas y la democracia en los Estados.

1693 Caso "Tristán Donoso vs. Panamá", numeral 56. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf. Fecha de consulta: 20 de agosto de 2018.
Caso "Escher y otros vs. Brasil", numeral 29. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp1.pdf. Fecha de consulta: 20 de agosto de 2018.

1694 Convención Americana sobre Derechos Humanos. Disponible en: https://www.cidh.oas.org/Basicos/Spanish/Basicos2.htm. Fecha de consulta: 8 de agosto de 2018.

1695 Caso "Kimel vs. Argentina". Fondo, reparaciones y costas. Sentencia 2 de mayo de 2008, numeral 51. Disponible en: http://www.corteidh.or.cr/docs/casos/articulos/seriec_177_esp.pdf. Fecha de consulta: 13 de agosto de 2018.

b) Derecho de acceso a la información pública. Tanto la fracción segunda del artículo 6 de la CPEUM, como los artículos 100 y 116 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP)[1696] contienen disposiciones que garantizan el derecho a la privacidad, al establecer los límites del ejercicio del derecho de acceso a la información, lo cual obliga a las autoridades federales, estatales y municipales a proteger cuando concedan el ejercicio de este derecho, aquella información denominada como confidencial y correspondiente a datos personales de los ciudadanos. En este punto es necesario decir que no todos los datos personales son confidenciales, particularmente considerando aquella información que identifique a servidores públicos y que sea una obligación en materia de transparencia divulgar, como el correo electrónico institucional o número de teléfono oficial asignado.

   En este apartado es importante decir que los principios de interpretación de los derechos involucrados permiten definir la prevalencia de uno sobre otro, por ejemplo, el principio de máxima publicidad asociado al derecho de acceso a la información, a la luz de los principios de proporcionalidad y finalidad vinculados al derecho de protección de datos personales.

   En este sentido, el principio de proporcionalidad se adscribe a la teoría sobre el contenido esencial de los derechos fundamentales, al establecer el límite de los límites de esos derechos, en cada caso concreto y de acuerdo con las circunstancias en que se relacionen los bienes jurídicos que colisionan, oponiéndose a la teoría absoluta que distingue en ellos un núcleo intangible e inmutable en toda situación.[1697]

Procedimientos en materia de protección de datos personales para el sector público

María Solange Maqueo Ramírez

1. Cuestiones generales

La tutela y la efectividad del derecho humano a la protección de datos personales, reconocido por los artículos 6 y 16 de la CPEUM, dependen en gran medida de los medios de defensa con los que cuenten los titulares de datos personales para hacer valer los derechos subjetivos que emanan del mismo. Para esos efectos, el título noveno de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) prevé como medios de impugnación a favor de los titulares de datos personales, los recursos de revisión e inconformidad, a fin de que estén en posibilidad de combatir aquellas actuaciones que consideran que lesionan sus derechos e intereses jurídicos en materia de protección de datos personales, además, por supuesto, de brindar la oportunidad de revisar y reflexionar sobre la legalidad de dichas actuaciones.

Dado que el derecho a la protección de datos personales es un derecho personalísimo, los recursos de revisión e inconformidad solo pueden interponerse por el titular de los datos personales, sea por sí mismo o a través de su representante legal, por lo cual es necesario que acredite su identidad y, además, en el caso de los representantes, su personalidad.

1696 Ley General de Transparencia y Acceso a la Información Pública. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf. Fecha de consulta: 23 de agosto de 2018.

1697 Sánchez, R. (2007). El principio de proporcionalidad. Instituto de Investigaciones Jurídicas. México. UNAM, p. 119. Disponible en: http://biblio.juridicas.unam.mx/libros/5/2422/12.pdf. Fecha de consulta: 24 de agosto de 2018.

No obstante, el artículo 97 de la LGPDPPSO abre la posibilidad de interponer estos recursos respecto de los datos personales concernientes a personas fallecidas a quienes demuestren un interés jurídico o legítimo para ello.[1698]

En ambos casos, los recursos de revisión e inconformidad constituyen "medios impugnativos […] que conforman una relación procesal autónoma para combatir una determinación anterior […] de carácter administrativo",[1699] dado que su sustanciación depende de una autoridad distinta de aquella ante la que se generó el acto reclamado. De hecho, su resolución descansa, dentro del ámbito de su competencia, en los órganos garantes del derecho a la protección de datos personales creados para tal efecto. En ese sentido, la característica distintiva de los recursos de revisión e inconformidad, frente a otro tipo de recursos administrativos o contencioso-administrativos previstos en el sistema jurídico mexicano, consiste en que se constituyen en medios de impugnación para la tutela de un derecho humano encomendado a órganos garantes constitucionalmente autónomos.

Si bien, tanto el recurso de revisión como el de inconformidad son medios de impugnación establecidos a favor de los titulares de datos personales, cuyo cometido consiste en dotar de efectividad el derecho a la protección de datos personales, con especial énfasis dirigido a la salvaguarda del ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO), aunque no exclusivamente, difieren en cuanto a su objeto, oportunidad procesal y autoridad resolutora. Mientras que el recurso de revisión está dirigido a combatir los actos realizados por los responsables del tratamiento de datos personales (también llamados sujetos obligados en el ámbito del sector público) ante los cuales el recurrente previamente manifestó sus pretensiones; el recurso de inconformidad recae sobre las resoluciones emitidas por los órganos garantes de las entidades federativas con motivo de los recursos de revisión de los que hubieran conocido. De tal forma que mientras los recursos de revisión se substancian y resuelven por cualquiera de los 33 órganos garantes en materia de protección de datos personales, de acuerdo con su ámbito de competencia territorial, el recurso de inconformidad corresponde de manera exclusiva al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Así, se trata de dos vías de impugnación concatenadas entre sí, donde el recurso de inconformidad solo es posible si previamente se ha agotado el recurso de revisión correspondiente.

Estas diferencias entre ambos recursos hacen necesario su tratamiento conceptual de manera individualizada.

2. Recurso de revisión

Este medio de impugnación se vincula con la existencia previa de un acto administrativo (o una omisión) realizada por alguno de los sujetos obligados previstos en la LGPDPPSO, esto es por "cualquier autoridad, entidad, órgano u organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos o fondos pú-

1698 El ahora abrogado acuerdo mediante el cual se aprueban los Lineamientos para la recepción, sustanciación y resolución de los recursos de revisión en materia de datos personales, interpuestos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales fue publicado en el *Diario Oficial de la Federación* el 12 de junio de 2017 y establecía en su lineamiento vigésimo qué debía entenderse por interés legítimo e interés jurídico y quiénes podían alegarlos. Actualmente estas disposiciones se encuentran previstas en el artículo 129 del "Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público", publicados en el *Diario Oficial de la Federación* el 26 de enero de 2018.

1699 Fix-Zamudio, H. (1998). Voz "Recurso", en *Diccionario Jurídico Mexicano*, 12ª. ed. UNAM. Instituto de Investigaciones Jurídicas, México, p. 2703.

blicos" en el ámbito federal, estatal o municipal,[1700] en el cual se actualice alguna de las siguientes causales de procedencia:

I. se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
II. se declare la inexistencia de los datos personales;
III. se declare la incompetencia por el responsable;
IV. se entreguen los datos incompletos;
V. se entreguen datos personales que no correspondan con lo solicitado;
VI. se niegue el acceso, rectificación, cancelación u oposición de datos personales;
VII. no se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia;
VIII. se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;
IX. el titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;
X. se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;
XI. no se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y
XII. en los demás casos que dispongan las leyes.

Como se observa, el recurso de revisión está dirigido fundamentalmente a salvaguardar la capacidad de autodeterminación informativa de las personas a través del ejercicio de sus derechos ARCO y, de manera extensiva y dudosa, dada una omisión legislativa que se ha pretendido subsanar a través de lineamientos, del derecho a la portabilidad de los datos personales.[1701] En ese sentido, la procedencia de este recurso está sujeta a que se hayan agotado previamente ante los sujetos obligados los procedimientos establecidos por la ley para dotar a los individuos de cierta capacidad de control y disposición sobre los datos personales que les conciernen.

Ello explica que, en términos del artículo 103 de la LGPDPPSO, el plazo para la interposición de este recurso sea de 15 días contados a partir del siguiente a la fecha de notificación de la respuesta del sujeto obligado recurrido, o bien, una vez que han transcurrido los plazos para que dé respuesta a la solicitud del peticionario para el ejercicio de los derechos ARCO. Además, el escrito de interposición del recurso puede presentarse indistin-

1700 Artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

1701 A pesar de que el artículo 24 del "Acuerdo mediante el cual se aprueben los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales" emitido por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y publicado en el *Diario Oficial de la Federación* el 12 de febrero de 2018 contempla el recurso de revisión como medio de impugnación ante la vulneración de la portabilidad de datos personales, lo cierto es que este supuesto no consta explícitamente en la Ley y, lo que es más, los requisitos para la interposición del recurso solo hacen referencia al procedimiento para el ejercicio de los derechos ARCO, como se observa en el artículo 105 de la LGPDPPSO. No obstante, algunas causales de procedencia del recurso de revisión pueden materializarse en el procedimiento establecido para el derecho a la portabilidad de datos personales, por ejemplo, aquellas que se refieren a la declaración de inexistencia de la información o que los datos se entreguen incompletos, pero ello no abarca integralmente algunas otras cuestiones que podrían generar una afectación a los titulares de datos personales en el ejercicio de este derecho, por ejemplo, en lo relativo a la transmisión de los datos personales en formatos interoperables con otros sistemas informáticos y que permitan la reutilización de los datos personales.

tamente ante la unidad de transparencia del responsable que ha conocido de la solicitud para el ejercicio de los derechos ARCO, o bien, ante los órganos garantes del derecho a la protección de datos personales que correspondan de acuerdo con la propia naturaleza del sujeto obligado, quienes serán los encargados de substanciar y resolver el recurso de revisión en cuestión siguiendo, para ello todas las garantías del debido proceso y las formalidades esenciales del procedimiento.

Si bien, por regla general las autoridades resolutoras de los recursos de revisión son los órganos garantes, sea el INAI en el ámbito federal o los institutos estatales que correspondan en el ámbito de su competencia, la CPEUM establece dos casos de excepción: (1) el primero referido a la facultad de atracción del INAI respecto de aquellos recursos de revisión que por su interés y trascendencia así lo justifiquen y (2) el segundo, relativo a los asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación (SCJN), cuya resolución quedará a cargo de un comité conformado por tres ministros.

En el primer supuesto, el INAI tiene facultades para atraer, sea de oficio o a solicitud del órgano garante especializado, a quien corresponda la competencia originaria, aquellos casos que por su "relevancia, novedad o complejidad", o bien, porque "su resolución podrá repercutir de manera sustancial en la solución de casos futuros para garantizar la tutela efectiva del derecho de protección de datos personales en posesión de sujetos obligados", así lo justifiquen.[1702] Se trata, pues, de una medida excepcional cuya procedencia depende del interés y la trascendencia del caso y siempre que el recurso de revisión implicado aún no haya sido resuelto por el órgano garante competente en origen.

El segundo hace referencia a un régimen especial que le atribuye facultades a un comité (especializado) integrado por tres ministros, para conocer, a través del recurso de revisión, aquellos asuntos de carácter jurisdiccional que le corresponden a la SCJN. De tal forma que el conocimiento y resolución de las impugnaciones que se formulen respecto de las decisiones o actuaciones de la SCJN, en su carácter de sujeto obligado, quedan excluidas del ámbito de competencia del INAI, siempre que hagan referencia a cuestiones del orden jurisdiccional. De tal forma que, en este caso excepcional, el recurso de revisión se constituye en un medio de impugnación en el que se identifica en un mismo ente público, aunque con diferencia entre sus unidades o componentes, la parte recurrida y resolutoria.

Al respecto, este alto tribunal ha sostenido que "se entenderá por información de asuntos jurisdiccionales aquella que se encuentre en posesión de la SCJN y tenga relación directa o indirecta con los asuntos que son competencia del Pleno, sus salas o la presidencia, de conformidad con la Ley Orgánica del Poder Judicial de la Federación y las leyes aplicables".[1703]

Cabe advertir que aún en estos supuestos de excepción, el procedimiento para el seguimiento y la resolución de los recursos de revisión previsto por la LGPDPPSO es el mismo y cuenta con las garantías del debido proceso y las formalidades esenciales de cualquier procedimiento seguido en forma de juicio, esto es, "1) la notificación del inicio del procedimiento y sus consecuencias; 2) la oportunidad de ofrecer y desahogar las pruebas en que se finque la defensa; 3) la oportunidad de alegar y 4) el dictado de una resolución que dirima las cuestiones debatidas".[1704]

1702 Artículo 131 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 27 de enero de 2017.

1703 "Acuerdo del Comité Especializado de Ministros relativo a la sustanciación de los recursos de revisión en materia de datos personales en el ámbito de la Suprema Corte de Justicia de la Nación", publicado en el *Diario Oficial de la Federación* el 2 de noviembre de 2017.

1704 "FORMALIDADES ESENCIALES DEL PROCEDIMIENTO. SON LAS QUE GARANTIZAN UNA ADECUADA Y OPORTUNA DEFENSA PREVIA AL ACTO PRIVATIVO". Suprema Corte de Justicia de la Nación (Pleno). Novena época, *Semanario Judicial de la Federación y su Gaceta*. Tomo II, diciembre de 2995. Tesis P./J. 47/95, p. 133.

En cuanto al contenido de la resolución del recurso de revisión cabe decir que ésta puede: (1) sobreseer o desechar el recurso por improcedente en los supuestos previstos por la ley; (2) confirmar la respuesta del responsable del tratamiento de los datos personales; (3) revocar o modificar la respuesta del responsable y (4) ordenar la entrega de los datos personales en caso de omisión del responsable.[1705] De tal forma que este medio de impugnación tiene por objeto confirmar, modificar o revocar el acto reclamado motivo del recurso.

Las resoluciones que en ese sentido adopten el INAI o los órganos garantes estatales, según sea el caso, serán vinculantes, definitivas e inatacables por parte de los sujetos obligados,[1706] con excepción de aquellos asuntos que pudieran representar un peligro para la seguridad nacional —resueltos por el INAI— en cuyo caso la propia LGPDPPSO establece un remedio procesal específico ante la Suprema Corte de Justicia de la Nación, del que nos ocuparemos más adelante. Ciertamente, el carácter definitivo e inatacable de las resoluciones de los órganos garantes no rivaliza con las instancias jurisdiccionales que asisten a los particulares, a través del juicio de amparo. "Tratándose de las resoluciones a los recursos de revisión de los organismos garantes de las entidades federativas", los particulares pueden optar por promover previamente ante el INAI el recurso de inconformidad previsto en la ley.[1707]

Finalmente, cabe decir que en términos del Capítulo IV del título noveno de la LGPDPPSO se establece la posibilidad de que el INAI ejerza su facultad de atracción respecto de los recursos de revisión que aún se encuentren pendientes de resolución, para aquellos casos que por su interés o trascendencia así lo justifiquen. El ejercicio de esta facultad también puede solicitarse por parte de los órganos garantes de las entidades federativas. No obstante, en cualquier caso, la decisión de atraer un determinado asunto es una facultad discrecional del Instituto.

3. Recurso de inconformidad

Este medio de impugnación, al igual que en el recurso anterior, supone la existencia de una decisión previa que conforma el acto reclamado. Solo que en este caso se trata de la revisión las resoluciones emitidas por los órganos garantes de las entidades federativas a través del recurso de revisión por parte del INAI. Al respecto, el artículo 118 de la LGPDPPSO establece que el recurso de inconformidad procederá en contra de las resoluciones emitidas por estos órganos garantes especializados que:

I. clasifiquen los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;

II. determinen la inexistencia de datos personales o

III. declaren la negativa de datos personales, es decir:

a) se entreguen datos personales incompletos;

b) se entreguen datos personales que no correspondan con los solicitados;

c) se niegue el acceso, rectificación, cancelación u oposición de datos personales;

d) se entregue o ponga a disposición datos personales en un formato incomprensible;

e) el titular se inconforme con los costos de reproducción, envió, o tiempos de entrega de los datos personales, o

1705 Artículo 111 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

1706 Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos y 115 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1707 Artículos 115 y 116 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

h) se oriente a un trámite específico que contravenga lo dispuesto por el artículo 54 de la presente Ley.

Como puede observarse, las causales de procedencia del recurso de inconformidad son similares a las que se establecen para el recurso de revisión, con excepción, naturalmente, de aquellas que se refieren específicamente a la actuación de los responsables del tratamiento de datos personales (esto es, cuando se declare su incompetencia u omita dar respuesta a una solicitud del ejercicio de los derechos ARCO en los plazos establecidos por la ley, o bien, obstaculice su ejercicio). En ese sentido, el recurso de inconformidad se constituye en una instancia adicional a favor de los titulares de datos personales para hacer efectivos sus derechos ARCO y, con ello, su capacidad de autodeterminación informativa, cuya procedencia está sujeta, además, a que se haya agotado previamente ante los órganos garantes de las entidades federativas competentes el recurso de revisión cuya resolución se pretende combatir ante el INAI.

No obstante, a pesar del valor agregado que representa para reforzar los derechos subjetivos con que cuentan los titulares de datos personales, el recurso de inconformidad se explica en la medida en que coadyuva a la realización de los objetivos planteados por la reforma constitucional del 2014, a fin de establecer estándares comunes de protección de datos personales en todo el territorio nacional. De tal forma que a través de este recurso se le otorgan facultades al INAI que exceden su ámbito competencial en el orden federal, para revisar a nivel nacional las resoluciones de los órganos garantes estatales. Todo lo cual pretende generar criterios homogéneos en el cumplimiento del derecho humano a la protección de datos personales.

El plazo de interposición del recurso de inconformidad es de 15 días contados a partir del siguiente a la fecha de la notificación de la resolución que se impugna, mismo que podrá presentarse de manera directa ante el INAI, o bien, ante el propio órgano garante de la entidad federativa que hubiere emitido la resolución, el cual deberá remitirlo al día siguiente de su recepción al Instituto.[1708]

En términos del artículo 128 de la LGPDPPSO, "corresponderá a los organismos garantes, en el ámbito de su competencia, realizar el seguimiento y vigilancia del debido cumplimiento por parte del responsable de la nueva resolución emitida como consecuencia de la inconformidad en términos de la presente Ley".

De manera similar a lo que ocurre con el recurso de revisión, las disposiciones jurídicas aplicables al recurso de inconformidad cuentan con las garantías propias del debido proceso y los elementos esenciales del procedimiento. Además, los efectos de su resolución consisten precisamente en el sobreseimiento o desechamiento del recurso ante las causales de improcedencia previstas en la ley, la confirmación, revocación o modificación de la resolución emitida por el órgano garante estatal que corresponda, o bien, la orden de entrega de la información personal en caso de que el responsable la hubiere emitido.[1709]

Finalmente cabe hacer mención de que tanto en el recurso de revisión como en el recurso de inconformidad, la LGPDPPSO prevé "la suplencia de la queja", siempre que ello no altere el contenido original del recurso interpuesto o los hechos o pretensiones aludidos por el recurrente.[1710] En ese sentido, se trata de un conjunto de atribuciones conferidas al

1708 Artículo 117 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

1709 Artículo 124 de la misma Ley.

1710 Artículos 109 y 121 de la misma Ley.

INAI o, según el caso, a los órganos garantes de las entidades federativas, "para corregir los errores o deficiencias en que incurran los reclamantes […]".[1711]

Como ha puesto de manifiesto la Suprema Corte de Justicia de la Nación, la suplencia de la queja debe operar en beneficio del quejoso o recurrente, pero su alcance debe ser acotado a aquellos casos en los que la autoridad resolutora, fundada y motivadamente, la considere útil para favorecer al beneficiado y nunca en su perjuicio.[1712] En ese sentido, "esta institución pertenece al género del principio *iura novit curia*, es decir, que el juez [y en este caso las institucionales garantes del derecho a la protección de actos personales] conoce el derecho y debe aplicarlo aun cuando las partes no lo invoquen, […]".[1713]

Además, debe tenerse presente que también en términos de la Suprema Corte de Justicia de la Nación, no resulta procedente la suplencia de la queja como medio para "suplir la deficiencia de los agravios, al punto de establecer argumentos no expuestos, ni mucho menos modificar la pretensión o los alcances de la inconformidad que la recurrente planteó en el momento procesal oportuno; es decir, dicho Instituto no tiene facultades para ir más allá de lo solicitado por la recurrente (*non ultrapetitia*) ya que esto significaría modificar el fondo de la litis contraviniendo lo dispuesto en el artículo 93 de la Ley Federal de Procedimiento Administrativo, de aplicación supletoria".[1714]

Las resoluciones que emita el INAI con motivo de los recursos de inconformidad que se le planteen son vinculantes, definitivas e inatacables para los sujetos obligados y los organismos garantes estatales. No obstante, los titulares de datos personales pueden impugnar estas resoluciones a través del juicio de amparo.[1715]

4. Recurso de revisión en materia de seguridad nacional

Este recurso constituye un "medio de defensa legal extraordinario o de carácter excepcional"[1716] previsto en el artículo 6 de la CPEUM y en el capítulo V del título noveno de la LGPDPPSO. Tiene el carácter de excepcional, en el sentido de que constituye una excepción al carácter vinculante, definitivo e inatacable de las resoluciones que emita el INAI a través del recurso de revisión por parte de los sujetos obligados. En ese sentido, el recurso de revisión en materia de seguridad nacional faculta al consejero jurídico de la Presidencia de la República para interponer un recurso de revisión en materia de seguridad nacional ante la Suprema Corte de Justicia de la Nación, "cuando considere que las resoluciones emitidas por el Instituto ponen en peligro la seguridad nacional".[1717]

De acuerdo con lo expresado por la Suprema Corte de Justicia de la Nación, este recurso de revisión "no puede suponer un medio de defensa de la legalidad de todas y cada una de

1711 Fix-Zamudio, H. (1998). Voz "suplencia de la queja", en *Diccionario Jurídico Mexicano*, 12ª. ed. UNAM. Instituto de Investigaciones Jurídicas, México, p. 3017.

1712 SUPLENCIA DE LA QUEJA DEFICIENTE. SOLO DEBE EXPRESARSE SU APLICACIÓN EN LA SENTENCIA CUANDO DERIVE EN BENEFICIO PARA EL QUEJOSO O RECURRENTE (LEY DE AMPARO VIGENTE HASTA EL 2 DE ABRIL DE 2013). Suprema Corte de Justicia de la Nación (2da. Sala). Décima época. *Semanario Judicial de la Federación y su Gaceta*. Libro 44. Tomo I, julio de 2017. Tesis 2a./J. 67/2017 (10ª.), p. 263.

1713 Fix-Zamudio, H. (1998). Voz "suplencia de la queja", en *Diccionario Jurídico Mexicano*, 12ª. ed. UNAM. Instituto de Investigaciones Jurídicas, México, p. 2703.

1714 Suprema Corte de Justicia de la Nación. Recurso de revisión en materia de seguridad nacional núm. 1/2015, sesionado el 3 de abril de 2017, p. 24.

1715 Artículo 129 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1716 Suprema Corte de Justicia de la Nación. Recurso de revisión en materia de seguridad nacional núm. 1/2015, sesionado el 3 de abril de 2017, p. 25.

1717 Artículo 139 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

las cuestiones resueltas por el INAI, como si se tratara de una segunda instancia; de ahí que, por su propia naturaleza, el recurso se limita al análisis de aquéllas determinaciones, ya sean de carácter sustantivo o adjetivo, que tengan como resultado la divulgación de cierta información que, a juicio de las autoridades responsables o sujetos obligados, pueda poner en peligro la seguridad nacional; cuestión que será resuelta de manera definitiva y con plena jurisdicción por [la]… Suprema Corte de Justicia de la Nación".[1718]

De tal forma que el recurso de revisión en materia de seguridad nacional presenta ciertas características que lo distinguen del recurso de revisión al que nos hemos referido con anterioridad, a saber: (1) la legitimación activa corresponde de manera exclusiva al consejero jurídico de la Presidencia de la República; (2) solo procede en asuntos de seguridad nacional; (3) el acto impugnado deviene de las resoluciones emitidas por el INAI, y (4) su sustanciación y resolución corresponde a la Suprema Corte de Justicia de la Nación.

Este medio de defensa legal excepcional se explica en atención al alto contenido del principio constitucional de seguridad nacional, a través del cual "se busca garantizar la integridad, estabilidad y permanencia del Estado mexicano en su territorio, estructura de gobierno y población, por lo que es dable considerar que la información relacionada con ella refleja la necesidad de establecer reservas que impidan su conocimiento público y, de esta manera, evitar que los fines del Estado se vean mermados".[1719] De tal forma que constituye un límite, tanto para el derecho de acceso a la información pública como para el derecho a la protección de datos personales. Ello, además, es consistente con lo dispuesto por el segundo párrafo del artículo 16 de la CPEUM que establece como excepción del derecho a la protección de datos personales la seguridad nacional.

El plazo para la interposición de este recurso es de siete días siguientes a aquél en el que el organismo garante notifique la resolución al sujeto obligado y la Suprema Corte de Justicia de la Nación, en atención al objeto de la litis del recurso de revisión en el que se funde y motive el peligro que supone el hecho concreto para la seguridad nacional expuesto por el peticionario, tendrá plenitud de jurisdicción para confirmar, modificar o revocar las resoluciones emitidas por el INAI.[1720]

Protección de datos personales

Isabel Davara Fernández de Marcos, Alexis Cervantes Padilla y Gregorio Barco Vega

Es el derecho humano que protege a la persona física identificada o identificable frente al tratamiento ilícito de sus datos personales, otorgándole, en la medida de lo posible dado el actual estado de la técnica, la facultad de decidir y controlar de manera libre e informada las condiciones y características del tratamiento de sus datos personales, permitiéndole, además, el ejercicio de determinados derechos y medios de tutela jurídicos para garantía y eficacia práctica de estos últimos.[1721]

1718 Suprema Corte de Justicia de la Nación. Recurso de Revisión en Materia de Seguridad Nacional núm. 1/2015, sesionado el 3 de abril de 2017, pp. 26 y 27.

1719 Cfr. Suprema Corte de Justicia de la Nación, Recurso de Revisión en Materia de Seguridad Nacional previsto en la Ley General de Transparencia y Acceso a la Información Pública núm. 1/2016, sesionado el 5 de diciembre de 2017, p. 10.

1720 Artículos 141 y 142 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

1721 En relación con la definición del derecho a la protección de datos personales en México, recomendamos consultar: Davara, I. (2016). "Protección de datos personales", en *Derechos del Pueblo Mexicano, México a través de sus constituciones*. México. Porrúa, pp. 567-581.

1. Fundamento constitucional

La protección de datos personales es un derecho humano reconocido[1722] en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) a favor de todas las personas físicas con independencia de su origen étnico o nacional, género, edad, discapacidades, condición social, condiciones de salud, religión, opiniones, preferencias sexuales, estado civil, o cualquier otro elemento que pudiera atentar contra su dignidad y/o afectar sus derechos y libertades fundamentales.[1723]

En el panorama jurídico mexicano, el derecho a la protección de datos personales es más que una simple prerrogativa de la que gozan las personas físicas, es un derecho humano cuya denominación se deriva del contenido del primer párrafo del artículo primero de la CPEUM, resultado de la histórica reforma constitucional en materia de derechos humanos del 10 de junio de 2011.[1724] Dicho artículo indica, con un alto grado de precisión, lo siguiente:

> Artículo 1o. En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece.

La redacción referida tiene sendas implicaciones jurídicas, teóricas y prácticas. Entre ellas está el establecimiento de la igualdad en la titularidad de los derechos reconocidos en el texto constitucional, una función didáctica para los justiciables y los órganos jurisdiccionales y, sobre todo, una contribución para una más clara y efectiva exigibilidad y protección de los derechos humanos ante la jurisdicción interna.[1725]

De lo anterior se desprende que el derecho a la protección de datos personales es un derecho humano y goza de la máxima protección normativa en nuestro país. El derecho humano a la protección de datos personales se reconoce particularmente en el segundo párrafo del artículo 16 constitucional que prevé lo siguiente:

> Artículo 16. Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Así, la Constitución remite a desarrollo legal el contenido práctico del derecho humano a la protección de datos personales.

1722 En lo que concierne a la expresión "derechos humanos" y de acuerdo con Miguel Carbonell, se trata de una acepción más moderna que la de garantías individuales y es la que comúnmente se usa en el ámbito del derecho internacional, que se refieren a una categoría más amplia y que, en la práctica, se suele utilizar con menos rigor jurídico que la de derechos fundamentales. Carbonell, M. (2013). "Derechos Humanos en la Constitución Mexicana", en Ferrer Mac-Gregor Poisot, Eduardo, *et al*, (Coords.), *Derechos humanos en la Constitución: Comentarios de Jurisprudencia Constitucional e Interamericana.* México. Suprema Corte de Justicia de la Nación. Coordinación de Compilación y Sistematización de Tesis: Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas/Konrad Adenauer Stiftung. Programa Estado de Derecho para Latinoamérica, p. 22.

1723 Derivado de lo dispuesto en el último párrafo del artículo 1 constitucional: queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

1724 Connotados autores como Miguel Carbonell y Pedro Salazar indican que la reforma constitucional en materia de derechos humanos, del 10 de junio de 2011, significó un nuevo paradigma para el sistema jurídico mexicano. *Vid.* Carbonell Sánchez, Miguel y Salazar Ugarte, Pedro, (coords.). (2011). *La reforma constitucional de derechos humanos: un nuevo paradigma*. México. Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas.

1725 Orozco, J. (2011, julio-diciembre). "Los derechos humanos y el nuevo artículo 1° constitucional". IUS. En *Revista del Instituto de Ciencias Jurídicas de Puebla*. México. Año V. No. 28, pp. 85-98.

2. Características

De acuerdo con las previsiones del texto constitucional, puede decirse que el derecho a la protección de datos personales es un derecho humano subjetivo, universal, inalienable, irrenunciable, intransferible, imprescriptible e indivisible,[1726] que encuentra su sustento y raíz en la propia dignidad[1727] y libertad personal.

Es, además, un derecho personalísimo que únicamente puede ser ejercido por el titular de los datos personales o, en su caso, por su representante legal debidamente acreditado para ello, según se dispone en las normatividades aplicables a los sectores público y privado.

Por último, cabe destacar su autonomía, puesto que goza de un reconocimiento específico e independiente, con regulación concreta y con características esencialmente distintas como hemos visto, tal y como lo especifica el párrafo segundo del artículo 16 de la CPEUM.

3. Objeto

La protección de datos personales es un derecho autónomo e independiente que gira en torno al individuo, es decir, a la persona física titular de esos datos personales. El objeto de este derecho es la protección del individuo frente al tratamiento ilícito de sus datos personales, y aunque se incluye cualquier tipo de tratamiento, es cierto que se presta especial atención cuando en dicho tratamiento se utilizan tecnologías de información y comunicaciones. El centro de este derecho lo constituye la persona y, por tanto, es a quien se protege frente a un posible tratamiento ilícito de su información por parte de terceros, estableciendo reglas e instituciones que tienden a velar porque el tratamiento se realice conforme a las disposiciones legales y principios jurídicamente aceptados.

En este contexto, resulta interesante lo señalado en los considerandos 1 y 2[1728] de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos). En ellos se precisa que el derecho a la protección de datos perso-

1726 En este sentido, resulta aplicable el criterio emitido por los tribunales colegiados de circuito bajo el rubro PRINCIPIOS DE UNIVERSALIDAD, INTERDEPENDENCIA, INDIVISIBILIDAD Y PROGRESIVIDAD DE LOS DERECHOS HUMANOS. EN QUÉ CONSISTEN, véase en la tesis I.4o.A.9 K (10a.). *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo I, abril de 2013, p. 2254.

1727 DIGNIDAD HUMANA. CONSTITUYE UNA NORMA JURÍDICA QUE CONSAGRA UN DERECHO FUNDAMENTAL A FAVOR DE LAS PERSONAS Y NO UNA SIMPLE DECLARACIÓN ÉTICA. La dignidad humana no se identifica ni se confunde con un precepto meramente moral sino que se proyecta en nuestro ordenamiento como un bien jurídico circunstancial al ser humano, merecedor de la más amplia protección jurídica, reconocido actualmente en los artículos 1o., último párrafo; 2o., apartado A, fracción II; 3o., fracción II, inciso c); y 25 de la Constitución Política de los Estados Unidos Mexicanos. En efecto, el Pleno de esta Suprema Corte ha sostenido que la dignidad humana funge como un principio jurídico que permea en todo el ordenamiento, pero también como un derecho fundamental que debe ser respetado en todo caso, cuya importancia resalta al ser la base y condición para el disfrute de los demás derechos y el desarrollo integral de la personalidad. Así las cosas, la dignidad humana no es una simple declaración ética, sino que se trata de una norma jurídica que consagra un derecho fundamental a favor de la persona y por el cual se establece el mandato constitucional a todas las autoridades, e incluso particulares, de respetar y proteger la dignidad de todo individuo, entendida ésta —en su núcleo más esencial— como el interés inherente a toda persona, por el mero hecho de serlo, a ser tratada como tal y no como un objeto, a no ser humillada, degradada, envilecida o cosificada.(Tesis: 1a. CCCLIV/2014 10a.).

1728 (1) Considerando que la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental que se encuentra reconocido con rango máximo en la mayoría de las constituciones políticas de los Estados iberoamericanos, bajo la forma del derecho a la protección de datos personales o habeas data, y que en algunos casos ha sido definido jurisprudencialmente por sus tribunales o cortes constitucionales.
(2) Determinando que el derecho a la protección de datos personales se ha conceptualizado en algunos países iberoamericanos, legislativamente o jurisprudencialmente, como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámica propias, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

nales es un derecho fundamental que se ha conceptualizado en algunos países iberoamericanos —legislativa o jurisprudencialmente— como un derecho de naturaleza distinta a los derechos a la vida privada y familiar, a la intimidad, al honor, al buen nombre y otros derechos similares, como lo habíamos señalado en el apartado anterior, que en su conjunto garantizan el libre desarrollo de la personalidad de la persona física, hasta conformarse en un derecho autónomo, con características y dinámica propias, que tiene por objeto salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las TIC que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana.

De esta forma, el objeto de este derecho es dotar al titular de los datos personales de un poder de disposición y control, en la medida de lo posible, sobre sus datos personales y facultar a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, y determinar cuáles datos puede recabar. Asimismo, también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.[1729] Si bien, las actuales técnicas de tratamiento de datos personales ponen en cuestión la posibilidad de que el principio de autodeterminación informativa se pueda aplicar en su totalidad, lo cierto es que el espíritu del mismo debe defenderse y procurar que el titular tenga el mayor control posible sobre su información personal o, cuando menos, el mayor acceso a la información y la transparencia sobre el tratamiento.

4. Relevancia del derecho a la protección de datos personales

El derecho a la protección de datos personales tiene una indiscutible relevancia, pues aunque su importancia a veces pasa desapercibida, no se trata de un derecho humano (o fundamental) por capricho del legislador (no solo nacional sino internacional), sino que se trata de un derecho humano constitucionalmente reconocido que entronca directamente con la dignidad[1730] humana y la libertad[1731] de la persona,[1732] y su relevancia, histórica, presente y futura es indiscutible, aunque a veces sea bastante desconocida o minusvalorada.

Cada vez más, mediante el tratamiento de nuestra información personal, se nos puede llegar a controlar por terceros, impidiéndonos desarrollar nuestra vida normal, atentando contra nuestra libertad y dignidad como personas. El titular de los datos corre peligro de convertirse en un ciudadano de vidrio, transparente a los ojos de todos.[1733]

También es cierto que en muchas ocasiones puede encontrarse vinculado, a pesar de su autonomía e independencia, a otros conceptos y derechos de naturaleza afín pero esencialmente distintos, como son la intimidad, la vida privada, el derecho al honor, el dere-

1729 Sentencia 292/2000, del 30 de noviembre de 2000, del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal.

1730 Por ejemplo, en el considerando 4 de la Decisión del Supervisor Europeo de Protección de Datos de 3 de diciembre de 2015 por la que se establece un grupo consultivo externo sobre las dimensiones éticas de la protección de datos (el Grupo Consultivo sobre Ética) se ha señalado lo siguiente:
(4) La evolución tecnológica, como la computación de datos masivos y el aprendizaje automático, permite la recopilación y la utilización de datos personales en términos cada vez más opacos y complejos, planteando de este modo amenazas significativas para la intimidad y la dignidad humana.

1731 Y así señala el artículo 1 de la CPEUM (reformado mediante decreto publicado en el *Diario Oficial de la Federación* el 10 de junio de 2011) y el artículo 1 de la Carta Europea de Derechos Humanos.

1732 Davara Abogados. (2017, septiembre). "Cómo garantizar la protección de los datos personales, Guía Auxiliar para diagnosticar y cumplir con la legislación en la materia al interior de una organización", en *Revista IDC Asesor Jurídico y Fiscal*, México. p. 1.

1733 Rodotà indica que "el hombre de vidrio es una metáfora nazi, que refleja la idea de un Estado que puede adueñarse por entero de la vida de las personas, que frente a sí no tiene ciudadanos, sino súbditos". *Vid.* Rodotà, S. (2003 mayo-diciembre). "Democracia y protección de datos", en *Cuadernos de Derecho Público*, Madrid. INAP. Números 19-20.

cho a la propia imagen y la dignidad humana. Para un estudio detallado de los conceptos aludidos, recomendamos consultar cada una de las definiciones correspondientes en el presente diccionario. En la práctica, además, se concreta en un derecho ambivalente que, por un lado representa un derecho humano y, por el otro, una obligación de los particulares y/o administraciones públicas que dan tratamiento a los datos personales.[1734]

Como decíamos, la no observancia de las obligaciones legales impuestas puede dar lugar a la actualización de infracciones legales y la consecuente imposición de sanciones. Además, su importancia se vincula directamente con la confianza que el titular deposita en quien trata sus datos personales y con la reputación como activo intangible de gran valor vinculado directamente con el valor del negocio en el mercado (o con la reputación de la administración competente), que toma tiempo y esfuerzo construir y que, una vez afectado, es difícil restaurarlo y en consecuencia, la garantía de la privacidad supone un elemento clave para obtener la confianza del cliente o administrado.[1735]

Así, desde el ámbito de la protección de datos personales en posesión de particulares donde se desarrollan múltiples actividades relacionadas con el tratamiento de datos personales, el respeto a la privacidad no debe ser visto como un obstáculo para lograr operaciones comerciales, sino como un aliado para fomentar la confianza en el comercio y una oportunidad de negocio para las empresas.[1736] Del lado de las administraciones públicas, este derecho no puede subestimarse, pues las actividades públicas también están sujetas al cumplimiento de la normatividad en materia de protección de datos personales y al escrutinio de los administrados.

5. Contenido esencial

La normatividad de desarrollo de los sectores público, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y privado, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y la normatividad de desarrollo de las mismas, configuran un conjunto de principios y deberes para el que trata los datos (principios: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; y deberes: seguridad y confidencialidad), unos derechos para los titulares (acceder a sus datos, solicitar su rectificación en caso de que sean inadecuados o excesivos, pedir su cancelación, y manifestar su oposición al tratamiento, esto es, el famoso acrónimo ARCO, añadiéndose en la normatividad del sector público el derecho a la portabilidad), y unas garantías de protección en caso de que esos derechos se vean infringidos o el tratamiento de los datos personales haya incurrido en algún otro tipo de violación (función de tutela que en la actualidad desempeña en México el INAI[1737] y los organismos garantes locales).

1734 Barco, G. (2016). "El derecho humano a la protección de datos personales en México. Actas del III Coloquio Internacional de Investigadores en Derecho", en *Revista Jurídica de la Universidad de León*. España. Núm. 3, p. 145.

1735 Davara Abogados. (2017, septiembre). "Cómo garantizar la protección de los datos personales, Guía Auxiliar para diagnosticar y cumplir con la legislación en la materia al interior de una organización", en *Revista IDC Asesor Jurídico y Fiscal*, México. p. 2

1736 Davara Abogados. (2017, abril). "El mundo del comercio electrónico bajo la Ley", en *Revista IDC Asesor Jurídico y Fiscal.* México, p. 55.

1737 La reforma constitucional al artículo 6 logró, entre otras cosas, que el Instituto Federal de Acceso a la Información y Protección de Datos (ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) transitara de ser un organismo descentralizado a un órgano constitucional autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propios y responsable de garantizar el cumplimiento del derecho a la protección de datos personales. En caso de que se vulnere algún principio o deber, o que el titular entienda que no se atendieron sus derechos, el Instituto Nacional de Acceso a la Información y Protección de datos (INAI) puede actuar de oficio o a petición de parte, para lo que tiene establecidos unos procedimientos por ley (en la LFPDPPP y normatividad de desarrollo), que son los procedimientos de verificación, protección de derechos e imposición de sanciones.

En cuanto al contenido y alcances del derecho, cabe resaltar la emblemática sentencia 292/2000 del Tribunal Constitucional Español,[1738] donde indicó que el contenido del derecho a la protección de datos personales se concreta en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero —sea el Estado o un particular— así como cuales puede recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. De esta manera destaca el citado órgano jurisdiccional, dichos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la atribución a su titular de un haz de facultades consistente en diversos poderes jurídicos, como la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero —sea el Estado o un particular— a los que les impone ciertos deberes jurídicos en consecuencia.[1739]

Como señalábamos, el componente fundamental de este derecho es la dignidad de la personal, pues ésta se perfila como el origen, la esencia y el fin de todos los derechos humanos,[1740] y representa un valor supremo[1741] establecido en el artículo 1 de la CPEUM, en virtud del cual se reconoce una calidad única y excepcional a todo ser humano[1742] por el simple hecho de serlo, cuya plena eficacia debe ser respetada y protegida integralmente sin excepción alguna.[1743]

Así, la dignidad humana no solo es un derecho en sí mismo, sino la base para otros derechos y libertades entre los que está el derecho a la protección de datos.

1738 Tribunal Constitucional Español, sentencia 292/2000, del 30 de noviembre de 2001.

1739 En este contexto, el fundamento séptimo de la sentencia 292/2000 indica:

7. De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

1740 Tesis I.5o.C. J/30 (9a.). *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo III, octubre de 2011, p. 1528. *Vid*, también, Fundamentación de la metafísica de las costumbres, de Emmanuel Kant, donde se reitera que el hombre siempre es un fin en sí mismo y no un medio.

1741 La Suprema Corte de Justicia de la Nación ha señalado que la dignidad humana funge como "un principio jurídico que permea en todo el ordenamiento, pero también como un derecho fundamental que debe ser respetado en todo caso, cuya importancia resalta al ser la base y condición para el disfrute de los demás derechos y el desarrollo integral de la personalidad. Así las cosas, la dignidad humana no es una simple declaración ética, sino que se trata de una norma jurídica que consagra un derecho fundamental a favor de la persona y por el cual se establece el mandato constitucional a todas las autoridades, e incluso particulares, de respetar y proteger la dignidad de todo individuo, entendida ésta —en su núcleo más esencial— como el interés inherente a toda persona, por el mero hecho de serlo, a ser tratada como tal y no como un objeto, a no ser humillada, degradada, envilecida o cosificada". Vid Tesis 1a. CCCLIV/2014 (10ª.), *Gaceta del Semanario Judicial de la Federación*, Décima época, tomo I, octubre de 2014, p. 602.

1742 De acuerdo con lo anterior, se reconoce que "en el ser humano hay una dignidad que debe ser respetada en todo caso, constituyéndose como un derecho absolutamente fundamental, base y condición de todos los demás, el derecho a ser reconocido y a vivir en y con la dignidad de la persona humana, y del cual se desprenden todos los demás derechos, en cuanto son necesarios para que los individuos desarrollen integralmente su personalidad, dentro de los que se encuentran, entre otros, el derecho a la vida, a la integridad física y psíquica, al honor, a la privacidad, al nombre, a la propia imagen, al libre desarrollo de la personalidad, al estado civil y el propio derecho a la dignidad personal". *Vid.* Tesis P. LXV/2009. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XXX, diciembre de 2009, p. 8.

1743 Tesis I.5o.C. J/31.9a.), *Semanario Judicial de la Federación y su Gaceta*, Décima época, t. III, octubre de 2011, p. 1529.

El Supervisor Europeo de Protección de Datos (SEPD) destaca la relevancia del derecho a la protección de datos personales para proteger la dignidad de la persona:

> Los derechos fundamentales a la intimidad y a la protección de los datos personales se han vuelto más importantes que nunca para la protección de la dignidad humana. Dichos derechos están consagrados en los tratados de la UE y en la Carta de Derechos Fundamentales de la UE. Permite a las personas físicas que desarrollen sus propias personalidades, lleven a cabo vidas independientes, innoven y ejerzan sus derechos y libertades. Los principios de protección de datos definidos en la Carta de la UE (necesidad, proporcionalidad, imparcialidad, minimización de los datos, limitación a una finalidad específica, consentimiento y transparencia) se aplican al tratamiento de datos en su integridad, tanto respecto a la recopilación como a su uso.[1744]

En resumen, cabe decir que el derecho a la protección de datos personales en México:

a) es un derecho humano según la definición del artículo 1 de la CPEUM;
b) está reconocido en el artículo 16 de la CPEUM;
c) está basado en la dignidad[1745] y libertad humana;
d) es universal, inalienable, irrenunciable, intransferible, imprescriptible e indivisible;[1746]
e) otorga a las personas físicas (titulares) la más amplia protección legal sobre sus datos personales sometidos a cualquier tipo de tratamiento al que pudieran ser sometidos, ya sea por un sujeto de derecho público o de derecho privado y
f) permite a las personas decidir, de manera libre e informada, sobre el uso y destino de sus datos personales en posesión del responsable.

1744 *Vid* Resumen ejecutivo del dictamen 4/2015 del Supervisor Europeo de Protección de Datos. *Hacia una nueva ética digital: datos, dignidad y tecnología.*

1745 DIGNIDAD HUMANA. CONSTITUYE UNA NORMA JURÍDICA QUE CONSAGRA UN DERECHO FUNDAMENTAL A FAVOR DE LAS PERSONAS Y NO UNA SIMPLE DECLARACIÓN ÉTICA. La dignidad humana no se identifica ni se confunde con un precepto meramente moral sino que se proyecta en nuestro ordenamiento como un bien jurídico circunstancial al ser humano, merecedor de la más amplia protección jurídica, reconocido actualmente en los artículos 1o., último párrafo; 2o., apartado A, fracción II; 3o., fracción II, inciso c); y 25 de la Constitución Política de los Estados Unidos Mexicanos. En efecto, el Pleno de esta Suprema Corte ha sostenido que la dignidad humana funge como un principio jurídico que permea en todo el ordenamiento, pero también como un derecho fundamental que debe ser respetado en todo caso, cuya importancia resalta al ser la base y condición para el disfrute de los demás derechos y el desarrollo integral de la personalidad. Así las cosas, la dignidad humana no es una simple declaración ética, sino que se trata de una norma jurídica que consagra un derecho fundamental a favor de la persona y por el cual se establece el mandato constitucional a todas las autoridades, e incluso particulares, de respetar y proteger la dignidad de todo individuo, entendida ésta —en su núcleo más esencial— como el interés inherente a toda persona, por el mero hecho de serlo, a ser tratada como tal y no como un objeto, a no ser humillada, degradada, envilecida o cosificada.(*Vid* Tesis: 1a. CCCLIV/2014 10a.)

1746 En este sentido, resulta aplicable el criterio emitido por los tribunales colegiados de circuito bajo el rubro PRINCIPIOS DE UNIVERSALIDAD, INTERDEPENDENCIA, INDIVISIBILIDAD Y PROGRESIVIDAD DE LOS DERECHOS HUMANOS. EN QUÉ CONSISTEN, *véase* en la Tesis I.4o.A.9 K (10a.). *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo I, abril de 2013, p. 2254

Protección de datos por defecto

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La protección de datos personales por defecto consiste en la obligación del responsable de aplicar medidas técnicas y organizativas apropiadas y orientadas a garantizar que, por defecto, esto es, por configuración ya previamente establecida del tratamiento, solo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento, con independencia de la cantidad de datos personales recabados, el alcance del tratamiento, o el plazo de conservación, entre otros factores que se consideren relevantes por parte del responsable.

Desde la perspectiva jurídica,[1747] el concepto de protección de datos por defecto resulta de la concreción práctica del principio de responsabilidad y como una medida necesaria para su adecuado cumplimiento.[1748] El principio de responsabilidad conmina a los responsables de tratamiento a implementar los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones, así como a rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control.[1749]

Como parte de las medidas admisibles para el cumplimiento del citado principio, los responsables deben garantizar que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, deberes, derechos y demás obligaciones previstas en la normatividad de datos personales que resulte aplicable.[1750]

El enfoque de protección de datos personales por defecto no aparece explícitamente regulado en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) ni en su Reglamento. No obstante, dicha situación no representa un impedimento para que este enfoque pueda ser adoptado por las organizaciones para cumplir de forma proactiva y responsable con el principio de responsabilidad y demostrar el efectivo cumplimiento de la normatividad. En cambio, en el sector público, sí aparecen varias y diversas referencias:

a) La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) precisa, en la fracción VIII de su artículo 30, que entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad, debe considerarse garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.[1751]

b) El primer párrafo del artículo 52 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) indica que para dar cumplimiento a las disposiciones de la LGPDPPSO, en particular a la fracción

1747 Ver definición de principio de responsabilidad en este diccionario.

1748 Artículo 14 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1749 Artículo 20.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1750 Artículo 38.2 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1751 Artículo 39, fracción VIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

VIII de su artículo 30, "el responsable deberá aplicar medidas técnicas y organizativas apropiadas y orientadas a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento". Es decir, este ordenamiento obliga a dar cumplimiento al principio de proporcionalidad y al criterio de minimización con el objetivo de que exclusivamente se traten los datos personales que resulten necesarios, adecuados y relevantes para los fines perseguidos por el responsable y que no puedan tratarse datos personales que resulten excesivos o que no sean requeridos para cumplir las finalidades del tratamiento informadas por el responsable al titular (principios de calidad y finalidad).

c) El segundo párrafo del artículo 52 de los Lineamientos Generales establece que la obligación de aplicar las medidas de protección de datos por defecto es aplicable, a título enunciativo,[1752] a la cantidad de datos personales recabados, al alcance del tratamiento, el plazo de conservación de los datos personales, entre otros factores que se juzguen relevantes por el responsable.

Por su parte, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos), en su artículo 38.2, establecen la obligación de los responsables (sean entidades públicas o privadas) de adoptar el enfoque de protección de datos por defecto. Así, en el citado artículo se previene que los responsables deben garantizar que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado iberoamericano que le resulte aplicable. Además, se resalta que esta práctica es fundamental para de garantizar que exclusivamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos a un número indeterminado de personas.[1753]

En este contexto, el Reglamento General de Protección de Datos Europeo (en adelante RGPD) instruye la obligación de los responsables de cumplir con el enfoque de protección de datos personales por defecto[1754] al señalar que el responsable del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.[1755]

El Reglamento General de Protección de Datos (RGPD o GDPR por sus siglas en inglés) específica también que dicha obligación se aplicará a la cantidad de datos personales recogi-

1752 Lo que quiere decir que además de ésta se pueden acompañar otras medidas proactivas que el responsable considere.

1753 Artículo 38.2 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1754 El considerando 78 del Reglamento General de Protección de Datos Personales prevé:
(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento y al responsable crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

1755 Artículo 25, apartado segundo del Reglamento General de Protección de Datos.

dos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.[1756] Bajo dicho esquema normativo, el RGPD obliga a garantizar que, por defecto, los datos personales no sean accesibles sin la intervención de la persona, a un número indeterminado de personas físicas. Con esta práctica, además, se garantiza la confidencialidad y seguridad de los datos personales aspara evitar intromisiones por parte de terceros.[1757] En definitiva, como decíamos, en el enfoque de protección de datos personales por defecto se concibe como una obligación del responsable la aplicación de medidas técnicas y organizativas apropiadas para que desde la configuración inicial del tratamiento solo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento con independencia de la cantidad de datos personales recabados, su alcance, el plazo de conservación, entre otros factores relevantes para el responsable.

Protección de datos personales por diseño

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La protección de datos personales por diseño consiste en la obligación de las empresas u organizaciones responsables del tratamiento de los datos personales a aplicar medidas de carácter administrativo, técnico y/o físico apropiadas en las primeras fases del diseño de las operaciones del tratamiento, de forma que se garanticen los derechos de los titulares y la aplicación de los principios y deberes de protección de datos, considerando factores como los avances tecnológicos, los costes de implementación, la naturaleza, el ámbito, los fines del tratamiento de los datos personales, el contexto, los riesgos de diversa probabilidad y gravedad que entraña para el derecho a la protección de datos personales de los titulares, entre otros.

El concepto "protección de datos personales por diseño" tiene muchas coincidencias con el de "privacidad por diseño"[1758] y es a partir de este último que procedemos a explicarlo.

El término "privacidad por diseño" también es conocido como *"privacy by design"* (PbD por sus siglas en inglés), fue acuñado por Ann Cavoukian cuando era comisionada de Información y Privacidad de la provincia de Ontario en Canadá en los noventa, para atender los efectos crecientes y sistemáticos del uso de las Tecnologías de la Información y la Comunicación (TIC), y de los sistemas de datos en red a gran escala.[1759]

La noción de privacidad por diseño no es unívoca, pues es concebida tanto como una filosofía como un enfoque, a partir del cual la privacidad se integra en el diseño tecnológico, siendo consistente con la arquitectura del sistema de información y el propio modelo de negocios.[1760]

1756 Artículo 25, apartado segundo del Reglamento General de Protección de Datos.

1757 Artículo 25, apartado segundo del Reglamento General de Protección de Datos.

1758 El término de protección de datos personales por defecto ha sido recientemente acuñado en diversas normativas de datos personales como el Reglamento General de Protección de Datos europeo, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos y los Lineamientos Generales de Protección de Datos Personales para el Sector Público en nuestro país. Sin embargo, de forma previa, el concepto de "privacidad por diseño" ya se había instaurado en la práctica a partir de las aportaciones de Ann Cavoukian, entonces comisionada de Información y Privacidad de la provincia de Ontario en Canadá.

1759 Cavoukian A. (s.f.). *Privacidad por Diseño. Los 7 principios fundamentales.* Fecha de consulta: 13 de noviembre de 2018. Disponible en: https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%CC%83o-1.pdf

1760 Brian, A. (2012. julio-diciembre). "La protección inteligente de los datos personales", en *Revista Internacional de Protección de Datos Personales.* Universidad de los Andes. Facultad de Derecho, No. 1. Colombia, p. 8. Disponible en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf Fecha de consulta: 13 de noviembre de 2018.

De acuerdo con su creadora, este concepto promueve la visión de que el futuro de la privacidad no puede ser garantizado solo por cumplir con los marcos regulatorios, sino que, idealmente, el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización.[1761]

En la práctica, el principio de privacidad por diseño se despliega en una trilogía de aplicaciones que incluye a los sistemas de tecnologías de la información, prácticas de negocio responsable y el diseño físico e infraestructura en red.[1762] Es decir, se trata de un principio que se aplica a multitud de esquemas de tratamiento de datos personales y que se extiende a todos los tipos de información personal.[1763]

De esta forma, se ha admitido que el concepto de privacidad por diseño como lo conocemos se sustenta en los siguientes siete principios fundamentales:

1. Proactivo, no reactivo; preventivo no correctivo: de acuerdo con su autora, este primer principio refiere que el enfoque de privacidad por diseño está caracterizado por medidas proactivas, en vez de reactivas. Es decir, anticipa y previene eventos de invasión de privacidad antes de que estos ocurran. El enfoque de privacidad por diseño no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron, puesto que su finalidad es prevenir que ocurran.
2. Privacidad como la configuración predeterminada: a partir de este principio se busca entregar el máximo grado de privacidad, asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema de tecnologías de la información o en cualquier práctica de negocios. Es decir, si la persona no toma una acción, aun así, la privacidad se mantiene intacta. No se requiere acción alguna de parte de la persona para proteger la privacidad, ésta se encuentra interconstruida en el sistema, como una configuración predeterminada.
3. Privacidad incrustada en el diseño: en función de este principio se preceptúa que la privacidad está incrustada en el diseño y la arquitectura de los sistemas de tecnologías de información y en las prácticas de negocios. Es decir, la privacidad se convierte en un componente esencial de la funcionalidad central que está siendo entregada y es parte integral del sistema, sin disminuir su funcionalidad.
4. Funcionalidad total —"todos ganan", no "si alguien gana, otro pierde": el esquema de privacidad por diseño intenta acomodar todos los intereses y objetivos legítimos en una forma "ganar-ganar", no a través de un método anticuado de "si alguien gana, otro pierde", donde se realizan concesiones innecesarias. El citado enfoque, evita la hipocresía de las falsas dualidades, tales como privacidad vs. seguridad, demostrando que sí es posible tener ambas al mismo tiempo.
5. Seguridad extremo a extremo —protección del ciclo de vida completo: conforme a este principio el enfoque de privacidad por diseño se extiende con seguridad a través del ciclo de vida completo de los datos involucrados —las medidas de seguridad robustas son esenciales para la privacidad de inicio a fin. Esto garantiza que todos los datos son retenidos con seguridad y luego destruidos con seguridad al final del proceso, sin demoras. Por lo tanto, la privacidad por diseño garantiza una administración segura del ciclo de vida de la información.

1761 Cavoukian A. (s.f.). Privacidad por Diseño. Los 7 principios fundamentales. Fecha de consulta: 13 de noviembre de 2018. Disponible en: https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%CC%83o-1.pdf.

1762 Cavoukian A. (s.f.). *Privacidad por Diseño. Los 7 principios fundamentales.*

1763 Cavoukian A. (s.f.). *Privacidad por Diseño. Los 7 principios fundamentales*, a partir de aquí el autor basa su estudio en *Los 7 principios fundamentales de Cavoukian.*

6. Visibilidad y transparencia —mantenerlo abierto: este principio pretende asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, ésta en realidad esté operando de acuerdo con las promesas y objetivos declarados, sujeta a verificación independiente. Sus partes componentes y operaciones permanecen visibles y transparentes a usuarios y a proveedores.
7. Respeto por la privacidad de los usuarios —mantener un enfoque centrado en el usuario: según este principio, la privacidad por diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada, y facultando opciones amigables para el usuario. Es decir, se requiere mantener al usuario en el centro de las prioridades.

La adopción del enfoque de privacidad por diseño implica la posibilidad de asegurar que las personas dispongan del control de la información que les concierne (una manifestación concreta, a través de herramientas tecnológicas, del derecho a la autodeterminación informativa) y las organizaciones obtengan una ventaja competitiva sostenible.

Desde la perspectiva jurídica, el concepto de protección de datos por diseño, al igual que el de protección de datos por defecto —plasmado en nuestra normatividad y con el que ya hemos dicho guarda muchas similitudes—, resulta de la concreción práctica del principio de responsabilidad.[1764] En síntesis, dicho principio[1765] conmina a los responsables de tratamiento a implementar los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones, así como rendir cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control.[1766]

Como parte de las medidas admisibles para el cumplimiento del citado principio, los responsables pueden hacer uso de técnicas que permitan acreditar que la protección de datos personales se ha establecido de forma previa al diseño de una determinada operación de tratamiento de datos personales.

El enfoque de protección de datos personales por diseño, como dijimos, no aparece explícitamente regulado en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) ni en su reglamento. No obstante, ello no es obstáculo para que pueda ser adoptado por las organizaciones para cumplir de forma proactiva y responsable con el principio de responsabilidad y demostrar el efectivo cumplimiento de la normatividad.

En cambio, en el sector público sí aparecen varias y diversas referencias:

a) La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) precisa, en la fracción VIII de su artículo 30, que entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad, debe considerarse garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que

1764 Ver definición de "principio de responsabilidad" en este diccionario.

1765 Artículo 14 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y artículo 29 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1766 20.1. El responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los presentes estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines.

implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la LGPDPPSO y las demás que resulten aplicables en la materia.[1767]

b) El primer párrafo del artículo 52 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) indica que para dar cumplimiento a las disposiciones de la LGPDPPSO, en particular a la fracción VIII de su artículo 30, "el responsable deberá aplicar medidas técnicas y organizativas apropiadas y orientadas a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales estrictamente necesarios para cada uno de los fines específicos del tratamiento". Es decir, este ordenamiento obliga a dar cumplimiento al principio de proporcionalidad y al criterio de minimización con el objetivo de que exclusivamente se traten los datos personales que resulten necesarios, adecuados y relevantes para los fines perseguidos por el responsable y que no puedan tratarse datos personales que resulten excesivos o que no sean requeridos para cumplir las finalidades del tratamiento informadas por el responsable al titular (principios de calidad y finalidad).

c) El segundo párrafo del artículo 52 de los Lineamientos Generales establece que la obligación de aplicar las medidas de protección de datos por defecto es aplicable, a título enunciativo,[1768] a la cantidad de datos personales recabados, al alcance del tratamiento, el plazo de conservación de los datos personales, entre otros factores que se juzguen relevantes por el responsable.

Por su parte, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) en su artículo 38.2 establecen la obligación de los responsables (sean entidades públicas o privadas) de adoptar el enfoque de protección de datos por defecto. Así, en el citado artículo se previene que los responsables deben garantizar que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado iberoamericano que le resulte aplicable. Además, se resalta que esta práctica es fundamental para de garantizar que exclusivamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de éstos a un número indeterminado de personas.[1769]

En este contexto, el Reglamento General de Protección de Datos Europeo (RGPD o GDPR por sus siglas en inglés) instruye la obligación de los responsables de cumplir con el enfoque de protección de datos personales por defecto[1770] al señalar que el responsable

1767 Artículo 39, fracción VIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

1768 Lo que quiere decir que además de ésta se pueden acompañar otras medidas proactivas que el responsable considere.

1769 Artículo 38.2 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

1770 El Considerando 78 del Reglamento General de Protección de Datos Personales prevé:
(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones

del tratamiento debe aplicar las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.[1771]

El RGPD específica también que dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.[1772]

Bajo dicho esquema normativo, el RGPD obliga a garantizar que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. Con esta práctica, además, se garantiza la confidencialidad y seguridad de los datos personales aspara evitar intromisiones por parte de terceros.[1773]

En definitiva, el enfoque de protección de datos personales desde el diseño se traduce como una obligación de los responsables del tratamiento de aplicar medidas de carácter físico técnico y administrativo de forma previa a la confección productos, servicios y aplicaciones que impliquen un tratamiento de datos personales con el ánimo de garantizar el derecho a la protección de datos personales de los titulares.

Procedimiento de Imposición de Sanciones (Pisan)

Gabriel López Lopez

Es un procedimiento administrativo sancionador por virtud del cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), a través de su unidad administrativa competente, ante la presunción de la existencia de conductas que podrían constituir una infracción a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), impone las sanciones establecidas en la ley de la materia.

La fracción XVIII del artículo 3 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación y de Imposición de Sanciones (Lineamientos de Procedimiento) establece que para efectos de los referidos lineamientos deberá entenderse por procedimiento de imposición de sanciones (Pisan) al conjunto de actos por los cuales el INAI, a través de la Dirección General de Protección de Derechos y Sanción, en caso de presunción de incumplimiento de alguno de los principios o disposiciones de la LFPDPPP, que el Pleno previamente determine en los procedimientos de protección de derechos o verificación, impone la o las sanciones que correspondan.[1774]

de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

1771 Artículo 25, apartado segundo del Reglamento General de Protección de Datos.

1772 Artículo 25, apartado segundo del Reglamento General de Protección de Datos.

1773 Artículo 25, apartado segundo del Reglamento General de Protección de Datos.

1774 Artículo 3. Además de las definiciones establecidas en los artículos 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 2 de su Reglamento, para los efectos de los presentes Lineamientos se entenderá por:
XVIII. Procedimiento de imposición de sanciones: Conjunto de actos por los cuales el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través de la Dirección General de Protección de Derechos y Sanción, en caso de presunción de incumplimiento de alguno de los principios o disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que el Pleno previamente determine en los procedimientos de protección de derechos o verificación, impone la o las sanciones que correspondan.

1. Delimitación conceptual y conceptos relacionados

El derecho administrativo sancionador tiene como objetivo fundamental garantizar a la colectividad en general el desarrollo correcto y normal de las funciones reguladas por las leyes administrativas, utilizando el poder del Estado para lograr los objetivos en ellas trazados.

El criterio extensivo sobre interpretación y traslación de los principios constitucionales que rigen en materia penal al derecho administrativo sancionador ha sido analizado previamente, sin embargo, destaca en los procedimientos administrativos sancionadores, el alcance de otros principios constitucionales que rigen su sustanciación.

Un ejemplo es el principio de presunción de inocencia como derecho fundamental de toda persona, aplicable y reconocible a quienes pudiesen estar sometidos a un procedimiento administrativo sancionador y, en consecuencia, soportar el poder correctivo del Estado a través de la autoridad competente.

Al respecto, el Pleno de la Suprema Corte de Justicia de la Nación (SCJN) se ha pronunciado sobre el particular, precisando en la tesis de jurisprudencia P./J. 43/2014 (10a.) que el principio de presunción de inocencia es aplicable al procedimiento administrativo sancionador —con matices o modulaciones, según el caso— debido a su naturaleza gravosa, por la calidad de inocente de la persona que debe reconocérsele en todo procedimiento de cuyo resultado pudiera surgir una pena o sanción cuya consecuencia procesal, entre otras, es desplazar la carga de la prueba a la autoridad, en atención al derecho al debido proceso.[1775]

Por otra parte, en los procedimientos administrativos sancionadores la autoridad se encuentra conminada a desarrollar diversas etapas en las cuales, el presunto infractor tenga oportunidad de comparecer, ofrecer pruebas y alegar lo que a sus intereses convenga, con el propósito de respetar su derecho de audiencia[1776] y atendiendo a la presunción de inocencia de que goza, y de no dejarlo en el más elemental estado de indefensión.

Aunado a lo anterior, en aquellos casos en que en un procedimiento administrativo sancionador no aluda en forma expresa a alguna de las etapas procesales conforme a las cuales debe de sustanciarse, ello no representa en forma alguna que la autoridad administrativa soslaye el cumplimiento de las mismas, pues en todo caso, debe concederse al presunto infractor el derecho de comparecer en el procedimiento, alegar y probar lo que a su derecho convenga y que tales cuestiones sean tomadas en consideración por la autoridad sancionadora al momento de emitir la resolución que corresponda, formalidades con las que se satisface la exigencia prevista por el primer párrafo del artículo 14 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM).[1777]

2. Sustanciación del procedimiento

a) Acuerdo de inicio

De conformidad con lo previsto por los artículos 61 de la LFPDPPP y 68 de los Lineamientos de Procedimiento, cuando como consecuencia de la resolución que se emita en los Procedimientos de Protección de Derechos o de Verificación, el INAI tenga conocimiento de un presunto incumplimiento de alguno de los principios establecidos en la Ley, iniciará el Pisan, a efecto de determinar la sanción que corresponda.

1775 Tesis P./J. 43/2014 (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo I, junio de 2014, p. 41.

1776 Tesis aislada 2a. XLIV/2018 (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo II, mayo de 2018, p. 1696.

1777 Tesis 2a. XLV/2018 (10a.). *Gaceta del Semanario Judicial de la Federación*. Décima época. Tomo II, mayo de 2018, p. 1696.

El artículo 140 del Reglamento de la Ley de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) previene que el procedimiento iniciará con la notificación de un acuerdo de inicio que se haga al presunto infractor, en el domicilio que el INAI tenga registrado, derivado de los procedimientos de protección de derechos o de verificación previamente sustanciados.

En el referido acuerdo, según lo previenen los artículos 62 de la LFPDPPP y 70 de los Lineamientos de Procedimiento, se emplazará al presunto infractor a fin de que comparezca al mismo y haga valer lo que a su derecho convenga, debiendo contener, además:

a) un informe que describa los hechos constitutivos de la(s) presunta(s) infracción(es);
b) el otorgamiento de un término de 15 días hábiles para que el presunto infractor rinda pruebas y manifieste lo que a su derecho convenga, mismo término que se contará a partir de que surta efectos la notificación correspondiente. Para tales efectos se considera que la notificación surte efectos el día en que la misma se realice;
c) el requerimiento al presunto infractor para que presente documentación idónea que acredite su situación financiera actual;
d) la puesta en conocimiento del presunto infractor de que las notificaciones subsecuentes podrán realizarse a través de medios electrónicos.
e) el plazo para formular manifestaciones

Habiendo sido notificado el acuerdo de inicio, de conformidad con lo previsto por el primer párrafo del artículo 62 de la LFPDPPP y el primer párrafo del artículo 141 del RLFPDPPP, el presunto infractor contará con un plazo de 15 días para manifestar lo que a su derecho convenga, pronunciándose concretamente respecto de cada uno de los hechos que se le imputen de manera expresa, afirmándolos, negándolos, señalando que los ignora por no ser propios o exponiendo cómo ocurrieron, según corresponda y ofrezca las pruebas que estime conducentes.

En términos del segundo párrafo del artículo 141 del RLFPDPPP, cuando el presunto infractor ofrezca prueba pericial o testimonial, deberá precisar los hechos sobre los que deban versar y señalará los nombres y domicilios del perito o de los testigos, exhibiendo al efecto el cuestionario o el interrogatorio respectivo en preparación de las mismas, so pena de tenerlas por no ofrecidas si no se formulan los respectivos señalamientos.

Transcurrido en exceso el plazo de 15 días aludido, de conformidad con el primer párrafo del artículo 71 de los Lineamientos de Procedimiento, en caso de que el presunto infractor manifieste en tiempo y forma lo que a su derecho convenga y ofrezca las pruebas que considere convenientes, el INAI emitirá un acuerdo de admisión o desechamiento de pruebas y se procederá a su desahogo, de ser necesario se señalará día y hora para la audiencia correspondiente, levantándose el acta respectiva.

Conforme al último párrafo del referido dispositivo, en el caso de que el presunto infractor no manifestare a lo que a su derecho conviniere o lo hiciera fuera del plazo referido, se procederá a emitir un acuerdo en el que se tendrá por perdido su derecho para hacer valer manifestaciones en su defensa y para ofrecer pruebas, debiendo notificarse el mismo personalmente.

b) Etapa probatoria

El segundo párrafo del artículo 62 de la LFPDPPP previene que el INAI admitirá las pruebas que estime pertinentes y procederá a su desahogo. Sobre el particular, el primer párrafo del artículo 42 del RLFPDPPP dispone que, al ofrecimiento de pruebas del pre-

sunto infractor, el INAI emitirá un acuerdo de admisión o desechamiento de las mismas, y posteriormente procederá a su desahogo.

Para tales efectos, el tercer párrafo del artículo 71 de los Lineamientos de Procedimiento establece que los medios de prueba que podrán ofrecerse en el Pisan son los siguientes:

a) la documental pública;
b) la documental privada;
c) la inspección, siempre y cuando se realice a través de la autoridad competente;
d) la de presunción, en su doble aspecto, legal y humana;
e) la pericial;
f) la testimonial, y
g) las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.

En el caso de que por su naturaleza lo requieran, se determinará lugar, fecha y hora para el desahogo de pruebas. Para tales efectos, se levantará un acta de la celebración de la audiencia y del desahogo de las pruebas.

c) Alegatos

Una vez concluido el desahogo de las pruebas ofrecidas y admitidas, el segundo párrafo del artículo 62 de la LFPDPPP, el primer párrafo del artículo 143 del RLFPDPPP y el primer párrafo del artículo 72 de los Lineamientos de Procedimiento prevén la notificación de un acuerdo al presunto infractor en el que se le conceda el plazo de cinco días para formular alegatos.

Asimismo, el primer párrafo del artículo 143 del RLFPDPPP y el primer párrafo del diverso 72 de los Lineamientos de Procedimiento establecen que habiendo transcurrido en exceso el plazo de cinco días para formular alegatos, se dictará un acuerdo por el que se decrete el cierre de la instrucción.

d) Resolución

Agotadas las etapas procesales a que se ha hecho referencia, de conformidad con lo establecido por el tercer párrafo del artículo 62 de la LFPDPPP, por el artículo 143 del RLFPDPPP y el segundo párrafo del artículo 73 de los Lineamientos de Procedimiento, el INAI deberá emitir la resolución que ponga fin al Pisan.

Cabe señalar que el plazo con que el INAI cuenta para sustanciar y concluir el Pisan, tiene una duración máxima de 50 días hábiles, conforme lo previsto por el segundo párrafo del artículo 73 de los Lineamientos de Procedimiento, mismos que se contarán a partir del inicio del referido procedimiento y que puede ser ampliado por una sola vez, por un periodo igual de 50 días hábiles.

En la resolución que recaiga al Pisan, el tercer párrafo del artículo 73 de los Lineamientos de Procedimiento previene la obligación del Pleno del INAI de analizar los argumentos expuestos por el presunto infractor en su escrito de manifestaciones al acuerdo de inicio, así como las pruebas que hubiese aportado y, en su caso, los alegatos que hubiese formulado, y realizar un pronunciamiento puntual en cuanto a las razones y motivos por los cuales con los mismos no desvirtuó las presuntas infracciones que se le atribuyeron.

Adicionalmente, para efectos de la motivación y cuantificación de las sanciones dentro de los umbrales a que se refiere el artículo 64 de la LFPDPPP,[1778] el INAI deberá considerar,

1778 Artículo 64. Las infracciones a la presente Ley serán sancionadas por el Instituto con:
I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior;

respecto del infractor, según lo ordenan tanto el artículo 65 de la misma Ley, como el cuarto párrafo del artículo 73 de los Lineamientos de Procedimiento, los siguientes elementos:

a) La naturaleza del dato;
b) La notoria improcedencia de la negativa del responsable para realizar los actos solicitados por el titular en términos de esta Ley;
c) El carácter intencional o no de la acción u omisión constitutiva de la infracción;
d) La capacidad económica del infractor; y
e) La reincidencia.

La resolución del Pleno será notificada personalmente al infractor

e) Medios de defensa

De conformidad con lo previsto por los artículos 144 del RLFPDPPP y 74 de los Lineamientos de Procedimiento, en concordancia con la fracción IV, del artículo 3 de la Ley Orgánica del Tribunal Federal de Justicia Administrativa (LOTFJA),[1779] en contra de la resolución que recaiga al Pisan, procede el juicio contencioso administrativo federal que se sustancia ante el Tribunal Federal de Justicia Administrativa (TFJA).

Procedimiento de investigación (PI)

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El Procedimiento de investigación (PI) se refiere al conjunto de actos jurídicos procesales que lleva a cabo el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) o los organismos garantes locales, en el ámbito de sus respectivas competencias y de forma previa al Procedimiento de Verificación (PV), a través de sus unidades administrativas competentes a efecto de obtener información, datos y evidencia o medios de convicción suficientes para que le permitan dilucidar los hechos denunciados por el titular o aquellos que pudieran representar un incumplimiento a la normatividad de protección de datos personales aplicable.[1780]

El PI, cualquiera que sea la faceta normativa en que se desenvuelva, tiene la característica de ser una secuencia procesal que se da siempre antes del PV y que, en consecuencia, puede dar lugar al inicio de este último mediante la emisión de un acuerdo de inicio de procedimiento de verificación.[1781]

II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior;
III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y
IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

1779 Artículo 3. El Tribunal conocerá de los juicios que se promuevan contra las resoluciones definitivas, actos administrativos y procedimientos que se indican a continuación:
[...]
IV. Las que impongan multas por infracción a las normas administrativas federales;
[...]

1780 En relación con el contenido de esta definición se recomienda consultar ciertas definiciones afines como: "acuerdo de inicio de procedimiento de verificación", "requerimiento de información", "procedimiento de verificación" y "acuerdo de inicio de procedimiento de imposición de sanciones".

1781 Para pronta referencia se recomienda consultar la definición de "acuerdo de inicio de procedimiento de verificación" presente en este *Diccionario de Protección de Datos Personales*.

En el sector privado, dicho procedimiento aparece regulado de forma exclusiva en los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de los Procedimientos)[1782] y se refiere como PI. En cambio, en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) se hace uso de la expresión "investigaciones previas", pero para efectos de esta definición referimos a dichas formalidades como PI en el sector público dada la identidad de este tipo de actos jurídicos.

Una vez explicadas las características generales que revisten al PI, a continuación, se presentan las cuestiones específicas que tiene este procedimiento tanto en la legislación aplicable al sector privado como al sector público.

1. Procedimiento de investigación en el sector privado

El PI se define legalmente en el artículo 3 fracción XVI de los Lineamientos de los Procedimientos como el "conjunto de actos que lleva a cabo la Dirección General de Investigación y Verificación del INAI con la finalidad de allegarse de elementos suficientes a efecto de dilucidar los hechos denunciados, de forma previa al procedimiento de verificación".[1783]

Respecto de la definición anterior, debe precisarse que el PI, actualmente, se tramita ante la Dirección General de Investigación y Verificación para el Sector Privado (DGIV) como unidad administrativa competente para conocer sobre la sustanciación del PI y del PV que resulta del mismo.

En este sentido, puede afirmarse que el PI hace referencia a una secuencia de actos procesales que desarrolla la DGIV para reunir los elementos de convicción necesarios con el objeto de que el INAI pueda adoptar una determinación respecto de los hechos denunciados por el titular de los datos o que se han hecho del conocimiento del este instituto y que pudieren involucrar un presunto incumplimiento de la legislación aplicable. Dicha secuencia de actos procesales se da mediante la emisión fundada y motivada de requerimientos de información[1784] al responsable y que tienen como propósito facilitar al INAI la información necesaria que permita a la autoridad investigar los hechos ocurridos.

El PI regulado en los Lineamientos de los Procedimientos está legitimado en la facultad de investigación que se le confiere al INAI en la fracción I del artículo 39 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que señala que el Instituto tiene la atribución de vigilar la debida observancia de la normatividad en materia de protección de datos personales, así como la atribución de expresa conocer y resolver los procedimientos de protección de derechos y de verificación señalados en la LFPDPPP e imponer las sanciones correspondientes.[1785]

1782 Publicados el 9 de diciembre de 2015 en el *Diario Oficial de la Federación*.

1783 Artículo 3. Además de las definiciones establecidas en los artículos 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 2 de su Reglamento, para los efectos de los presentes Lineamientos se entenderá por:

XVI. Procedimiento de investigación: conjunto de actos que lleva a cabo la Dirección General de Investigación y Verificación del INAI con la finalidad de allegarse de elementos suficientes a efecto de dilucidar los hechos denunciados, de forma previa al procedimiento de verificación.

1784 Ver definición de "requerimiento de información" en este *Diccionario de Protección de Datos Personales.*

1785 Artículo 39. El Instituto tiene las siguientes atribuciones:

I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación.

[...]

VI. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda.

Con base en lo dispuesto por la LFPDPPP, el INAI cuenta con atribuciones para recibir las denuncias formuladas por los particulares, por lo que de presentarse una denuncia ante este último, dicho órgano colegiado se encuentra en posibilidad de solicitar documentación previa al inicio del PV,[1786] y es precisamente esta secuela procesal la que se conoce como PI.

1.1 Inicio del procedimiento de investigación

De acuerdo con los Lineamientos de los Procedimientos,[1787] el PI se puede iniciar de las siguientes formas:

A. De oficio. Cuando se presuma de manera fundada y motivada alguna violación a las disposiciones de la LFPDPPP o su Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP). En relación con el inicio del PI bajo la modalidad de oficio, el segundo párrafo del artículo 59 de la LFPDPPP al referirse al PV añade que éste procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de un PPD o se presuma fundada y motivadamente la existencia de violaciones a la LFPDPPP.

B. A petición de parte. Mediante la presentación de una denuncia por parte del titular a través de los medios admitidos por el INAI para tal efecto[1788] y en la que se indiquen presuntas violaciones a las disposiciones de la LFPDPPP y demás ordenamientos aplicables.[1789] En este sentido, el artículo 129 del RLFPDPPP contempla la posibilidad de que cualquier persona pueda denunciar el incumplimiento de la LFPDPPP y sus disposiciones de desarrollo.[1790] Sobre este particular, para que el PI pueda instaurarse a peti-

1786 VII-CASR-8ME-58
REQUERIMIENTO DE DOCUMENTACIÓN. PREVIO AL INICIO DEL PROCEDIMIENTO DE VERIFICACIÓN ESTABLECIDO EN LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. El Instituto Federal de Acceso a la Información y Protección de Datos tiene facultades para vigilar la debida observancia de las disposiciones relacionadas con el cumplimiento de obligaciones por parte de los sujetos a que alude la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y derivado de ese cumplimiento cuenta con atribuciones para recibir las denuncias formuladas por los particulares, por lo que de presentarse ante el Instituto denuncia, con fundamento en el artículo 131, último párrafo del Reglamento de la ley antes aludida en relación con los artículos 38 y 39, fracción I de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la autoridad competente se encuentra en posibilidad de solicitar documentación previo al inicio del procedimiento de verificación, sin que esta actuación pueda tenerse como ilegal, ya que se trata de ejercicio de facultades para allegarse de elementos que le permitan ejercer sus facultades de comprobación.
Cumplimiento de ejecutoria resuelto en juicio contencioso administrativo núm. 12180/13-17-08-3. Resuelto por la octava sala regional metropolitana del Tribunal Federal de Justicia Fiscal y Administrativa, el 2 de septiembre de 2015, por unanimidad de votos. Magistrada instructora: Lucila Padilla López. Secretaria: Lic. Faviola Chávez Martínez.
R.T.F.J.F.A. Séptima época. Año V. No. 52. Noviembre, 2015, p. 634

1787 De acuerdo con lo establecido en el artículo 52 de los Lineamientos de los Procedimientos que señala:
Artículo 52. El Procedimiento de Investigación se podrá iniciar, según sea el caso, de oficio, cuando se presuma de manera fundada y motivada alguna violación a la Ley o su Reglamento, o a petición de parte, a través de los medios señalados para tales efectos, al cual se le asignará un número de expediente para su ubicación y, en su caso, se acusará recibo de la denuncia respectiva, en términos de lo previsto por el artículo 131, último párrafo, del Reglamento.

1788 En este sentido, el artículo 49 de los Lineamientos de los Procedimientos señala:
Artículo 49. La presentación de las denuncias ante el Instituto podrá realizarse a través de los siguientes medios:
I. por escrito. A través de documento presentado, de manera personal o mediante correo certificado, en oficialía de partes, en el domicilio del Instituto ubicado en Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco, Delegación Coyoacán. Código Postal 04530, México, Distrito Federal, o por
II. medios electrónicos: a través de correo electrónico enviado a la cuenta *verificacion@inai.org.mx* o mediante el Sistema de Protección de Datos Personales (IFAI-Prodatos), ubicado en el sitio: https://www.datospersonales.org.mx/.

1789 Cumpliendo los requisitos del artículo 131 del RLFPDPPP y desarrollados por los artículos 49, 50 y 51 de los Lineamientos de los Procedimientos.

1790 Causales de procedencia
Artículo 129. El procedimiento de verificación se iniciará de oficio o a petición de parte, por instrucción del Pleno del Instituto.

ción de parte, la denuncia que formule el denunciante deberá de incluir los siguientes elementos previstos en el artículo 51 de los Lineamientos de los Procedimientos:[1791]

a) nombre completo del denunciante y domicilio o medio, ya sea electrónico o algún otro, para recibir notificaciones;

b) descripción de hechos precisos en los que basa su denuncia y los elementos o documentos con que cuenta para probar su dicho;

c) nombre y domicilio del denunciado o, en su caso, datos para su ubicación;

d) firma autógrafa de quien promueve, para lo cual se deberá observar lo siguiente: 1) si la denuncia se presentó por escrito, ésta deberá tener su firma autógrafa a menos que no sepa o no pueda firmar, caso en el cual, se imprimirá su huella digital; 2) si la denuncia se presentó por medios electrónicos, ésta deberá incluir el documento digitalizado que contenga su firma autógrafa, o bien, que contenga su firma electrónica avanzada (FIEL).

Una vez presentada la denuncia, el INAI, por conducto de su DGIV, acusará la recepción al titular y asignará un número de expediente al caso concreto.[1792] La DGIV podrá, en caso de que lo considere necesario, solicitar al titular la documentación que estime oportuna para el desarrollo del PI.

La DGIV del INAI, al realizar un estudio y análisis de la descripción de los hechos en que se funda la denuncia, así como a partir de la información presentada por el denunciante, podrá realizar las siguientes acciones:

a) Reconducir la denuncia. La denuncia se reconducirá en un plazo no mayor a 10 días hábiles a partir de que se tuvo por presentada la denuncia cuando los hechos en que se funda ésta última se refieran a alguno de los supuestos para el inicio del procedimiento de protección de derechos.[1793]

"Cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas en la Ley y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos. En este caso, el Pleno determinará, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente".

1791 Esto en relación con el artículo 131 del RLFPDPPP:
Requisitos de la denuncia
Artículo 131. La denuncia deberá indicar lo siguiente:
I. nombre del denunciante y el domicilio o el medio para recibir notificaciones, en su caso;
II. relación de los hechos en los que basa su denuncia y los elementos con los que cuente para probar su dicho, y
III. nombre y domicilio del denunciado o, en su caso, datos para su ubicación.
La denuncia podrá presentarse en los mismos medios establecidos para el procedimiento de protección de derechos.
Cuando la denuncia se presente por medios electrónicos a través del sistema que establezca el Instituto, se entenderá que se acepta que las notificaciones sean efectuadas por dicho sistema o a través de otros medios electrónicos generados por éste, salvo que se señale un medio distinto para efectos de estas.
Cuando las actuaciones se lleven a cabo como consecuencia de una denuncia, el Instituto acusará recibo de la misma, pudiendo solicitar la documentación que estime oportuna para el desarrollo del procedimiento.

1792 De acuerdo con el artículo 53 de los Lineamientos de los Procedimientos:
Artículo 53. Las actuaciones del personal adscrito a la Dirección General de Investigación y Verificación se harán constar en el expediente en que se tramita, en términos del artículo 130 del Reglamento, de acuerdo con el cual, en el ejercicio de las funciones de verificación, el personal de dicha Dirección General estará dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo.

1793 Los supuestos previstos en el artículo 115 del RLFPDPPP, que son las causales de procedencia del procedimiento de protección de derechos, son los siguientes:
a) el titular no haya recibido respuesta por parte del responsable;
b) el responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
c) el responsable se niegue a efectuar las rectificaciones a los datos personales;
d) el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;
e) el responsable se niegue a cancelar los datos personales;

b) Orientar al denunciante sobre las instancias legales a las que puede acudir en defensa de sus derechos, en un plazo no mayor a 10 días hábiles a partir de que se haya tenido por presentada la denuncia.

c) Prevenir al denunciante, en caso de que su denuncia no sea clara, o bien, no cumpla con los elementos que señala el artículo 51 de los Lineamientos de los Procedimientos previamente aludidos. En el supuesto de que el titular no responda la prevención formulada en un plazo de cinco días hábiles, se tendrá por desechada la denuncia.

Según lo dispuesto en el segundo párrafo del artículo 52 de los Lineamientos de los Procedimientos, el PI durará 90 días hábiles, contados a partir de la fecha en que se emita el acuse de recibo de la denuncia presentada por el titular, o bien, a partir de la fecha en que la DGIV emita el acuerdo de inicio del procedimiento de investigación.[1794]

1.2 Desarrollo del procedimiento de investigación

Una vez que la denuncia haya cumplido con las formalidades requeridas,[1795] la DGIV expedirá un requerimiento de información[1796] al denunciado o a cualquier tercero solicitando que:

A. se proporcione la información que se estime oportuna respecto a las pretensiones de la denuncia;

B. se manifieste respecto de los hechos vertidos en la denuncia, y

C. aporte la información y documentación que acredite su dicho.

La respuesta al requerimiento de información que formule la DGIV deberá presentarse en un plazo máximo de cinco días hábiles, contados a partir de que surta efectos su notificación. Dicha contestación, según dispone el artículo 56 de los Lineamientos de los Procedimientos, deberá contener, al menos, los siguientes elementos:[1797]

a) nombre completo, denominación o razón social de quien promueve. Si éste fuera en representación de alguna persona física o moral, deberá adjuntarse el documento en original o copia certificada, que acredite su personalidad;

b) domicilio o algún medio electrónico para recibir notificaciones, y

c) documentales que acrediten su dicho, así como la precisión de cualquier información que considere necesaria para la atención del requerimiento.

Derivado de lo anterior, cuando se cuente con información suficiente proporcionada por las partes, la DGIV realizará el análisis y estudio de cada asunto. En el caso de que, a partir de este análisis, la DGIV considere que existe información que no fue del todo clara o precisa, podrá requerir nuevamente al denunciado o a cualquier tercero para que proporcione la información solicitada dentro de un plazo idéntico al concedido para la contestación del requerimiento original requerimiento.

Finalmente, la DGIV podrá dar vista al denunciante para que en un plazo de cinco días hábiles manifieste lo que a su derecho convenga respecto a la información presentada por el denunciante o algún tercero.

---

f) el responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición, y
g) por otras causas que a juicio del Instituto sean procedentes conforme a la Ley o al presente Reglamento.

1794 Este plazo podrá ampliarse por una vez y hasta por un periodo igual, cuando exista causa justificada.

1795 *Vid*, artículo 51 de los Lineamientos de los Procedimientos.

1796 De acuerdo con el artículo 55 de los Lineamientos de los Procedimientos.

1797 Artículo 56 de los Lineamientos de los Procedimientos.

1.3 Conclusión del PI

El PI culmina con la determinación fundada y motivada que la DGIV emita respecto de los hechos señalados en la denuncia del titular o aquellos de los que el INAI hubiere tenido conocimiento, misma que podrá consistir en cualquiera de los siguientes actos procesales:

a) Emisión de un acuerdo de determinación.[1798]

b) Emisión de un acuerdo de inicio de procedimiento de verificación.[1799]

De esta forma, el PI concluirá mediante la emisión de un oficio en el que se determine que el INAI no cuenta con elementos suficientes para acreditar la comisión de actos contrarios a lo establecido por la LFPDPPP y su Reglamento o mediante la emisión del acuerdo de inicio de procedimiento de verificación que se constituirá como el acto procesal necesario para el inicio del PV.

2. Investigaciones previas en el sector público

En el sector público, tanto el INAI como los organismos garantes de las entidades federativas cuentan con la atribución legal de vigilar y verificar el cumplimiento de la normatividad que resulte aplicable[1800] y en consecuencia se encuentran habilitados —cada uno en el ámbito de sus respectivas competencias— de conocer del PV y desarrollar investigaciones previas, con el fin de contar con elementos para fundar la procedencia del PV.[1801]

Las investigaciones previas en el ámbito federal tienen el mandato de desarrollarse de conformidad con los principios de legalidad, certeza jurídica, independencia, imparcialidad, eficacia, objetividad, profesionalismo y transparencia que rigen la actuación del INAI, cumpliendo con los requisitos de fundamentación y motivación.[1802] Además, las investigaciones previas desarrolladas en el sector público federal también quedan sujetas al cumplimiento del deber de confidencialidad respecto de la información relacionada con éstas últimas o el propio PV.[1803]

Otro rasgo importante de las investigaciones previas es que, de acuerdo con lo previsto por el penúltimo párrafo del artículo 147 de la LGPDPPSO y el artículo 188 de los Lineamientos Generales, éstas no procederán en aquellos supuestos en los que resulte procedente el recurso de revisión o el recurso de inconformidad.

2. 1 Inicio de las investigaciones previas

Las investigaciones previas por parte del INAI son un acto preparatorio al inicio del PV que le permiten allegarse de la información necesaria para dilucidar los hechos que presuntamente podrán construir un incumplimiento a la LGPDPPSO y los Lineamientos Generales.

El artículo 189 de los Lineamientos Generales dispone que las investigaciones previas podrán dar comienzo mediante las siguientes modalidades:

1798 *Vid*, definición de "acuerdo de determinación" en este *Diccionario de Protección de Datos Personales*.

1799 Vid, definición de "acuerdo de inicio de procedimiento de verificación" en este *Diccionario de Protección de Datos Personales.*

1800 En este sentido, los artículos 181 y 189 de los Lineamientos Generales señalan:
Facultad de vigilancia y verificación
Artículo 181. De conformidad con lo previsto en el artículo 146 de la Ley General, el Instituto, a través de la unidad administrativa competente conforme a su estatuto orgánico vigente, tendrá la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en dicho ordenamiento y los presentes Lineamientos Generales.

1801 De acuerdo con lo previsto por el último párrafo del artículo 147 de la LGPDPPSO.

1802 *Vid*, artículo 183 de los Lineamientos Generales.

1803 *Vid*, artículo 184 de los Lineamientos Generales.

A. De oficio: cuando el Instituto cuente con indicios que hagan presumir, de manera fundada y motivada, la existencia de violaciones a la LGPDPPSO y a los Lineamientos Generales.

B. A petición de parte: cuando el titular o cualquier persona presente una denuncia, en la que se considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la LGPDPPSO y los Lineamientos Generales, o bien, al tener conocimiento de presuntos incumplimientos a las obligaciones previstas en dichos ordenamientos. De acuerdo con las referidas directrices normativas, la denuncia puede presentarse mediante escrito libre o a través de medios electrónicos[1804] dentro de días y horas hábiles.[1805] La denuncia[1806] deberá contener los siguientes requisitos:

   a) el nombre de la persona que denuncia, o en su caso, de su representante;
   b) el domicilio o medio para recibir notificaciones de la persona que denuncia;
   c) la relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho;
   d) el responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación;
   e) la firma del denunciante, o en su caso, de su representante. En caso de no saber firmar, bastará la huella digital.

De forma posterior a la recepción de la denuncia referida, la autoridad competente acusará la recepción de esta y notificará al denunciante sobre dicha actuación procesal. Deberán acusar recibo de esta. El acuerdo correspondiente se notificará al denunciante. Asimismo, se procederá a asignar un número de expediente para identificar la investigación previa (artículo 193 de los Lineamientos Generales).

Consecuentemente, el INAI procederá a realizar un estudio y análisis de la denuncia presentada por el titular afectado,[1807] y derivado de ello, podrá:

a) Reconducir la denuncia. Cuando ésta se ubique en uno de los supuestos de procedencia del recurso de revisión previsto en la LGPDPPSO. Lo anterior ocurrirá en un plazo no mayor a cinco días contados a partir de que se presentó la misma.
b) Orientar al denunciante sobre las instancias legales a las que puede acudir en defensa de sus derechos, en un plazo no mayor a 10 días hábiles a partir de que se haya tenido por presentada la denuncia.

1804 Presentación de la denuncia
Artículo 190. De conformidad con lo previsto en la fracción II del artículo anterior, la presentación de las denuncias ante el Instituto podrá realizarse a través de los siguientes medios:
   I. Por escrito libre: a través de documento presentado de manera personal o mediante correo certificado en el domicilio del Instituto, o
   II. Por medios electrónicos: a través de correo electrónico, o bien, mediante el sistema electrónico que para tal efecto establezca el instituto.

1805 Horarios y días de recepción de la denuncia
Artículo 191. El Instituto recibirá las denuncias, por escrito y medios electrónicos, en días y horarios hábiles.
Las denuncias recibidas en horas y días inhábiles, se tendrán por presentadas el día hábil siguiente al de su recepción.

1806 De acuerdo con el artículo 192 de los Lineamientos Generales, la denuncia podrá presentarse por escrito libre, o a través de los formatos, medios electrónicos o cualquier otro medio que al efecto establezca el INAI o los organismos garantes. Las denuncias que se hayan presentado por escrito deberán contener la firma autógrafa del denunciante a menos que no sepa o no pueda firmar, en cuyo caso se imprimirá su huella digital, y en el caso de las presentadas por medios electrónicos, se deberá incluir el documento digitalizado que contenga la firma autógrafa, o bien, la firma electrónica avanzada del denunciante o del instrumento que lo sustituya.

1807 *Vid*, artículo 194 de los Lineamientos Generales.

c) Prevenir al denunciante, en caso de que su denuncia no sea clara, o bien, no cumpla con los elementos que señala el artículo 148 de la LGPDPPSO y 192 de los Lineamientos Generales en un plazo no mayor a cinco días a partir de la presentación de la denuncia. La falta de respuesta a la prevención tendrá como consecuencia que se deseche la denuncia.

Así, en el caso de que la denuncia responda a los elementos previstos en la normatividad aplicable, se procederá a la sustanciación de las investigaciones previas.

2.2 Desarrollo de las investigaciones previas

Las investigaciones previas en el orden federal, según ordena el artículo 195 de los Lineamientos Generales, se desarrollarán mediante requerimientos de información que el INAI formule al responsable, encargado o cualquier tercero.

En este contexto, los requerimientos de información que se formulen, podrán, además, solicitar que el responsable, encargado y/o tercero, dentro de un plazo máximo de cinco días contados a partir de que surta efectos la notificación del requerimiento de información, se manifieste respecto de los hechos vertidos en la denuncia o que se aporte la información y documentación que acredite su dicho.

Por otro lado, las respuestas a los requerimientos de información[1808] que formule el INAI a los sujetos obligados deben contener los siguientes elementos materiales:

a) el nombre completo y cargo del servidor público que promueve, así como la denominación de la unidad administrativa y del responsable al que se encuentra adscrito. En caso de actuar en representación de alguna persona moral, con el carácter de encargado o de tercero, deberá adjuntarse el documento, en original o copia certificada, que acredite su identidad y personalidad;

b) el medio para recibir notificaciones y

c) los documentales que acrediten su dicho.

Derivado del análisis que el INAI realice, se podrán formular requerimientos adicionales al responsable, encargado y/o tercero bajo los términos procesales en que se haya formulado el primer requerimiento de información.[1809] En esta misma etapa, también se podrá dar vista al denunciante y solicitarle que, derivado del análisis realizado y/o respuesta del sujeto obligado, facilite información adicional o manifieste lo que a su derecho convenga dentro de un plazo máximo de cinco días contados a partir de que surta efectos la notificación correspondiente.[1810]

2.3 Conclusión de las investigaciones previas

Las investigaciones previas desarrolladas por la autoridad garante federal se considerarán concluidas[1811] cuando la unidad administrativa competente (Dirección General de Investigación y Verificación para el Sector Público) emita cualquiera de los siguientes acuerdos:

a) Acuerdo de determinación: cuando de manera fundada y motivada, no cuente con elementos suficientes para acreditar actos u omisiones que presuntamente constituyan un incumplimiento a lo establecido por la LGPDPPSO y los Lineamientos Generales.

1808 Estos requisitos los establece el artículo 196 de los Lineamientos Generales.

1809 *Vid* artículo 197 de los Lineamientos Generales.

1810 *Vid* artículo 197 de los Lineamientos Generales.

1811 *Vid*, artículo 198 de los Lineamientos Generales.

b) Acuerdo de inicio de procedimiento de verificación: cuando de manera fundada y motivada, se presuma que el responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la LGPDPPSO y los Lineamientos Generales.

En cuanto a su duración, las diligencias de investigaciones realizadas por la autoridad garante en el orden federal deben tener una duración máxima de 50 días. Plazo que se computará a partir de la fecha en que ésta hubiere emitido el acuse de recibo de la denuncia correspondiente, o bien, a partir de la fecha en que se hubiere dictado el acuerdo de inicio de las referidas acciones de investigación.[1812]

Finalmente, debe notarse que, la conclusión de éstas últimas se considerará que ocurre en la fecha en que se emita el acuerdo de determinación o, en su caso, el acuerdo de inicio del procedimiento de verificación respectivo por parte de la unidad administrativa competente del INAI.[1813]

Procedimiento de protección de derechos

Gabriel López López

Es un procedimiento administrativo seguido en forma de juicio, por virtud del cual el titular que habiendo ejercido previamente sus derechos de acceso, rectificación, cancelación y oposición (ARCO) ante el responsable y considerando que los mismos no fueron atendidos o que fueron indebidamente atendidos, acude ante el INAI, quien actuando como órgano materialmente jurisdiccional, previa audiencia y conciliación de las partes, determina si el responsable atendió debida y oportunamente la solicitud de derechos ARCO y, en su caso, ordenar el inicio del procedimientos de imposición de sanciones (Pisan).

La fracción XV, del artículo 3 de los Lineamientos de los Procedimientos de Protección de Derechos de Investigación y Verificación, y de Imposición de Sanciones (en adelante Lineamientos de Procedimientos), establece que el procedimiento de protección de derechos (PPD) es el conjunto de actos a través de los cuales, el INAI, por medio de la Dirección General de Protección de Derechos y Sanción (DGPDS), garantiza el efectivo ejercicio de los derechos ARCO.

Asimismo, de conformidad con la *Guía para Titulares de Datos Personales*,[1814] el PPD tiene fundamento en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y en su Reglamento, y es sustanciado por la DGPDS, para atender las solicitudes de protección de derechos recaídas a las respuestas emitidas por responsables del sector privado a las solicitudes de ejercicio de derechos ARCO, o por falta de éstas.

1812 Artículo 199 de los Lineamientos Generales.

1813 Artículo 199 de los Lineamientos Generales.

1814 Guía para Titulares de Datos Personales, Vol. 4, INAI, p. 6.

1. Sustanciación del procedimiento de protección de derechos (PPD)

A) Procedencia del PPD

Particularmente, los artículos 45, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),[1815] en sus párrafos primero, segundo y tercero y 115 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) previenen las hipótesis conforme a las cuales procede el PPD:

I. cuando el titular no haya recibido respuesta por parte del responsable;
II. cuando el responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
III. cuando el responsable se niegue a efectuar las rectificaciones a los datos personales;
IV. cuando el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;
V. cuando el responsable se niegue a cancelar los datos personales;
VI. cuando el responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición y
VII. por otras causas que a juicio del Instituto sean procedentes conforme a la Ley o al Reglamento.

B) Medios de presentación de la solicitud

De la interpretación conjunta de los artículos 114 del RLFPDPPP y 12 de los Lineamientos de Procedimientos se aprecia que la solicitud de protección de derechos podrá ser presentada a través de las siguientes modalidades:

I. mediante escrito libre o a través de los formatos que proporcione el INAI, directamente ante las oficinas de dicho instituto;
II. mediante escrito libre o a través de los formatos que proporcione el INAI, a través de correo certificado con acuse de recibo;[1816]
III. mediante escrito libre o a través de los formatos que proporcione el INAI, por servicio de mensajería dirigido a las oficinas de dicho instituto y
IV. por medios electrónicos, a través del sistema electrónico del Instituto IFAI-Prodatos,[1817] para lo cual es necesario que el solicitante cuente con la Firma Electrónica Avanzada (FIEL).[1818]

1815 Artículo 45. El procedimiento se iniciará a instancia del titular de los datos o de su representante legal, expresando con claridad el con tenido de su reclamación y de los preceptos de esta Ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los 15 días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.
En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable. En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.
La solicitud de protección de datos también procederá en los mismos términos cuando el responsable no entregue al titular los datos personales solicitados o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

1816 De conformidad con el artículo 42, de la Ley del Servicio Postal Mexicano, "el servicio de acuse de recibo de envíos o de correspondencia registrados consiste en recabar en un documento especial la firma de recepción del destinatario o de su representante legal y en entregar ese documento al remitente, como constancia".

1817 El artículo 3, fracción IX, de los Lineamientos de Procedimientos, define al sistema electrónico del instituto (IFAI–Prodatos) como la plataforma informática proporcionada por el Instituto para que los titulares de datos personales o sus representantes legales, y denunciantes a través de medios electrónicos, presenten solicitudes de protección de derechos y denuncias por presuntos incumplimientos a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y a la normatividad que de ésta derive; así como para la sustanciación de los procedimientos que de ellas resulten; mismo que se encuentra disponible en el sitio: https://www.datospersonales.org.mx/.

1818 El artículo 3, fracción VIII, de los LPDDIVIS, define a la Firma Electrónica Avanzada (FIEL), como el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo

C) Requisitos de la solicitud

Por lo que corresponde a la solicitud de protección de derechos, los elementos que debe contener son los siguientes:

I. el nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si existe;

II. el nombre del responsable ante el cual se presentó la solicitud de ejercicio de los derechos ARCO;

III. el domicilio para oír y recibir notificaciones;

IV. la fecha en que se le dio a conocer la respuesta del responsable, salvo que el procedimiento se inicie ante la ausencia de respuesta del responsable;

V. los actos que motivan su solicitud de protección de datos y

VI. los demás elementos que se considere procedente hacer del conocimiento del INAI.

D) Documentos que deben adjuntarse a la solicitud

Conforme a lo establecido en los artículos 46, párrafos tercero y cuarto, de la LFPDPPP, 116 del RLFPDPPP y 15 de los Lineamientos de Procedimiento, al formularse su solicitud, el titular deberá acompañarla de la siguiente documentación:

I. copia de la solicitud del ejercicio de derechos que corresponda, así como copia de los documentos anexos para cada una de las partes, de ser el caso;

II. el documento que acredite que actúa por su propio derecho o en representación del titular;

III. el documento en que conste la respuesta del responsable, de ser el caso;

IV. en el supuesto en que impugne la falta de respuesta del responsable, deberá acompañar una copia en la que obre el acuse o constancia de recepción de la solicitud del ejercicio de derechos por parte del responsable;

V. las pruebas documentales que ofrece para demostrar sus afirmaciones;

VI. el documento en el que señale las demás pruebas que ofrezca, tales como documentales públicas o privadas, la inspección judicial, el cuestionario sobre el que verse la prueba pericial o testimonial, precisando los hechos sobre los que deban versar, así como los nombres y domicilios de los peritos o testigos, las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología y

VII. cualquier otro documento que se considere procedente someter a consideración del INAI.

En aquellos casos en que el titular no pueda acreditar que acudió con el responsable, ya sea porque se hubiere negado a recibir la solicitud de ejercicio de derechos ARCO o a emitir el acuse de recibo, lo hará del conocimiento del INAI mediante escrito, y éste le dará vista al responsable para que manifieste lo que a su derecho convenga, a fin de garantizar al titular el ejercicio de sus derechos ARCO.

E) Plazo para presentar la solicitud

Conforme a lo previsto por los artículos 45, primer párrafo de la LFPDPPP y 17, fracción I, de los Lineamientos de Procedimiento, el plazo para presentar la solicitud es de 15 días hábiles siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.

control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.

En aquellos casos en que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá presentarse a partir de que haya vencido el plazo de 20 días con que el responsable cuenta para emitir respuesta a la solicitud del titular. Para estos efectos, bastará que acompañe a su solicitud de protección de derechos el documento en el que conste la fecha de presentación de la solicitud de derechos ARCO.

De conformidad con lo previsto por el artículo 18 de los Lineamientos de Procedimiento, el horario de presentación de las solicitudes ante el INAI comprende de las 9:00 a las 18:00 horas de lunes a viernes. Asimismo, tratándose de las solicitudes que se presenten a través del sistema IFAI-Prodatos, después de las 18:00 horas, o en días inhábiles, éstas se tendrán por recibidas el día y hora hábil siguiente. Para efectos del cómputo relativo, resulta ilustrativa la tesis aislada del Poder Judicial de la Federación que a continuación se transcribe:

> PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. MOMENTO EN QUE INICIA EL CÓMPUTO DEL PLAZO DE QUINCE DÍAS QUE ESTABLECE EL ARTÍCULO 45 DE LA LEY FEDERAL RELATIVA PARA PROMOVER EL PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS, DEPENDIENDO DE SI EL RESPONSABLE EMITIÓ O NO RESPUESTA A LA SOLICITUD DE ACCESO, RECTIFICACIÓN, CANCELACIÓN U OPOSICIÓN A LA PUBLICACIÓN DE DATOS PERSONALES PLANTEADA POR SU TITULAR. De los artículos 32, 45, 46, 51 y 52 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 124 de su reglamento se advierte que: i) El titular de los datos personales tiene derecho a solicitar ante el responsable que los posea, le confiera el acceso, su rectificación, cancelación, así como la oposición a su publicación; ii) El responsable puede asumir dos actitudes ante la petición presentada: a) emitir la respuesta correspondiente; o, b) ser omiso en emitir pronunciamiento alguno; iii) En contra de la respuesta u omisión, el titular de los datos personales puede acudir ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a solicitar su tutela mediante el procedimiento de protección de derechos. En este supuesto, el plazo de quince días que para su promoción establece el artículo 45 citado, debe aplicarse de forma general, independientemente de que el responsable haya emitido o no respuesta a la solicitud del titular y, en consecuencia, para computar su inicio debe atenderse a la actitud tomada por aquél. Así, en caso de que el responsable emita una respuesta, su cómputo comenzará a contar al día siguiente de su notificación y, si omite hacerlo, iniciara una vez que concluya el diverso plazo de veinte días que tiene para dar respuesta, en términos del artículo 32 aludido para que, efectivamente, pueda considerarse que no se pronunció en algún sentido y, por tanto, a partir de ese momento, el titular podrá instar al organismo mencionado la protección de sus datos personales.[1819]

F) Análisis de procedencia y admisión de la solicitud

Recibida la solicitud, y a fin de proveer respecto de la procedencia de la solicitud y las pruebas ofrecidas, de conformidad con lo establecido en el artículo 20 de los Lineamientos de Procedimiento, el INAI podrá:

I. prevenir al titular dentro de los 20 días hábiles siguientes a la presentación de la solicitud por una sola ocasión, en caso de que la misma no cumpla con la totalidad de los requisitos exigido o bien, no hubiese acompañado la documentación respectiva, para que subsane las omisiones. si no desahogara la prevención de referencia, dentro del plazo de cinco días hábiles, se tendrá por no presentada la solicitud;

II. admitir la solicitud en un plazo no mayor a 10 días hábiles a partir de su recepción;

III. desechar por improcedente la solicitud o

1819 Tesis I.4o.A.117 A (10a.). *Semanario Judicial de la Federación*. Décima época. Libro 58. Tomo III, septiembre de 2018, p. 2473.

IV. reconducir la solicitud si el INAI considera que no se actualiza alguna de las hipótesis de procedencia, debiendo turnarla a la unidad administrativa competente, en un plazo no mayor a 10 días hábiles contados a partir del día en que se recibió la misma.

En todo caso, el INAI deberá proveer bajo alguno de los supuestos enunciados en un plazo no mayor a 10 días siguientes a partir de su recepción.

Una vez acordada la admisión, el INAI deberá notificarla al promovente y correrá traslado al responsable, en un plazo no mayor a 10 días, anexando copia de todos los documentos que el titular hubiere aportado, a efecto de que dentro del plazo de quince días manifieste lo que a su derecho convenga y ofrezca las pruebas que estime pertinentes.

En aquellos casos en que el procedimiento se inicie por falta de respuesta del responsable, el INAI correrá traslado al responsable para que, en su caso, acredite haber dado respuesta a la misma, o bien, a falta de ésta, emita la respuesta correspondiente y la notifique al titular con copia al INAI, dentro del plazo de 10 días hábiles contados a partir de la notificación. Cuando el responsable no atienda el requerimiento el INAI emitirá la resolución considerando los elementos que consten en el expediente.

Cuando el responsable acredite haber dado respuesta a la solicitud de ejercicio de derechos en tiempo y forma, y haberla notificado al titular o su representante, el PPD quedará sin materia y se decretará el sobreseimiento del mismo.

Cuando la respuesta sea emitida por el responsable durante el PPD o hubiere sido emitida fuera del plazo de 20 días establecido por el artículo 32 de la LFPDPPP,[1820] el responsable notificará dicha respuesta al INAI y al titular, para que éste, en un plazo de 15 días hábiles contados a partir de la notificación, manifieste lo que a su derecho convenga, a efecto de continuar la sustanciación del procedimiento.

Bajo este supuesto, si el titular se muestra conforme con el contenido de la respuesta, el PPD quedará sin materia y se decretará el sobreseimiento del mismo. Cuando así se requiera, el INAI suplirá las deficiencias de la queja de la solicitud del titular, siempre y cuando no altere el contenido original de la solicitud ARCO, ni se modifiquen los hechos o peticiones expuestos en la misma o en la solicitud de protección de derechos.

G) Pruebas

Conforme a lo establecido en el quinto párrafo del artículo 45, de la LFPDPPP, el INAI admitirá las pruebas que estime pertinentes y procederá a su desahogo, teniendo además la facultad de solicitar del responsable las que estime necesarias.

En términos de los artículos 119 del RLFPDPPP y 36 de los Lineamientos de Procedimiento, en el PPD son admisibles las siguientes pruebas:

I. las documentales públicas y privadas;

II. la inspección, siempre y cuando se realice a través de la autoridad competente;

III. la presunción, en su doble aspecto, legal y humana;

1820 Artículo 32. El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Tratándose de solicitudes de acceso a datos personales, procederá la entrega previa acreditación de la identidad del solicitante o representante legal, según corresponda.
Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

IV. la pericial y testimonial,

V. las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.

Tratándose de las pruebas periciales o testimoniales, el oferente deberá precisar los hechos sobre los que deban versar y señalar los nombres y domicilios del perito o de los testigos, exhibiendo, además, el cuestionario o el interrogatorio respectivo para su desahogo, sin lo cual, se tendrán por no ofrecidas.

Ofrecidas las pruebas, conforme lo disponen los artículos 118 del RLFPDPPP y 35 de los Lineamientos de Procedimiento, el INAI dictará un acuerdo de admisión o desechamiento de las pruebas ofrecidas por las partes, y de resultar necesario, éstas serán desahogadas en una audiencia, de la cual se notificará el lugar o medio, la fecha y hora a las partes, la cual solo podrá posponerse por causa justificada.

H) Procedimiento conciliatorio

Según lo establecen los artículos 54, de la LFPDPPP, 120, primer párrafo del RLFPDPPP y 25 de los Lineamientos de Procedimiento, el INAI podrá, en cualquier momento del procedimiento, buscar una conciliación entre el titular de los datos y el responsable.

Solo en el caso de que el titular fuese menor de edad y se hubiese vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes[1821] vinculados con la LFPDPPP y el RLFPDPPP, queda exceptuada la etapa de conciliación, salvo que el mismo cuente con representación legal debidamente acreditada.

Para tales efectos, una vez admitida la solicitud de PPD, el INAI requerirá a las partes que manifiesten, por cualquier medio, su voluntad de conciliar, en un plazo no mayor a 10 días, contados a partir de la notificación de dicho acuerdo, mismo que contendrá un resumen de la solicitud de protección de derechos y de la respuesta del responsable, en su caso, señalando los elementos comunes y los puntos de controversia.

Conforme a los artículos 120, fracción II y 121, del RLFPDPPP y 27 de los Lineamientos de Procedimiento, cuando las partes expresen su voluntad de conciliar, el INAI señalará el lugar o medio, día y hora para la celebración de una audiencia de conciliación, la cual deberá realizarse dentro de los 20 días siguientes en que el INAI haya recibido la manifestación de la voluntad de conciliar de las partes, en la que se procurará avenir los intereses entre el titular y el responsable.

Para ello, la conciliación podrá celebrarse presencialmente por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el INAI pero, en todo caso, deberá de hacerse constar por el medio que permita acreditar su existencia.

En caso de que se requiera contar con elementos probatorios de convicción, el conciliador podrá, en todo momento durante la etapa conciliatoria, requerir a las partes para que presenten en un plazo máximo de cinco días, los elementos probatorios que se estimen necesarios.

Las audiencias podrán ser suspendidas por el INAI o a petición de ambas partes hasta en dos ocasiones, cuando se estime pertinente, en cuyo caso, se señalará día y hora para su reanudación.

Conforme lo prevén el cuarto párrafo de la fracción IV, del artículo 120, del RLFPDPPP y el artículo 29, de los Lineamientos de Procedimiento, de toda audiencia se levantará un acta en la que conste el resultado de la misma. En caso de que el responsable o el titular

1821 Publicada en el DOF el 4 de diciembre de 2014.

o sus respectivos representantes se nieguen a firmar el acta, tal circunstancia no afectará su validez, y deberá de hacerse constar dicha negativa.

En el caso de que alguna de las partes no acuda a la audiencia y justifique su ausencia dentro del plazo de tres días siguientes a la fecha programada, será convocada a una segunda audiencia y, en caso de que no acuda a esta última, se continuará con el PPD. Esta consecuencia ocurre también en el caso de que alguna de las partes no acuda a la audiencia sin justificación alguna.

Cuando las partes no lleguen a acuerdo alguno en la audiencia, el INAI continuará con la sustanciación del PPD.

Cuando las partes lleguen a un acuerdo de conciliación entre ellas, éste se hará constar por escrito y tendrá efectos vinculantes, el PPD quedará sin materia y el INAI verificará el cumplimiento del acuerdo respectivo dentro del plazo establecido para tal efecto, como lo disponen el artículo 54, segundo párrafo, de la LFPDPPP, la fracción V, del artículo 120, del RLFPDPPP y 33 de los Lineamientos de Procedimiento.

Cumplido el acuerdo, se tendrá por concluido el PPD, de lo contrario, el INAI acordará la reanudación del mismo. Durante el plazo que se otorgue a las partes para el cumplimiento del acuerdo conciliatorio, se suspenderá el plazo de 50 días con que cuenta el INAI para dictar resolución en el PPD.

I) Alegatos

Una vez que concluyan las etapas procesales a que se ha hecho referencia, el INAI notificará a las partes que cuentan con un plazo de cinco días hábiles[1822] para que formulen sus alegatos. Transcurrido en exceso el plazo de referencia, se cerrará la instrucción del PPD y el Pleno emitirá la resolución correspondiente.

J) Resolución del PPD

Una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, ya sea que hubiesen sido aportados por el titular al formular su solicitud de protección de derechos, por el responsable al manifestar lo que a sus intereses conviniere o aquéllos aportados durante la celebración de alguna audiencia, el Pleno emitirá la resolución al PPD dentro del plazo máximo de 50 días, contados a partir de la fecha de presentación de la solicitud y, pudiendo ampliar por una ocasión y hasta por un período igual este plazo, existiendo causa justificada.

Al emitir su resolución en el PPD, de conformidad con los artículos 51 de la LFPDPPP y 40 de los Lineamientos de Procedimiento, el Pleno podrá:

a) Sobreseer la solicitud de protección de derechos por improcedente cuando el titular fallezca o se desista expresamente; cuando sobrevenga una causal de improcedencia, y en aquellos casos en que por cualquier motivo quede sin materia la misma.

b) Desechar la solicitud de protección de datos por improcedente, cuando el INAI no sea competente; cuando el Instituto hubiese conocido anteriormente de la solicitud contra el mismo acto y resuelto en definitiva respecto del mismo recurrente; cuando se esté tramitando ante los tribunales competentes algún recurso o medio

1822 De conformidad con lo previsto por el quinto párrafo del artículo 45 de la LFPDPPP, el plazo de cinco días hábiles para formular alegatos, transcurre dentro de los cinco días siguientes a su notificación, mientras que los artículos 122 del RLFPDPPP y 38 de los LPPDIVIS, establecen que, dicho plazo de cinco días, es contado a partir de la notificación del acuerdo a que se refiere este artículo.

de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo; cuando se trate de una solicitud ofensiva o irracional, o cuando su presentación resulte extemporánea.

c) Confirmar, revocar o modificar la respuesta del responsable.

Acorde con lo previsto por los artículos 48 de la LFPDPPP, 125 del RLFPDPPP y 41 de los Lineamientos de Procedimiento, cuando la resolución del PPD resulte favorable al titular, se requerirá al responsable para que, en el plazo de 10 días siguientes a la notificación o cuando así se justifique, uno mayor que fije la propia resolución, haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento al Instituto dentro de los siguientes 10 días.

Asimismo, en la resolución del PPD, el INAI podrá ordenar la instrucción de otros procedimientos establecidos en la Ley de la materia, como el Pisan, cuando se presuma la comisión de alguna conducta que contravenga lo previsto por la LFPDPPP o su Reglamento.

K) Medios de defensa

En contra de la resolución del PPD, el titular o el responsable podrán promover un juicio contencioso administrativo federal ante el TFJA.

Procedimiento de Verificación (PV)

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

Es el conjunto de actos procesales mediante los cuales el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y los organismos garantes a través de sus unidades administrativas competentes verifican el cumplimiento por parte de los sujetos obligados a la normatividad de protección de datos personales que resulta aplicable.

El Procedimiento de Verificación (PV) es el resultado del ejercicio de las facultades de investigación, supervisión y resolución[1823] de la autoridad de control[1824] con la finalidad de verificar el cumplimiento por parte de los sujetos obligados a la normatividad de protección de datos personales y garantizar así la salvaguarda del derecho de protección de datos personales de los titulares. El PV destaca por ser un procedimiento seguido en forma de juicio cuya tramitación se da ante la autoridad de control competente en el orden federal y/o local, según corresponda, y que comienza con la emisión del acuerdo de inicio de PV y concluye con la emisión de una resolución emitida por la autoridad garante competente.[1825]

1823 Por ejemplo, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos mencionan en su artículo 42.4 los poderes que las autoridades de control pueden tener:
42.4. La legislación nacional de los Estados Iberoamericanos que resulte aplicable en la materia deberá otorgar a las autoridades de control suficientes poderes de investigación, supervisión, resolución, promoción, sanción y otros que resulten necesarios para garantizar el efectivo cumplimiento de ésta, así como el ejercicio y respeto efectivo del derecho a la protección de datos personales.

1824 Para una referencia detallada sobre la figura de la autoridad de control se recomienda consultar las definiciones de "autoridad de control" e "INAI" que se encuentran en este *Diccionario de Protección de Datos Personales.*

1825 Ver definición de "acuerdo de inicio de procedimiento de verificación" en este *Diccionario de Protección de Datos Personales.*

El PV tiene su génesis en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), específicamente en los artículos 59 y 60. De forma posterior, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) regula diversos aspectos normativos sobre la sustanciación de este procedimiento (artículos 128 al 139 del RLFPDPPP). Por su parte, los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de los Procedimientos)[1826] contienen regulación complementaria al PV.

En el sector público, es en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) donde se configura el procedimiento de verificación, en particular, en los artículos 146 al 151. Complementan la regulación del PV en el sector público los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales).

De esta forma, la definición del PV que se presenta se divide en dos secciones generales a partir de las cuales se presentan las particularidades de dicho procedimiento en la normatividad del sector privado y en la normatividad de datos personales aplicable para el sector público.

1. Procedimiento de verificación en el sector privado

El PV es resultado del ejercicio de las facultades de vigilancia y verificación sobre el cumplimiento de la normatividad de datos personales correspondientes al INAI en términos de lo dispuesto por la fracción I del artículo 39 de la LFPDPPP.[1827]

En este contexto, el primer párrafo del artículo 59 de la LFPDPPP precisa que corresponde al INAI verificar el cumplimiento de la LFPDPPP y de la normatividad que de ella emane:

> Artículo 59. El Instituto verificará el cumplimiento de la presente Ley y de la normatividad que de ésta derive. La verificación podrá iniciarse de oficio o a petición de parte.

En sintonía con lo dispuesto por el artículo 59 de la LFPDPPP,[1828] el artículo 128 del RLFPDPPP previene lo siguiente:

> Artículo 128. El Instituto, con el objeto de comprobar el cumplimiento de las disposiciones previstas en la Ley o en la regulación que de ella derive, podrá iniciar el procedimiento de verificación, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas.

De la transcripción anterior se desprende que es facultad exclusiva del INAI conocer el PV con la finalidad de verificar la observancia de la legislación nacional de protección de datos personales aplicable al sector privado y que, para ello, se podrá requerir al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas.

En cuanto al alcance del PV, el artículo 60 de la LFPDPPP indica que durante la tramitación de este último, el INAI tendrá acceso a la información y documentación que considere necesarias, de acuerdo con la resolución que lo motive.[1829]

1826 Publicados el 9 de diciembre de 2015 en el *Diario Oficial de la Federa*ción.

1827 En este sentido, la LFPDPPP señala lo siguiente:
Artículo 39. El Instituto tiene las siguientes atribuciones:
I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación […]

1828 Además del contenido del artículo 59 se advierte también que el referido PV podrá iniciarse de manera oficiosa y/o a petición de parte, situación que se explica de forma posterior.

1829 Artículo 60. En el procedimiento de verificación el Instituto tendrá acceso a la información y documentación que considere necesarias, de acuerdo con la resolución que lo motive.

Posteriormente, el segundo párrafo del artículo 60 de la LFPDPPP instruye la confidencialidad de la información derivada del PV a los servidores públicos competentes, y el último párrafo del citado artículo remite al RLFPDPPP para la concreción de las formalidades, términos y plazos en que se sustanciará el PV.[1830]

En cuanto a su definición, los Lineamientos de los Procedimientos en la fracción XVII de su artículo 3 definen al PV como el "conjunto de actos mediante los cuales el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través de la Dirección General de Investigación y Verificación, vigila el cumplimiento de la Ley, su Reglamento y demás normatividad que de ella derive".[1831]

Sobre la definición prevista en los Lineamientos de los Procedimientos, cabe anotar que, actualmente, la tramitación del PV se lleva ante Dirección General de Investigación y Verificación para el Sector Privado (DGIV) que es la unidad administrativa competente para conocer sobre los actos relacionados con el PV.[1832]

Señalado lo anterior, en los siguientes apartados explicaremos algunas de las particularidades del PV.

A. Inicio del PV

De acuerdo con lo previsto en los Lineamientos de los Procedimientos, el PV debe ser necesario y resultado de la sustanciación de un PI. Es decir, no puede haber PV sin la previa instauración de un PI en virtud del cual la DGIV haya emitido un acuerdo de inicio de procedimiento de verificación (ver definición de "acuerdo de inicio de procedimiento de verificación") con fundamento en lo previsto por el artículo 59 de dicho instrumento normativo.[1833]

De esta manera, los Lineamientos de los Procedimientos en el párrafo primero de su artículo 60 establecen que el PV dará inicio como resultado del PI o por incumplimiento a resoluciones dictadas con motivo del PPD y si se presume de manera, fundada y motivada la existencia de un probable incumplimiento a la Ley o el RLFPDPPP.[1834] Lo anterior debe analizarse en sintonía con lo dispuesto por el artículo 59 del RLFPDPPP.[1835]

1830 Artículo 60. En el procedimiento de verificación el Instituto tendrá acceso a la información y documentación que considere necesarias, de acuerdo con la resolución que lo motive.
Los servidores públicos federales estarán obligados a guardar confidencialidad sobre la información que conozcan derivada de la verificación correspondiente.
El Reglamento desarrollará la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere el presente artículo.

1831 Artículo 3. Además de las definiciones establecidas en los artículos 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 2 de su Reglamento, para los efectos de los presentes Lineamientos se entenderá por: XVII. Procedimiento de verificación: conjunto de actos mediante los cuales el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través de la Dirección General de Investigación y Verificación, vigila el cumplimiento de la Ley, su Reglamento y demás normatividad que de ella derive.

1832 *Vid*, artículo 5 de los Lineamientos de los Procedimientos:
Artículo 5. El Instituto, a través de la Dirección General de Investigación y Verificación, es la autoridad competente para investigar, conocer y resolver los procedimientos de verificación y de investigación, ya sea de oficio o a petición de parte, en términos de los artículos 39, fracciones I y VI, 59 y 60 de la Ley, 129 de su Reglamento; y 39, fracciones I, II, VII y VIII, del Reglamento Interior, publicado en el *Diario Oficial de la Federación* el 20 de febrero de 2014.

1833 Artículo 59. Una vez que, dentro del procedimiento de investigación, se cuente con elementos suficientes para iniciar el procedimiento de verificación o en su caso, concluir el procedimiento de investigación, la Dirección General de Investigación y Verificación podrá emitir lo siguiente:
I. Acuerdo de determinación. Se expedirá, de manera fundada y motivada, cuando el Instituto no cuente con elementos suficientes para acreditar la comisión de actos contrarios a lo establecido por la Ley y su Reglamento.
II. Acuerdo de inicio de procedimiento de verificación. Se dictará cuando de manera fundada y motivada se presuma que el Responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la Ley y su Reglamento.

1834 Artículo 60. El procedimiento de verificación se podrá iniciar, derivado de un procedimiento investigación o por incumplimiento a resoluciones dictadas con motivo de procedimiento de protección de derechos. Asimismo, se podrá iniciar de oficio si se presume de manera, fundada y motivada la existencia de un probable incumplimiento a la Ley o el Reglamento.

1835 Inicio
Artículo 128. El Instituto, con el objeto de comprobar el cumplimiento de las disposiciones previstas en la Ley o en la regulación que de ella derive, podrá iniciar el procedimiento de verificación, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas.

Derivado de esto, los Lineamientos señalan que habrá de emitirse un acuerdo de inicio de procedimiento de verificación[1836] y que el mismo deberá notificarse personalmente al responsable en el domicilio que éste haya señalado para tal efecto y al denunciante en su domicilio o a través del medio electrónico que éste hubiere precisado.[1837]

En este tenor, vale la pena destacar que el acuerdo de inicio de procedimiento de verificación es el acto procesal por virtud del cual se da comienzo al PV y se habilita al INAI a través de la DGIV para requerir al responsable la documentación e información considerada necesaria para verificar si ha existido una violación a las disposiciones de la LFPDPPP.

También debe señalarse que el acuerdo de inicio de procedimiento de verificación al ser el acto jurídico que da inicio al PV, representa también el momento procesal a través del cual habrá de comenzar a computarse el plazo de ciento ochenta días hábiles de duración del PV conforme a lo dispuesto en el RLFPDPPP[1838] y los lineamientos de los Procedimientos.[1839]

Un aspecto interesante del PV es la posibilidad de que, derivado del análisis del contenido de la denuncia interpuesta por el titular (denunciante), si a juicio de la DGIV no se actualizan las causales de procedencia del PV, sino que se presentan los supuestos de admisibilidad del PPD, se procederá a turnar la misma a la unidad administrativa competente (Dirección General de Protección de Derechos y Sanción) en un plazo no mayor a mayor a 10 días, contados a partir del día en que se recibió la denuncia.[1840]

Finalmente, es importante tener presente que en relación con la naturaleza del procedimiento de verificación, el Tribunal Federal de Justicia Administrativa ha determinado que dicho procedimiento es autónomo e independiente al procedimiento de imposición de sanciones regulado en la normatividad, ya que, ambos procedimientos inician, se substancian y resuelven de manera distinta.[1841]

1836 Segundo párrafo del artículo 60 de los Lineamientos de los Procedimientos. Se emitirá el acuerdo de inicio de procedimiento de verificación, ya sea por instrucción del Pleno del Instituto, de conformidad con el artículo 129 del Reglamento, o por el Secretario de Protección de Datos Personales y el Director General de Verificación(2) conjuntamente y de conformidad con el artículo 14 del Reglamento Interior del Instituto, en relación con el punto primero del acuerdo por el que se delegan al secretario de Protección de Datos Personales diversas facultades para dictar, conjuntamente con los directores generales que se indican, diversos acuerdos en los procedimientos de verificación, protección de derechos e imposición de sanciones, publicado en el *Diario Oficial de la Federación* el 4 de marzo de 2015.

1837 Artículo 61. El acuerdo de inicio de procedimiento de verificación se deberá notificar personalmente al responsable en el domicilio que éste haya señalado para tal efecto y al denunciante en su domicilio o medio electrónico que, para el caso, haya precisado.

1838 Desarrollo de la verificación
Artículo 132. El procedimiento de verificación tendrá una duración máxima de ciento ochenta días, este plazo comenzará a contar a partir de la fecha en que el Pleno hubiera dictado el acuerdo de inicio y concluirá con la determinación del mismo, el cual no excederá de ciento ochenta días. El Pleno del Instituto podrá ampliar por una vez y hasta por un periodo igual este plazo.
El Instituto podrá realizar diversas visitas de verificaciones para allegarse de los elementos de convicción necesarios, las cuales se desarrollarán en un plazo máximo de diez días cada una. Este plazo deberá ser notificado al responsable o encargado y, en su caso, al denunciante.

1839 Artículo 60. El procedimiento de verificación se podrá iniciar, derivado de un procedimiento investigación o por incumplimiento a resoluciones dictadas con motivo del procedimiento de protección de derechos. Asimismo, se podrá iniciar de oficio si se presume de manera, fundada y motivada la existencia de un probable incumplimiento a la Ley o el Reglamento.
El procedimiento de verificación tendrá una duración máxima de ciento ochenta días hábiles, este plazo comenzará a contar a partir de la fecha en que se haya dictado el acuerdo de inicio. El Pleno del Instituto podrá ampliar por una vez y hasta por un periodo igual dicho plazo de conformidad con el artículo 132 del Reglamento.

1840 Cfr. artículo 139 del RLFPDPPP.

1841 (Tesis de jurisprudencia aprobada por acuerdo G/62/2016) VIIIJSS24.

B. Procedencia del PV

Como adelantábamos, el PV resulta procedente cuando se actualizan los supuestos previstos en el artículo 59 de la LFPDPPP y 129 de su Reglamento[1842] que indican que este procedimiento se podrá presentar de oficio y/o a petición de parte.

En relación con el inicio del PV bajo la modalidad de oficio, el segundo párrafo del referido artículo 59 de la LFPDPPP añade que éste procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de un PPD o se presuma fundada y motivadamente la existencia de violaciones a la LFPDPPP.

En cuanto a la procedencia del PV a petición de parte, es el segundo párrafo del artículo 129 del RLFPDPPP el que contempla la posibilidad de que cualquier persona pueda denunciar el incumplimiento de la LFPDPPP y sus disposiciones de desarrollo:

> Causales de procedencia
>
> Artículo 129. El procedimiento de verificación se iniciará de oficio o a petición de parte, por instrucción del Pleno del Instituto.
>
> Cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas en la Ley y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos. En este caso, el Pleno determinará, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente.

Para que el PV pueda instaurarse a petición de parte (esto siempre dentro de un PI como instancia previa al PV), la denuncia que formule el denunciante deberá de incluir los siguientes elementos previstos en el artículo 51 de los Lineamientos de los Procedimientos:[1843]

i. Nombre completo del denunciante y domicilio o medio, ya sea electrónico o algún otro, para recibir notificaciones.

ii. Descripción de hechos precisos en los que basa su denuncia y los elementos o documentos con que cuenta para probar su dicho.

iii. Nombre y domicilio del denunciado o, en su caso, datos para su ubicación.

iv. Firma autógrafa de quien promueve, para lo cual se deberá observar lo siguiente:

Si la denuncia se presentó por escrito, ésta deberá tener su firma autógrafa a menos que no sepa o no pueda firmar, caso en el cual, se imprimirá su huella digital.

Si la denuncia se presentó por medios electrónicos, ésta deberá incluir el documento digitalizado que contenga su firma autógrafa, o bien, que contenga su Firma Electrónica Avanzada (FIEL).

Finalmente, una vez presentada la denuncia, el INAI por conducto de su unidad administrativa competente (DGIV) acusará la recepción de la denuncia pudiendo solicitar la documentación que estime oportuna para el desarrollo del procedimiento.

1842 Causales de procedencia. Artículo 129. El procedimiento de verificación se iniciará de oficio o a petición de parte, por instrucción del Pleno del Instituto.

1843 Esto en relación con el artículo 131 del RLFPDPPP:
Requisitos de la denuncia. Artículo 131. La denuncia deberá indicar lo siguiente:
I. Nombre del denunciante y el domicilio o el medio para recibir notificaciones, en su caso;
II. Relación de los hechos en los que basa su denuncia y los elementos con los que cuente para probar su dicho.
III. Nombre y domicilio del denunciado o, en su caso, datos para su ubicación.
La denuncia podrá presentarse en los mismos medios establecidos para el procedimiento de protección de derechos.
Cuando la denuncia se presente por medios electrónicos a través del sistema que establezca el Instituto, se entenderá que se acepta que las notificaciones sean efectuadas por dicho sistema o a través de otros medios electrónicos generados por éste, salvo que se señale un medio distinto para efectos de las mismas.
Cuando las actuaciones se lleven a cabo como consecuencia de una denuncia, el Instituto acusará recibo de la misma, pudiendo solicitar la documentación que estime oportuna para el desarrollo del procedimiento.

C. Desarrollo del PV

El PV como decíamos es un procedimiento que se desarrolla en forma de juicio y ante la DGIV del INAI para dilucidar el posible incumplimiento de las disposiciones de la LFPDPPP y demás normatividad aplicable. De manera general, según dispone el artículo 62 de los Lineamientos de los Procedimientos, se puede decir que éste se puede desarrollar de esta forma:

a) Mediante requerimientos de información.[1844] La DGIV emite requerimientos de información al responsable y le concede un plazo cinco días hábiles para dar respuesta a los mismos, contados a partir de que surta efectos la notificación del requerimiento respectivo. En esta etapa el responsable podrá presentar las pruebas que considere pertinentes sobre el tratamiento que brinda a los datos personales, así como manifestar lo que a su derecho convenga respecto de la denuncia y el PV instaurado en su contra.

b) A través de visitas de verificación.[1845] Las visitas de verificación tendrán una duración máxima de 10 días hábiles cada una y se realizan en el establecimiento del responsable, o bien en donde se encuentren las bases de datos objeto de la verificación con la finalidad de que el INAI se allegue de diversos elementos de convicción sobre el tratamiento que el responsable da a los datos personales tanto de titulares como del denunciante.[1846]

Respecto de las visitas de verificación, éstas deberán practicarse conforme a lo dispuesto por los artículos 133, 134, 135 y 136 del RLFPDPPP y los artículos 63, 64, y 65 de los Lineamientos de los Procedimientos.[1847] Dicho acto procesal, concluirá con el levantamiento de un acta de verificación que deberá contener los elementos señalados en el artículo 135 del RLFPDPPP y el artículo 65 de los Lineamientos de los Procedimientos.

D. Conclusión del PV

Según lo señalado por el RLFPDPPP el PV concluirá con la resolución que emita el Pleno del INAI, en la cual se podrán establecer las medidas que deberá adoptar el responsable para cumplir con la normatividad aplicable, así como el plazo en el que las mismas deberán de ser instrumentadas.[1848]

1844 En relación con este tema, recomendamos la consulta de la definición de "requerimiento de información" en este diccionario.

1845 Recomendamos para ulterior detalle la consulta de la definición de "visitas de verificación" en este diccionario.

1846 En este sentido el último párrafo del artículo 132 dispone: "El Instituto podrá realizar diversas visitas de verificaciones para allegarse de los elementos de convicción necesarios, las cuales se desarrollarán en un plazo máximo de diez días cada una. Este plazo deberá ser notificado al responsable o encargado y, en su caso, al denunciante".

1847 En relación con la legalidad de las visitas de verificación derivadas del PV, la Segunda Sala de nuestro Máximo Tribunal ha señalado que éstas últimas no vulneran el derecho de inviolabilidad del domicilio: "PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. LOS ARTÍCULOS QUE REGULAN EL PROCEDIMIENTO DE VERIFICACIÓN PREVISTO EN LA LEY FEDERAL RELATIVA Y EN SU REGLAMENTO, NO VULNERAN EL DERECHO A LA INVIOLABILIDAD DEL DOMICILIO. Si bien el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos establece que la autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios y de policía; y exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, lo cierto es que esa facultad no está limitada a la aplicación de normas que únicamente se refieran al orden sanitario, fiscal o de policía en sentido estricto, en tanto que debe entenderse que se trata de cualquier norma jurídica que otorgue facultades a las autoridades administrativas para regular la conducta de los particulares y cerciorarse de que se ajusta a las normas de orden público aplicables; de lo que deriva que el Congreso de la Unión, mediante la expedición de una ley, puede facultar a un órgano público para practicar visitas domiciliarias a fin de constatar que los particulares han cumplido con las disposiciones en materia de protección de datos personales; de ahí que los artículos 59 y 60 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como 132 a 136 de su Reglamento, que regulan el procedimiento de verificación en la materia, no vulneran el derecho a la inviolabilidad del domicilio reconocido por el artículo 16 constitucional". *Vid*. Tesis: 2a. CXXXIX/2017 (10a.). Décima época. Segunda Sala. *Gaceta del Semanario Judicial de la Federación*. Libro 46, septiembre de 2017. Tomo I, p. 780.

1848 El artículo 137 indica lo siguiente:
Resolución
Artículo 137. El procedimiento de verificación concluirá con la resolución que emita el Pleno del Instituto, en la cual, en

La resolución derivada del PV que emita el INAI podrá instruir el inicio del procedimiento de imposición de sanciones[1849] o establecer un plazo para el inicio de este conforme a las disposiciones de la LFPDPPP, su Reglamento y los Lineamientos de los Procedimientos.

La determinación que el INAI alcance derivado de la sustanciación del PV será notificada de forma personal al responsable y al denunciante.

Finalmente, no puede pasar desapercibido que una de las características de las resoluciones recaídas de los PV que se sustancien ante la DGIV del INAI es su carácter público, razón por la cual éstas pueden difundirse públicamente a través de versiones públicas[1850] que se pueden encontrar en el portal del INAI.[1851]

E. Impugnación de la Resolución del PV

La resolución definitiva del PV emitida por la DGIV del INAI podrá ser impugnada por medio del juicio contencioso administrativo federal (ver definición de "juicio contencioso administrativo federal") ante el Tribunal Federal de Justicia Fiscal y Administrativa (antes Tribunal Federal de Justicia Fiscal y Administrativa) en términos de lo dispuesto por la Ley Federal de Procedimiento Contencioso Administrativo.[1852] En el supuesto de que dicha resolución no sea impugnada podrá considerarse que se trata de un acto consentido por el responsable y/o el titular de los datos personales.[1853]

---

su caso, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma establezca.
La resolución del Pleno podrá instruir el inicio del procedimiento de imposición de sanciones o establecer un plazo para su inicio, el cual se llevará a cabo conforme a lo dispuesto por la Ley y el presente Reglamento.
La determinación del Pleno será notificada al verificado y al denunciante.
En este mismo sentido, los Lineamientos de los Procedimientos disponen:
Artículo 66. El procedimiento de verificación concluirá con la resolución que emita el Pleno del Instituto, en la cual, en su caso, se podrán establecer las medidas que deberá adoptar el responsable en el plazo que la misma establezca.
La resolución del Pleno podrá instruir el inicio del procedimiento de imposición de sanciones o establecer un plazo para su inicio, el cual se llevará a cabo conforme a lo dispuesto por la Ley y el Reglamento.
La resolución del Pleno será notificada personalmente al verificado y al denunciante.

1849 En relación con este procedimiento, en la esfera jurisdiccional se ha destacado la independencia de estos procedimientos:
VIII-J-SS-24
LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. LOS PROCEDIMIENTOS DE VERIFICACIÓN Y DE IMPOSICIÓN DE SANCIONES PREVISTOS EN EL CITADO ORDENAMIENTO, INSTAURADOS POR EL INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS, SON AUTÓNOMOS E INDEPENDIENTES. Del análisis efectuado a los artículos 56 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 138 y 144 de su Reglamento, se colige, que los procedimientos de verificación y de imposición de sanciones instaurados por el Instituto Federal de Acceso a la Información y Protección de Datos, son autónomos e independientes; ya que, ambos procedimientos inician, se substancian y resuelven de manera distinta; pues, el procedimiento de verificación procederá cuando el Instituto Federal de Acceso a la Información y Protección de Datos advierta el incumplimiento a resoluciones dictadas por el propio Instituto dentro de un procedimiento de protección de derechos; o bien, cuando presuma la existencia de violaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; por lo que, el procedimiento de verificación podrá iniciarse de oficio o a petición de parte, se substancia mediante una visita de verificación, dentro de la cual el citado Instituto podrá requerir toda la información que considere necesaria y culmina con la determinación de iniciar o no un procedimiento de imposición de sanciones; en tanto, que el procedimiento de imposición de sanciones inicia con la notificación al presunto infractor de las irregularidades detectadas por el Instituto en comento en los procedimientos de protección de derechos o de verificación, otorga el plazo de quince días para que el presunto infractor rinda pruebas y manifieste por escrito lo que a su derecho convenga, y una vez substanciado el procedimiento, concluye con la emisión del acto en el que se determina o no la imposición de una multa; inclusive, la ley prevé que la resolución recaída a cada procedimiento es impugnable por sí sola a través del juicio contencioso administrativo federal. (Tesis de jurisprudencia aprobada por acuerdo G/62/2016).

1850 Artículo 57. Todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo identifiquen o lo hagan identificable.

1851 Resoluciones del sector privado. Disponible en: http://inicio.ifai.org.mx/SitePages/ResolucionesPDP.aspx

1852 En este sentido, el RLFPDPPP indica:
Artículo 138. En contra de la resolución al procedimiento de verificación, se podrá interponer el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa
De la misma manera el artículo 67 de los Lineamientos de los Procedimientos señala:
Artículo 67. En contra de la resolución al procedimiento de verificación, se podrá interponer el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa, conforme al artículo 138 del Reglamento.

1853 "LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. CASO EN QUE LOS ACTOS DESPLEGADOS EN EL PROCEDIMIENTO DE VERIFICACIÓN INSTAURADO POR EL INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS SE CONSTITUYEN COMO ACTOS CONSENTIDOS. Debido a que, en términos de los artículos 56 de la Ley Federal de Protección

2. Procedimiento de verificación del sector público

La LGPDPPSO otorga al INAI y los organismos locales la facultad de vigilar y verificar el cumplimiento de la normatividad de datos personales en el ámbito de sus correspondientes competencias.[1854] Derivado de ello, los organismos garantes en el ámbito federal (INAI) y local (órganos garantes de las entidades federativas) podrán conocer el PV y realizar las diligencias de investigación y verificación necesarias para la sustanciación de este.[1855]

Es importante tener en cuenta que la Dirección General de Evaluación Investigación y Verificación del Sector Público (en adelante DGIVSP) es la unidad administrativa competente para conocer sobre el PV regulado en la LGPDPPSO y su etapa previa en la que se desarrollan diversas diligencias de investigación.

Así, el PV en el sector público se sujeta a los siguientes principios:

a) Deber de confidencialidad.[1856] Se establece que los servidores públicos que conozcan de las actuaciones relacionadas con este procedimiento deberán guardar confidencialidad sobre información a la que tengan acceso en virtud del PV correspondiente.

b) El PV se debe desarrollar conforme a los principios de legalidad, certeza jurídica, independencia, imparcialidad, eficacia, objetividad, profesionalismo y transparencia que rigen la actuación del INAI, cumpliendo con los requisitos de fundamentación y motivación.[1857]

Derivado de lo anterior, el responsable no podrá negar el acceso a la documentación solicitada con motivo de una verificación, o a sus bases de datos personales, ni podrá invocar la reserva o la confidencialidad de la información.

Señalado lo anterior, en los siguientes apartados pasamos a explicar algunas de las particularidades del PV.

---

de Datos Personales en Posesión de los Particulares, 138 y 144 de su Reglamento, los procedimientos de verificación y de imposición de sanciones son autónomos e independientes; en virtud, de que culminan cada uno con un acto que es recurrible por sí solo, mediante juicio contencioso administrativo federal ante el Tribunal Federal de Justicia Fiscal y Administrativa, si el acto impugnado en el juicio es la resolución recaída a un procedimiento de imposición de sanciones, los argumentos esgrimidos por la parte actora tendentes a controvertir las actuaciones desplegadas en el procedimiento de verificación que le antecede, no deben ser objeto de análisis en el fallo respectivo; dado que, la actora tuvo la posibilidad de controvertir el procedimiento de verificación por vicios propios, de acuerdo con lo dispuesto en los artículos 56 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 138 de su Reglamento, y al no hacerlo, se adquiere la convicción de que ello obedece a que se encontraba conforme con lo determinado en el procedimiento de verificación; es decir, que consintió lo actuado y resuelto en el procedimiento de verificación, presunción que se deduce de lo dispuesto en el artículo 8 fracción IV primer párrafo, de la Ley Federal de Procedimiento Contencioso Administrativo". *Vid*, Juicio Contencioso Administrativo Núm. 13776/1417073/605/15PL0204. Resuelto por el Pleno de la Sala Superior del Tribunal Federal de Justicia Fiscal y Administrativa, en sesión de 19 de agosto de 2015, por unanimidad de 11 votos a favor. Magistrada ponente: Nora Elizabeth Urby Genel. Secretaria: Lic. María Laura Camorlinga Sosa. (Tesis aprobada en sesión de 18 de noviembre de 2015) RTFJFA. Séptima época. Año VI. No. 55. Febrero 2016. p. 37

1854 Artículo 146. El Instituto y los organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta.

1855 En este sentido, los Lineamientos Generales previenen lo siguiente:
Facultad de vigilancia y verificación
Artículo 181. De conformidad con lo previsto en el artículo 146 de la Ley General, el Instituto, a través de la unidad administrativa competente conforme a su estatuto orgánico vigente, tendrá la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en dicho ordenamiento y los presentes Lineamientos Generales.

1856 El segundo párrafo del artículo 146 de la LGPDPPSO indica lo siguiente:
En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los organismos garantes estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.
Por su parte, los Lineamientos Generales establecen:
Deber de confidencialidad
Artículo 184. De conformidad con lo previsto en el artículo 146, segundo párrafo de la Ley General, en el ejercicio de las funciones de investigación, vigilancia y verificación, el personal del Instituto estará obligado a guardar confidencialidad sobre información a la que tengan acceso en virtud de la investigación previa y, en su caso, el procedimiento de verificación correspondiente.

1857 De acuerdo con lo previsto por el artículo 183 de los Lineamientos Generales.

A. Inicio del PV

De acuerdo con lo previsto por el artículo 147 de la LGPDPPSO el PV podrá iniciarse de oficio o por denuncia del titular. En ambos casos el PV resultará de las investigaciones previas iniciadas por el INAI con el fin de contar con elementos suficientes a efecto de dilucidar sobre los hechos que presuntamente podrán constituir un incumplimiento de la LGPDPPSO y los Lineamientos Generales.[1858]

En este contexto, si al concluir las investigaciones previas el INAI, de manera fundada y motivada, presume que el responsable incurrió en acciones u omisiones contrarias a la normatividad de datos personales aplicable, se procederá a emitir el acuerdo de inicio de procedimiento de verificación[1859] que constituirá el acto procesal por virtud del cual se dará legal inicio al PV.[1860]

Con base en lo anterior, la LGPDPPSO detalla que el PV dará inicio con una orden escrita que funde y motive la procedencia de la actuación por parte del INAI o de sus homólogos locales para requerir al responsable la documentación e información relacionada con la presunta violación de la normatividad aplicable y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.[1861]

Así, el PV dará inicio con la notificación personal que el INAI realice del acuerdo de inicio de procedimiento de verificación al responsable y/o al denunciante en el caso de que el PV tuviera origen en una denuncia. Una vez notificado el referido Acuerdo comenzará el cómputo del plazo de 50 días hábiles de duración del PV.[1862]

B. Procedencia del PV

El PV procederá de oficio y/o por denuncia del titular según se señala en el artículo 147 de la LGPDPPSO y el artículo 200 de los Lineamientos Generales.

En relación con los supuestos anteriormente referidos, es prudente tener en cuenta que la normatividad referida determina que estos tendrán las siguientes particularidades:

a) Procedencia de oficio del PV. Procederá cuando el INAI o los organismos garantes locales cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a la normatividad de datos personales aplicable.

1858 Inicio de las investigaciones previas
Artículo 189. De acuerdo con el artículo 147, último párrafo de la Ley General, previo a dar inicio al procedimiento de verificación, el Instituto, a través de la unidad administrativa competente conforme a su estatuto orgánico vigente, podrá desarrollar investigaciones previas con el fin de contar con elementos suficientes a efecto de dilucidar sobre los hechos que presuntamente podrán construir un incumplimiento a la Ley General y los presentes Lineamientos generales.
Lo anterior para fundar y motivar el acuerdo de inicio a que hace referencia el artículo 201 de los presentes Lineamientos Generales.

1859 Se recomienda consultar el apartado de sector público de la definición de "acuerdo de inicio de procedimiento de verificación" en este diccionario.

1860 *Vid*, artículo 198 de los Lineamientos Generales:
Conclusión de las investigaciones previas
Artículo 198. Una vez concluida la investigación previa, el Instituto, a través de la unidad administrativa competente conforme a su estatuto orgánico vigente, deberá emitir un acuerdo de:
I. Determinación: cuando, de manera fundada y motivada, no cuente con elementos suficientes para acreditar actos u omisiones que presuntamente constituyan un incumplimiento a lo establecido por la Ley General y los presentes Lineamientos Generales.
II. Inicio de procedimiento de verificación: cuando, de manera fundada y motivada, se presuma que el responsable incurrió en acciones u omisiones que constituyen un probable incumplimiento a la Ley General y los presentes Lineamientos Generales.

1861 *Vid*, artículo 149, primer párrafo de la LGPDPPSO.

1862 *Vid*, artículo 213 de los Lineamientos Generales.

b) Procedencia del PV por denuncia del titular. Procederá cuando el denunciante considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la LGPDPPSO y demás normativa aplicable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la normatividad aplicable. Según previene el artículo 148 de la citada Ley, la denuncia podrá presentarse por escrito libre, o a través de los formatos, medios electrónicos o cualquier otro medio que al efecto establezca la autoridad competente y contendrá como mínimo los siguientes elementos:

   a. El nombre de la persona que denuncia, o en su caso, de su representante.
   b. El domicilio o medio para recibir notificaciones de la persona que denuncia.
   c. La relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho.
   d. El responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación.
   e. La firma del denunciante, o en su caso, de su representante. En caso de no saber firmar, bastará la huella digital. En este sentido, los Lineamientos Generales destacan además que, tratándose de la presentación por escrito de la denuncia, deba acompañarse la firma autógrafa y en el caso de la presentación por medios electrónicos, el documento en el que se contiene la firma autógrafa digitalizada y/o la firma electrónica avanzada.[1863]

Un aspecto relevante de este PV es que tanto la LGPDPPSO como los Lineamientos Generales[1864] también destacan que el éste último no procederá en los supuestos de procedencia del recurso de revisión o inconformidad.

Si como resultado del estudio y análisis de la descripción de los hechos manifestados en la denuncia, así como a partir de la información presentada por el denunciante, el INAI podrá, a través de la DGIVSP y en un plazo no mayor a cinco días contados a partir de que surta efectos la notificación respectiva, reconducir la denuncia, si ésta se ubica en alguno de los supuestos de procedencia de los recursos de revisión o de conformidad señalados en los artículos 104 y 118 de la LGPDPPSO.[1865]

Es oportuno tener en consideración que en el PV del sector público se establece un plazo de prescripción de un año para la presentación de las denuncias con motivo del incumplimiento de la LGPDPPSO y demás normatividad aplicable.[1866]

1863 En adición a lo anterior, los Lineamientos Generales señalan:
Contenido de la denuncia
Artículo 192. La denuncia a que hace referencia el artículo 189, fracción II de los presentes Lineamientos generales, no deberá contener mayores requisitos de los previstos en el artículo 148 de la Ley General.
Si las denuncias se presentaron por escrito o medios electrónicos, se deberá observar lo siguiente:
I. Si la denuncia se presentó por escrito, ésta deberá contener la firma autógrafa del denunciante a menos que no sepa o no pueda firmar, en cuyo caso se imprimirá su huella digital.
II. Si la denuncia se presentó por medios electrónicos, ésta deberá incluir el documento digitalizado que contenga la firma autógrafa, o bien, la firma electrónica avanzada del denunciante o del instrumento que lo sustituya.

1864 Improcedencia del procedimiento de verificación y de las investigaciones previas
Artículo 188. De conformidad con lo previsto en el artículo 147 de la Ley General, las investigaciones previas y el procedimiento de verificación no procederán en aquellos supuestos de procedencia del recurso de revisión o del recurso de inconformidad, según corresponda.

1865 *Vid*, artículo 194 de los Lineamientos Generales.

1866 *Vid,* artículo 147 de la LGPDPPSO.

C. Sustanciación del PV

El PV en el sector público se sustanciará a través de requerimientos de información y visitas de verificación. En este contexto, los Lineamientos Generales[1867] previenen lo siguiente:

a) Requerimientos de información: el INAI emitirá requerimientos de información al responsable o a cualquier tercero para que, en un plazo máximo de cinco días, contados a partir del día siguiente a que surta efectos la notificación presenten las pruebas que consideren pertinentes sobre el tratamiento que brinda a los datos personales, y/o manifiesten lo que a su derecho convenga respecto de los hechos materia de la verificación y el procedimiento instaurado en su contra.

b) Visitas de verificación: el INAI realizará las visitas de verificación con una duración máxima de cinco días hábiles cada una, que resulten necesarias con la finalidad de que la DGIVSP se allegue de la documentación e información necesaria sobre el tratamiento que el responsable lleva a cabo. Dichas diligencias se realizarán en las oficinas o instalaciones del responsable o, en su caso, en el lugar donde estén ubicadas las bases de datos personales o se realice el tratamiento de los datos personales objeto del PV.

Respecto de las visitas de verificación, el artículo 205 establece las formalidades de éstas últimas y el artículo 206 del mismo ordenamiento instituye los requisitos que deberá de contener el acta derivada de las mismas.

D. Medidas cautelares

La LGPDPPSO establece la posibilidad de que, durante la sustanciación del PV, tanto el INAI como los órganos garantes locales puedan ordenar medidas cautelares[1868] correctivas y de carácter temporal hasta entonces los sujetos obligados lleven a cabo las recomendaciones hechas por el Instituto o los organismos garantes, según corresponda.[1869] Dichas medidas podrán ser ordenadas, si del desahogo del PV se advierte un daño inminente o irreparable en materia de protección de datos personales, siempre y cuando no se impida el cumplimiento de las funciones ni el aseguramiento de bases de datos de los sujetos obligados.[1870]

En este contexto, los Lineamientos Generales señalan que el otorgamiento de las medidas cautelares[1871] será considerado con base en los elementos ofrecidos por el titular, en su caso, así como aquéllos que tenga conocimiento durante la sustanciación del PV para determinar la procedencia de la solicitud del titular. No obstante, los aludidos Lineamientos también establecen la posibilidad de reconsideración del otorgamiento de las medidas cautelares cuando se adviertan nuevos elementos que pudieran modificar la medida cautelar previamente impuesta.[1872]

1867 Artículo 204 de los Lineamientos Generales.

1868 De acuerdo con el artículo 210 de los Lineamentos Generales, las medidas cautelares que puede ordenar el INAI podrán consistir en lo siguiente: 1) el cese inmediato del tratamiento, de los actos o las actividades que estén ocasionando o puedan ocasionar un daño inminente o irreparable en materia de protección de datos personales; 2) la realización de actos o acciones cuya omisión hayan causado o puedan causar un daño inminente o irreparable en materia de protección de datos personales; 3) el bloqueo de los datos personales en posesión del responsable y cuyo tratamiento esté provocando o pueda provocar un daño inminente o irreparable a sus titulares y 4) cualquier otra medida, de acción o de omisión que el Instituto considere pertinente dirigida a proteger el derecho a la protección de los datos personales de los titulares.

1869 Según se prevé en el párrafo cuarto del artículo 149 de la LGPDPPSO y el artículo 207 de los Lineamientos Generales.

1870 Según se prevé en el párrafo cuarto del artículo 149 de la LGPDPPSO y el artículo 207 de los Lineamientos Generales.

1871 De acuerdo con el artículo 109 de los Lineamientos Generales, la aplicación de medidas cautelares será improcedente cuando: 1) tengan por efecto dejar si material el procedimiento de verificación; 2) Eximan al responsable del cumplimiento de las obligaciones previstas en la Ley General u los presentes Lineamientos generales, o 3) Impidan el cumplimiento de las atribuciones y funciones de los responsables conferidas por la normatividad que les resulten aplicable o impliquen el aseguramiento de sus bases de datos.

1872 Reconsideración de la aplicación de medidas cautelares
Artículo 211. Si durante el procedimiento de verificación, el Instituto, a través de la unidad administrativa competente

E. Conclusión del PV

El PV concluirá con la resolución que emita la autoridad garante (el INAI o los organismos garantes locales) en la cual se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.[1873] Dicha resolución, deberá ser notificada personalmente, mediante oficio, al responsable y al denunciante a través del medio que hubiera proporcionado para tal efecto.

F. Impugnación de la resolución del PV

La resolución definitiva del PV emitida por la DGIVSP del INAI podrá ser impugnada por los titulares a través del juicio de amparo ante el Poder Judicial Federal (PJF).[1874] Igualmente, las medidas de apremio impuestas al responsable podrán ser impugnadas ante el PJF o ante las instancias correspondientes de las entidades federativas.[1875]

G. Cumplimiento de las resoluciones de PV

El cumplimiento de las resoluciones del PV debe ser cumplido por el comité de transparencia (ver definición de "comité de transparencia") del sujeto obligado correspondiente, y una vez transcurrido el plazo de cumplimiento de la resolución que corresponda,[1876] el responsable deberá entregar un informe al INAI a través del cual señale las acciones y gestiones realizadas para dar cumplimiento a la resolución del PV acompañando la documentación que acredite sus manifestaciones y declaraciones.[1877] Finalmente, como resultado de la entrega del informe de cumplimiento al INAI, éste tendrá un plazo no mayor a 15 días para pronunciarse sobre el cumplimiento de la resolución.

De esta forma, si el INAI considera que se dio cumplimiento a la resolución del PV emitirá un acuerdo de cumplimiento y ordenará el archivo del expediente. En caso contrario, se emitirá un acuerdo de incumplimiento y se notificará al superior jerárquico del servidor público involucrado para que en un plazo no mayor a 10 días dé cumplimiento a la resolución del PV so pena de aplicar las medidas de apremio previstas en la LGPDPPSO.[1878]

---

a su estatuto orgánico vigente, advierte nuevos elementos que pudieran modificar la medida cautelar previamente impuesta, éste deberá notificar al responsable al menos, con veinticuatro horas de anticipación, la modificación a que haya lugar fundando y motivando su actuación.

1873 *Vid*, artículo 150 de la LGPDPPSO y artículo 212 de los Lineamientos Generales.

1874 En este sentido, los Lineamientos Generales indican:
Artículo 214. Las resoluciones dictadas por el Instituto en el procedimiento de verificación serán vinculantes, definitivas e inatacables para los responsables, los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante juicio de amparo.

1875 Artículo 162. En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante el Poder Judicial de la Federación, o en su caso ante el Poder Judicial correspondiente en las entidades federativas.

1876 *Vid*, artículo 215 de los Lineamientos Generales.

1877 *Vid*, artículo 216 de los Lineamientos Generales.

1878 *Vid*, artículo 217 de los Lineamientos Generales.

Programa Nacional de Protección de Datos Personales

Trinidad Zaldívar Ángel y
Marina San Martín Rebolloso

Pronadatos es el acrónimo que identifica al Programa Nacional de Protección de Datos Personales,[1879] que es el instrumento rector, acordado por los integrantes del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT), para impulsar y desarrollar la política pública de protección de datos personales, en los sujetos obligados del sector público[1880] considerados por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

El Programa Nacional de Protección de Datos Personales constituye una guía de cumplimiento para los integrantes del SNT, que les brinda una especie de hoja de ruta, mediante elementos orientadores que van de lo general a lo particular, que contiene la identificación del problema a combatir, el planteamiento de objetivos y estrategias para hacerle frente, así como una amplia variedad de líneas estratégicas y de acciones a implementar en el ámbito de su competencia y de acuerdo con sus posibilidades y recursos, además de prever indicadores de medición y metas a lograr.

1. Antecedentes

El SNT[1881] se origina en la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y tiene como finalidad coordinar y evaluar las acciones relativas a la política pública transversal de transparencia, acceso a la información y protección de datos personales, tiene entre sus funciones, establecer instrumentos, objetivos, indicadores, metas, estrategias y políticas integrales, sistemáticas, continuas y evaluables, así como establecer programas comunes de alcance nacional para la promoción, investigación, diagnóstico y difusión en transparencia, acceso a la información, protección de datos personales y apertura gubernamental en el país.[1882]

Asimismo, en el marco de la LGPDPPSO, el SNT, a fin de coadyuvar en la construcción de una política pública nacional en la materia, deberá: i) acordar y establecer los mecanismos de coordinación que permitan la formulación y ejecución de instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendentes a cumplir con los objetivos y fines del propio sistema nacional y de las disposiciones que resulten aplicables; ii) diseñar, formular, establecer, ejecutar e implementar políticas generales en materia de protección de datos personales; iii) desarrollar proyectos comunes de alcance nacional y iv) proponer acciones para vincular el SNT con otros sistemas y programas nacionales, regionales o locales.[1883]

1879 Artículo 3, fracción XXVI, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). México. *Diario Oficial de la Federación*, 26 de enero de 2017.

1880 Son sujetos obligados por la LGPDPPSO (artículo 1), cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares. En los supuestos diferentes a los mencionados, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

1881 Son integrantes del SNT: el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI); los organismos garantes de transparencia de las entidades federativas; la Auditoría Superior de la Federación; el Archivo General de la Nación y el Instituto Nacional de Estadística y Geografía. *Vid*, artículo 30 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP). México, *Diario Oficial de la Federación*, 4 de mayo de 2015.

1882 Artículos 28 y 31, fracciones I y III, de la LGTAIP.

1883 Artículo 14, fracciones IV, VI, IX, XI y XVI, de la LGPDPPSO.

En congruencia con lo anterior, para el cumplimiento de las normativas generales tanto de acceso a la información como de protección de datos personales, el SNT tiene la tarea específica de diseñar, aprobar, ejecutar y evaluar dos instrumentos de política pública: i) el Programa Nacional de Transparencia y Acceso a la Información (Protai) y ii) el Programa Nacional de Protección de Datos Personales (Pronadatos).[1884]

El Pronadatos define la política pública nacional de protección de datos personales y establece objetivos, estrategias, acciones y metas, de manera jerarquizada, para:

a) promover la educación y una cultura de protección de datos personales entre la sociedad mexicana;
b) fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición;
c) capacitar a los sujetos obligados en materia de protección de datos personales;
d) impulsar la implementación y mantenimiento de un sistema de gestión de seguridad, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia y
e) prever los mecanismos que permitan medir, reportar y verificar las metas establecidas.[1885]

La LGPDPPSO estableció la obligación del SNT de emitir y publicar el Pronadatos a más tardar en un año a partir de la entrada en vigor de dicho ordenamiento.[1886]

2. Elaboración del Programa

Cabe destacar que la construcción del Pronadatos demandó un proceso de elaboración complejo que requirió transitar por varias etapas para llegar al documento final: una primera diagnóstica, seguida del diseño, análisis, integración, presentación, discusión, ajuste y, finalmente, la aprobación del Consejo Nacional del SNT.[1887]

El punto de partida para la conformación del Pronadatos fue la realización de un diagnóstico[1888] que permitiera identificar las problemáticas en materia de datos personales. Con base en este documento se desarrollaron los objetivos y líneas estratégicas, acciones, actividades, metas, indicadores de resultados y demás componentes del Programa Nacional. A fin de hacerlo más robusto, se previó una consulta pública para que cualquier interesado pudiera opinar sobre su contenido.[1889] La integración final del Pronadatos correspondió a los miembros del SNT con la participación de académicos del Instituto de Investigaciones Jurídicas de la UNAM, así como de servidores públicos especializados y con la colaboración y opinión de la Comisión de Protección de Datos Personales de dicho sistema.[1890]

1884 Artículo 31, fracción XII, de la LGTAIP y artículos 12 y 14, fracción, XVIII, de la LGPDPPSO.

1885 Artículo 12, fracciones I a V de la LGPDPPSO.

1886 Artículo sexto transitorio de la LGPDPPSO y tercero transitorio de los Lineamientos para la Elaboración, Ejecución y Evaluación del Programa Nacional de Protección de Datos Personales (Lineamientos del). *Vid*, Pronadatos CONAIP/SNT/ACUERDO/EXT04-05/10/2017-04 "Acuerdo por el cual se aprueban los Lineamientos para la elaboración, ejecución y evaluación del Programa Nacional de Protección de Datos Personales" (Lineamientos del Pronadatos), en Síntesis de Acuerdos de la cuarta sesión extraordinaria de 2017 del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, celebrada el 5 de octubre de 2017, en la Ciudad de México, en la que se aprobaron, entre otros, los Acuerdos que se indican. México. *Diario Oficial de la Federación*, 16 de octubre de 2017. Disponible en: http://snt.org.mx/images/Doctos/CONAIP/SNT/ACUERDO/EXT04-05/10/2017-04

1887 Décimo sexto de los Lineamientos del Pronadatos.

1888 Véase: Documento Diagnóstico del Programa Nacional de Protección de Datos Personales (Pronadatos) 2018-2022, Secretaría Ejecutiva del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Disponible en: http://proyectos.inai.org.mx/pronadatos/images/Doctos/Documento_Diagnostico_PRONADATOS_2018-2022.pdf

1889 Capítulo IV "De la consulta pública en la construcción del Programa Nacional de Protección de Datos Personales" de los Lineamientos de Pronadatos l.

1890 Apartado 1.1. "Primer Pronadatos" en el Anexo Único del Acuerdo CONAIP/SNT/ACUERDO/EXT01-23/01/2018-04. Véase Acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales. México. *Diario Ofi-*

Para facilitar la integración del Pronadatos, desde octubre de 2017, el Consejo Nacional del SNT aprobó los Lineamientos para la elaboración, ejecución y evaluación del Programa Nacional de Protección de Datos Personales (Lineamientos del Pronadatos).[1891]

Los lineamientos referidos son de observancia obligatoria y aplicación general para los integrantes del SNT y tienen por objeto sentar las bases normativas para el diseño, ejecución y evaluación del programa referido —que tendrá una duración de cuatro años— a fin de coordinar acciones a nivel nacional en materia de protección de datos personales.[1892] Acorde a lo mandatado por la LGPDPPSO y por los Lineamientos del Pronadatos, el consejo nacional del SNT aprobó por unanimidad el Programa Nacional de Protección de Datos Personales 2018-2022 (Pronadatos) en enero de 2018.[1893]

En los tres meses posteriores a su publicación, le correspondió al secretario ejecutivo del SNT[1894] llevar a cabo las acciones necesarias para la conformación y seguimiento de un grupo de implementación del programa, así como para el establecimiento de los enlaces, las rutas de implementación y las fichas de indicadores del primer Pronadatos, junto con su respectiva actualización.[1895]

De acuerdo con la ley general, el Pronadatos debe evaluarse y actualizarse al final de cada ejercicio anual, con el propósito de mejorar sus resultados y cumplimiento.[1896]

3. Ejes temáticos

El Pronadatos se compone de ocho ejes temáticos que son:

1. Educación y cultura de protección de datos personales entre la sociedad mexicana.
2. Ejercicio de los derechos ARCO y de portabilidad.
3. Capacitación a los responsables en materia de protección de datos personales.
4. Implementación y mantenimiento de un sistema de gestión de seguridad.
5. Estándares nacionales, internacionales y buenas prácticas en la materia.
6. Monitoreo, seguimiento y verificación de metas.
7. Acciones preventivas en materia de protección de datos personales, y
8. Perspectiva normativa con enfoque de política pública.[1897]

---

cial de la Federación, 26 de enero de 2018. Disponible en: http://snt.org.mx/images/Doctos/CONAIP/SNT/ACUERDO/EXT01-23/01/2018-04.pdf

1891 CONAIP/SNT/ACUERDO/EXT04-05/10/2017-04. "Acuerdo por el cual se aprueban los Lineamientos para la Elaboración, Ejecución y Evaluación del Programa Nacional de Protección de Datos Personales" (Lineamientos del Pronadatos), publicado en el *Diario Oficial de la Federación*, el 16 de octubre de 2017, como parte del anexo síntesis de acuerdos de la cuarta sesión extraordinaria de 2017, del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, celebrada el 5 de octubre de 2017, en la Ciudad de México, en la que se aprobaron, entre otros, los Acuerdos que se indican.

1892 Primero y Décimo Tercero de los Lineamientos del Pronadatos.

1893 Acuerdo CONAIP/SNT/ACUERDO/EXT01-23/01/2018-04 aprobado en la primera sesión extraordinaria de 2018, del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, celebrada el 23 de enero de 2018.

1894 El secretario ejecutivo ejecuta y da seguimiento a los acuerdos y resoluciones del consejo nacional y verifica el cumplimiento de los programas. Véase artículo 36, fracciones I y III de la LGTAIP.

1895 Artículos cuarto y quinto del acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales.

1896 Artículo 12 de la LGPDPPSO y cuadragésimo cuarto de los Lineamientos del Pronadatos.

1897 Artículo décimo de los Lineamientos del Pronadatos.

El diagnóstico identificó la problemática de cada eje, lo que llevó a proponer un objetivo y una estrategia, acompañadas de líneas de acción específicas, con la finalidad de avanzar en el cumplimiento de la normatividad en la materia.

Como se define en los Lineamientos del Pronadatos, el eje es la "temática sobre la cual versará el contenido general que sirve de línea vertebral o referencia con respecto al cual se desarrollan asuntos referentes a la protección de datos personales dentro del Programa Nacional de Protección de Datos Personales".[1898] El objetivo estratégico consiste en el fin o propósito general al que se ajustan las líneas de acción y que se asocia con la estrategia, es reflejo de la solución de las problemáticas identificadas en el eje temático o transversal[1899] y las estrategias son el conjunto de acciones interrelacionadas para atender cada problemática asegurando un resultado.[1900] El resultado del objetivo estratégico requiere de líneas de acción que constituyen un catálogo de actividades orientadas a lograrlo.[1901]

La organización y estructura del Pronadatos es compleja. Basta ver el anexo único del acuerdo CONAIP/SNT/ACUERDO/EXT01-23/01/2018-04 que está incluido en el acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales, donde se describen los ocho ejes temáticos con la problemática que plantea, su estrategia y objetivo, las líneas estratégicas y líneas de acción que prevé, asociadas a las líneas estratégicas transversales en los que casos que corresponda, así como a la mención de los integrantes del SNT responsables de participar en ellas.[1902]

Por otro lado, como parte del diagnóstico se detectaron problemáticas recurrentes y generalizadas para todos los ejes, identificando tres líneas estratégicas transversales que buscan facilitar soluciones comunes y que son:

a) Sensibilización, promoción, difusión y socialización, en razón de que uno de los problemas reiterados refiere al desconocimiento generalizado sobre la protección de los datos personales.
b) Fortalecimiento institucional, que implica pugnar por instituciones fuertes y sólidas que trabajen por resultados y de manera eficaz y eficiente.
c) Fortalecimiento presupuestal, en virtud de que la asignación de recursos para hacer frente a las nuevas facultades concedidas a los organismos garantes de transparencia de las entidades federativas y a las nuevas obligaciones en materia de protección de datos personales ha sido insuficiente.[1903]

4. Evaluación

Toda política pública debe ser mensurable para poder evaluarla, de ahí la importancia de establecer indicadores que nos permitan saber si los objetivos se cumplieron, para conocer la pertinencia de las estrategias y para estar ciertos que las líneas de acción planteadas permitieron llegar a los resultados esperados.

1898 Tercero, fracción X, de los Lineamientos del Pronadatos.

1899 Tercero, fracción XX, de los Lineamientos del Pronadatos.

1900 Tercero, fracción XI, de los Lineamientos del Pronadatos.

1901 Tercero, fracción XVIII, de los Lineamientos del Pronadatos.

1902 Apartado IV. 4. "Contenidos por temática del Programa" en el anexo único del acuerdo CONAIP/SNT/ACUERDO/EXT01-23/01/2018-04. Véase Acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales.

1903 Apartado IV.3 "Líneas estratégicas transversales" en el anexo único del acuerdo CONAIP/SNT/ACUERDO/EXT01-23/01/2018-04. Véase, Acuerdo Mediante el cual se Aprueba el Programa Nacional de Protección de Datos Personales.

Los indicadores de resultados hacen alusión a las variables o factores que permiten verificar o evaluar los cambios en el estado de los beneficiarios de las acciones a las que se asocia,[1904] mientras que, una meta se refiere al valor que se espera alcance un indicador y que sirva de evidencia del avance en la consecución de los objetivos estratégicos en un periodo establecido.[1905]

Para lograr el cumplimiento del Pronadatos, al inicio del ejercicio anual, cada integrante del SNT debe poner su parte, es decir, desarrollar su propia ruta de implementación en la cual describa las actividades a realizar en el marco de los objetivos estratégicos y líneas de acción previstas en el Programa Nacional que cada miembro defina realizar durante el transcurso del año. Idealmente, esto debería de considerarse en los procesos de planeación institucionales o en los programas anuales de cada integrante.[1906]

Además, el titular de cada integrante del SNT deberá nombrar un enlace con la capacidad de requerir información al interior de la institución que representa, el cual fungirá como un canal de comunicación con el secretariado ejecutivo para facilitar el flujo de información.[1907]

Para el seguimiento del Pronadatos, se contará con una pizarra de avances, diseñada por el secretario ejecutivo en coordinación con la Comisión de Indicadores, Evaluación e Investigación, así como con la Comisión de Protección de Datos Personales del SNT, la cual mostrara el grado de desarrollo que cada integrante lleva de sus actividades programadas para hacer un balance de los esfuerzos que cada estrategia y línea de acción recibe, permitiendo reorientar acciones, ajustar el programa y facilitar a los integrantes el cumplimiento del mismo.[1908] Esta pizarra deberá publicarse, en formatos abiertos, en el portal oficial del SNT y en la página *web* habilitada para tal efecto.[1909]

En el Pronadatos también se contempla un apartado de perspectivas que resalta la importancia de desarrollar las políticas públicas en materia de protección de datos personales de manera progresiva y gradual, en razón de que, al tratarse de un programa nacional ambicioso en su contenido y atendiendo a la diversidad de condiciones de los integrantes del SNT, no resulta posible llevar a cabo todas las acciones contempladas desde un inicio, sin embargo, es factible comenzar con determinados esfuerzos, institucionalizarlos y mejorarlos para que en el largo plazo se proteja y garantice el ejercicio de este derecho en el país. La tabla siguiente refiere las etapas propuestas de 2018 hasta 2037:[1910]

1904 Tercero, fracción XIII, de los Lineamientos del Pronadatos.

1905 Tercero, fracción XIX, de los Lineamientos del Pronadatos.

1906 Tercero, fracción XXV y Trigésimo sexto de los Lineamientos del Pronadatos.

1907 Cuadragésimo tercero de los Lineamientos del Pronadatos.

1908 38, 39, 40 y 41 de los Lineamientos del Pronadatos.

1909 Cuadragésimo segundo de los Lineamientos del Pronadatos.

1910 Apartado VI. "Perspectivas del Pronadatos" en el anexo único del acuerdo CONAIP/SNT/ACUERDO/EXT01-23/01/2018-04. Véase el acuerdo mediante el cual se aprueba el Programa Nacional de Protección de Datos Personales.

Dónde estamos 2018-2020 (etapa 1)	Dónde estaremos 2020-2022 (etapa 2)	Hacia dónde vamos 2022-2026 (2º Pronadatos)	Qué aspiramos 2037 (20 años de la LGPDPPSO)
Se establecen las condiciones institucionales que permitan que los integrantes del SNT cumplan sus obligaciones establecidas en la LGPDPPSO y las legislaciones locales.	Los integrantes del SNT cumplen a cabalidad las obligaciones que les ha establecido la LGPDPPSO.	Los organismos garantes se consolidan como instituciones capaces de garantizar la protección de los datos personales de las y los titulares y los integrantes federales del SNT (AGN, ASF e INEGI) son parámetros de buenas prácticas en la materia.	El SNT se consolida como un mecanismo comprobado y reconocido para la generación de una garantía efectiva y homogénea del derecho a la protección de los datos personales para todo el país.
Se comienzan esfuerzos generalizados para incrementar el conocimiento del derecho y su ejercicio entre la población.	Hay un incremento en el porcentaje de personas que identifica la legislación en materia de protección de datos personales, así como en el conocimiento de las instituciones encargadas de la garantía de este derecho.	La población incrementa el ejercicio de su derecho a la protección de datos personales para proteger su privacidad y la de sus familiares.	La mayoría de la población identifica los mecanismos que le permiten ejercer su derecho a la protección de datos personales.
Se impulsa el cumplimiento de los responsables del ámbito público en los distintos niveles de gobierno en materia de sus obligaciones en materia de protección de datos personales.	Se evalúa a todos los responsables del ámbito público en el cumplimiento de sus obligaciones en materia de protección de datos personales.	Las instituciones públicas que manejan una mayor cantidad de datos personales lo hacen cumpliendo con lo dispuesto en la LGPDPPSO.	La gestión de la seguridad de la información en todos los niveles del sector público está internalizada y es aplicada constante y eficientemente por los servidores públicos.
Se generan las líneas bases para la medición de los aspectos más relevantes de la protección de datos personales en el sector público.	Se desarrolla una serie de instrumentos y mecanismos que otorgan la información necesaria para la evaluación del estado que guardan los principales aspectos de la protección de datos en el sector público del país.	Se tiene un análisis de las fuentes de información que permiten dar cuenta de los cambios generados por las acciones del Pronadatos	La generación de información, su conversión en conocimiento y su integración en la toma de decisiones en materia de protección de datos personales es una rutina institucionalizada en el Estado mexicano.

El Pronadatos busca que las instituciones atiendan lo previsto en la LGPDPPSO de manera paulatina, y se sensibilicen e incrementen su conocimiento respecto del derecho a la protección de los datos personales mediante el impulso de acciones o proyectos diversos que faciliten a las personas su ejercicio y que garanticen la seguridad de dichos datos.

Prueba electrónica

Jonathan Gabriel Garzón Galván

De acuerdo con el *Diccionario Jurídico Mexicano* del Instituto de Investigaciones Jurídicas de la UNAM,[1911] la prueba en un sentido estricto es la obtención de seguridad del juzgador acerca de los hechos discutidos y discutibles, cuyo esclarecimiento es necesario para la resolución del conflicto sometido a un litigio, proceso o procedimiento. Es decir, la prueba es la verificación o confirmación de las afirmaciones o negaciones expresadas por las partes.

Este mismo diccionario señala que, en sentido amplio, la prueba es un conjunto de actos desarrollados por las partes, terceros y los juzgadores, con el objeto de lograr cerciorarse sobre los hechos controvertidos.

En este sentido, el Código Federal de Procedimientos Civiles[1912] valida, en sus artículos 79 y 86, lo mencionado anteriormente:

> Artículo 79. Para conocer la verdad, puede el juzgador valerse de cualquier persona, sea parte o tercero, y de cualquier cosa o documento, ya sea que pertenezca a las partes o a un tercero, sin más limitaciones que las de que las pruebas estén reconocidas por la ley y tengan relación inmediata con los hechos controvertidos.
>
> [...]
>
> Artículo 86. Solo los hechos estarán sujetos a prueba, así como los usos o costumbres en que se funde el derecho.

Con el avance de la tecnología muchos actos jurídicos han migrado su generación, perfeccionamientos y evidencia a través de nuevos medios que difieren de los métodos tradicionales y en papel. Por ello es posible definir la prueba electrónica o tecnológica a todo mensaje de datos, es decir, información generada, almacenada, comunicada o presentada a través de medios electrónicos, ópticos o cualquier otra tecnología que permita a una autoridad o juzgador conocer la verdad de hechos controvertidos.

Actualmente, la legislación mexicana ya tiene en algunos marcos normativos el reconocimiento, aceptación y método de valoración de la prueba electrónica, donde el pilar principal es el artículo 210-A del Código Federal de Procedimientos Civiles,[1913] que se basa en los artículos 5, 6, 8, 9 y 10 de la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional[1914] y es supletorio en la mayoría de las materias.

> Artículo 210-A. Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

1911 Instituto de Investigaciones Jurídicas. (1982). *Diccionario Jurídico Mexicano*. México. Universidad Nacional Autónoma de México. Disponible en: https://biblio.juridicas.unam.mx/bjv/detalle-libro/4282-libreria-migrante

1912 Código Federal de Procedimientos Civiles, última reforma DOF 09/04/. Disponible en: http://www.diputados .gob.mx/LeyesBiblio/pdf/6.pdf

1913 Código Federal de Procedimientos Civiles, última reforma DOF 09/04/2012. Disponible en: http://www.diputados .gob.mx/LeyesBiblio/pdf/6.pdf

1914 Ley Modelo de la CNUDMI sobre comercio electrónico y su guía para su incorporación al derecho interno. Disponible en: https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y pueda ser accesible para su ulterior consulta.

En este mismo sentido, otros ordenamientos jurídicos establecen dentro de sus artículos la aceptación y/o valoración de la prueba electrónica de forma directa, haciendo referencia al propio artículo 210 A antes señalado, o dejan abierta la posibilidad de aceptar cualquier información aportada por la ciencia.[1915] Este último caso es el contemplado por la fracción VII, del artículo 102, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[1916] y la fracción VII, del artículo 36, de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación y de Imposición de Sanciones (Lineamientos de Procedimiento).

Este tipo de prueba debe ser admitida por las autoridades y jueces siempre que sea ofrecida por las partes o terceros. La forma de ofrecimiento de la prueba electrónica es, generalmente, por vía documental pública o privada contenida en un mensaje de datos,[1917] sin embargo, es posible que se presente como prueba pericial, testimonial y/o confesional, en este último caso, se opta por presentar la declaración de la persona a través de comunicación electrónica a distancia.

El método para desahogar las pruebas electrónicas varía de los métodos tradicionales, ya que la información se expresa a través de un soporte electrónico, por lo que se requiere elementos físicos (*hardware*) y no físicos (programas de cómputo o *software*) para tener acceso a dicha información, es decir, para que la información (texto, imágenes, sonido, etc.) sea perceptible para quien deba valorarla, la prueba debe presentarse a través de un dispositivo físico (CD, USB, computadoras, dispositivos móviles, etc.) que —en conjunto con los sistemas de cómputo óptimos— traduzcan, muestren o permitan el acceso a la información. Sin ambos elementos (físico y no físico) no será viable su siguiente paso: la valoración.

No debe entenderse que una impresión del mensaje de datos o de la información en medios tecnológicos es una prueba electrónica, ya que, al materializar la información en un medio distinto al tecnológico pierde su calidad de prueba electrónica para ser una prueba tradicional, por lo que el juzgador deberá valorarla a su criterio como tal.

1915 1834 bis del Código Civil Federal, última reforma DOF 09/03/2018.
Disponible en: http://www.diputados.gob.mx /LeyesBiblio/pdf/2_090318.pdf
89, bis, 93, 93 bis, 1205, 1298 A y 1061 bis del Código de Comercio, última reforma DOF 28/03/2018.
Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf /3_280318.pdf
51 y 381 del Código Nacional de Procedimientos Penales, última reforma DOF 17/06/2019.
Disponible en: http:// www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf
17-D del Código Fiscal de la Federación, última reforma DOF 25/06/2018.
Disponible en: http://www.diputados. gob.mx /LeyesBiblio/pdf/8_250618.pdf
35, 69-C y 69-C bis de la Ley Federal del Procedimiento Administrativo, última reforma DOF 18/05/2018.
Disponible en: http://www. diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf
46 y 58 K de la Ley Federal del Procedimiento Contencioso Administrativo, última reforma DOF 27/01/2017,
Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf
776 de la Ley Federal del Trabajo última reforma DOF 22/06/2018.
Disponible en: http://www.diputados. gob.mx/Leyes Biblio/pdf/125_220618.pdf

1916 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el DOF 26/01/2017.
Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

1917 Véase la definición de "documento electrónico (mensaje de datos)" del presente diccionario.

La valoración de la prueba corresponde a una operación mental y técnica que realiza la autoridad o juzgador con el objetivo de conocer la eficacia de la prueba para lograr su cometido. Tal acción está enfocada a verificar la concordancia entre el resultado de la prueba con la hipótesis o hechos sometidos a demostración por dicho medio.[1918] Es decir, se refiere a aquello que la prueba aporta de convencimiento a la causa acerca de la existencia o inexistencia de los hechos que se afirman o se niegan entre las partes.

La valoración de una prueba electrónica supone la necesidad de revisar y/o redefinir algunos conceptos como consecuencia del uso de la tecnología en los actos jurídicos, como son los conceptos "original" y "copia". En la prueba tradicional —para darle cierto valor a una evidencia o prueba— es idóneo, y por tanto requerido por la propia regulación, presentar el original, ya que la mera copia podría ser un indicio insuficiente para que el juzgador o autoridad tenga por verdaderos los hechos que busca comprobar.[1919]

En la prueba electrónica, dado que cualquier reproducción o copia de un mensaje de datos es idéntica al mensaje de datos que permitió su reproducción, no pierde funcionalmente ninguno de sus elementos por el simple hecho de ser copia, incluso no sería posible conocer cuál fue el original con solo compararlos.

Es por ello que tanto las leyes modelos de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional como la regulación mexicana antes referenciada adoptaron para la prueba electrónica el principio de equivalente funcional, que en forma general establece que si la ley requiere que una prueba o documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la prueba electrónica se ha mantenido íntegra a partir del momento en que se generó en su forma definitiva, es accesible para presentarla ante quien deba valorarla, que pueda ser atribuible a las personas que se requiera y que sea fiable para su generación, transmisión y conservación.

Las características antes descritas (integridad, accesibilidad, atribución, fiabilidad) son aquellas que deben demostrarse al presentar una prueba electrónica para que en su valoración se le brinde la eficacia probatoria, tal como si fuera un original en los medios tradicionales:

a) Accesibilidad/disponibilidad: es aquella característica que ratifica que la información puede ser localizada, presentada y mostrada ante las autoridades o ante quienes tengan derecho a ello en el momento que se requiera. Es una cualidad o condición de la información de estar legible o entendible para ser valorada. Incluye los mecanismos de equipos y programas de cómputo que —en conjunto— permiten llegar a la información, así como sus respaldos[1920] y actualizaciones. Resulta relevante que quien haga uso de mensajes de datos en sus actividades realice las acciones tendientes a que no se pierda o destruya la información en el formato que haya sido definido como su forma decisiva, para lograr mantener esta característica.

b) Integridad: es la característica con la que es posible validar que el contenido y/o información de la prueba electrónica está completa y no ha sido alterado a partir de que se generó o transmitió en su forma definitiva. Para obtener un concepto claro de

1918 Nava, A. (2011). *La prueba electrónica en materia penal*. Porrúa. México, p. 148.

1919 En las pruebas tradicionales al reproducir copias generalmente se pierden ciertas características con las cuales contaban los originales y existen riesgos de no poder identificar alguna modificación.

1920 El medio físico a través del cual el contenido de un mensaje de datos se pone a disposición del usuario puede ser diferente de aquel en que se creó, ya que se debe garantizar la integridad del mensaje de datos, no del medio físico que lo contiene. Esto es, que el mensaje puede estar contenido en el disco duro de una computadora y ponerse a disposición del usuario en un diskette, al copiarse a ese medio físico distinto al en que fue creado no lo hace de ninguna manera perder integridad. Reyes, A. (2008). *La firma Electrónica y las Entidades de Certificación*, 2da. edición. Porrúa. México, p. 7.

integridad es posible referirse al artículo 93 del Código de Comercio[1921] que establece que se considerará que el contenido de un mensaje de datos es íntegro, si éste ha permanecido completo e inalterado, independientemente de los cambios que hubiere podido sufrir el medio que lo contiene, resultado del proceso de comunicación, archivo o presentación.

c) Atribución: es la característica que permite identificar y vincular a las personas que han aceptado o expresado su consentimiento para obligarse al contenido del mensaje de datos, sin que puedan repudiar su consentimiento ni el propio contenido de mensaje de datos o prueba electrónica. Incluye tanto autenticidad como no repudio, la primera establece quién es el autor de un mensaje de datos y su destinatario. El no repudio prueba que el autor envió la información (no repudio en origen) y que el destinatario la recibió (no repudio en destino), estando ambas en posibilidad de actuar y responder ante tal comunicación. La atribución vincula las obligaciones contenidas en la información del documento electrónico, tanto a su emisor como a su destinatario.

d) Fiabilidad: es la característica que permite señalar que todo el proceso —desde que se generó la prueba electrónica o mensaje de datos, hasta que fue presentada a la autoridad— es fiable[1922] de acuerdo con la finalidad que se requiera, por lo que al presentar una prueba electrónica se deberá especificar la metodología utilizada a lo largo de todo el ciclo de vida del mensaje de datos, su importancia, volumen, finalidad de su generación, recepción y/o envío, entre otras particularidades, para adjuntar todos los elementos que comprueben la metodología seguida para cumplir las otras tres características ya mencionadas. Se deben mantener las evidencias para comprobar que los procesos y sistemas que manejan las pruebas electrónicas ofrecen seguridad y no permiten error en cuanto a mantener sus garantías de integridad, autenticidad, atribución y accesibilidad. Ahora bien, no todo método tiene la misma fiabilidad, su valoración debe atender a la criticidad y valor de la información contenida en los documentos electrónicos. Será parte de esta característica el que la prueba electrónica haya sido obtenida de manera lícita, o sin afectar derechos fundamentales.[1923]

1921 Código de Comercio, última reforma DOF 28/03/2018.
Disponible en: http://www.diputados.gob.mx/Leyes Biblio/pdf /3_280318.pdf

1922 RAE. (2017). Fiable en *Diccionario de la Lengua Española.* Disponible en: http://dle.rae.es/ Fecha de consulta: agosto 2018: fiable.
1. adj. Dicho de una persona: que es digna de confianza.
2. adj. Que ofrece seguridad o buenos resultados. Mecanismo fiable. Método fiable.
3. adj. Creíble, fidedigno, sin error. *Datos fiables*

1923 A este respecto vale la pena observar la siguiente tesis:
PRUEBA ELECTRÓNICA O DIGITAL EN EL PROCESO PENAL. LAS EVIDENCIAS PROVENIENTES DE UNA COMUNICACIÓN PRIVADA LLEVADA A CABO EN UNA RED SOCIAL, VÍA MENSAJERÍA SINCRÓNICA *(CHAT),* PARA QUE TENGAN EFICACIA PROBATORIA DEBEN SATISFACER COMO ESTÁNDAR MÍNIMO, HABER SIDO OBTENIDAS LÍCITAMENTE Y QUE SU RECOLECCIÓN CONSTE EN UNA CADENA DE CUSTODIA. El derecho a la inviolabilidad de las comunicaciones privadas, previsto en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos se extiende a las llevadas a cabo mediante cualquier medio o artificio técnico desarrollado a la luz de las nuevas tecnologías, desde el correo o telégrafo, pasando por el teléfono alámbrico y móvil, hasta las comunicaciones que se producen mediante sistemas de correo electrónico, mensajería sincrónica *(chat)*, en tiempo real o instantánea asincrónica, intercambio de archivos en línea y redes sociales. En consecuencia, para que su aportación a un proceso penal pueda ser eficaz, la comunicación debe allegarse lícitamente, mediante autorización judicial para su intervención o a través del levantamiento del secreto por uno de sus participantes pues, de lo contrario, sería una prueba ilícita, por haber sido obtenida mediante violación a derechos fundamentales, con su consecuente nulidad y exclusión valorativa. De igual forma, dada la naturaleza de los medios electrónicos, generalmente intangibles hasta en tanto son reproducidos en una pantalla o impresos, fácilmente susceptibles de manipulación y alteración, ello exige que para constatar la veracidad de su origen y contenido, en su recolección sea necesaria la existencia de los registros condignos que a guisa de cadena de custodia, satisfagan el principio de mismidad que ésta persigue, o sea, que el contenido que obra en la fuente digital sea el mismo que se aporta al proceso. Así, de no reunirse los requisitos mínimos enunciados, los indicios

Cabe señalar que la atribución, fiabilidad e integridad, a partir del momento en que el mensaje de datos se crea en su forma definitiva, es posible cumplirlos con la tecnología de firma electrónica avanzada y cumpliendo con el apéndice A de la norma oficial mexicana NOM-151-SCFI-2016,[1924] que tiene como sustento el artículo 49 del Código de Comercio.[1925]

La carga de demostrar que las pruebas electrónicas cuentan con estas características corresponde a quien las ofrece, y debe analizarse la postura procesal de las partes en relación de la prueba electrónica. De no impugnarse, es viable tener por ciertos los hechos o contenidos que buscan probar sin tener que requerir mayor ahondamiento en las características antes señaladas. En caso de impugnación, la parte interesada deberá presentar los medios suficientes para fortalecer estas cualidades.

Ejemplos de lo anterior pueden observarse en los artículos 20 (obtención del consentimiento del titular), 31 (puesta a disposición del aviso de privacidad) y 69 (transferencias en cumplimiento con la normatividad) del Reglamento de la LFPDPPP,[1926] donde la carga de la prueba (en todos estos casos) es del responsable, y cuando se utilizaron medios electrónicos, el responsable debe poder demostrar ese hecho a través de mensajes de datos que contengan todas las características anteriormente analizadas.

A manera de conclusión, la información que nace o que, en alguna fase, fue transmitida o almacenada a través de medios electrónicos o tecnológicos puede presentarse como prueba en un procedimiento judicial o administrativo, y tendrá los mismos efectos y valor probatorio que las pruebas en medios tradicionales, cumpliendo con el principio de equivalencia funcional.

En estos procesos, la norma exige que a efecto de que todos y cada uno de los medios de prueba allegados al proceso sean analizados por las autoridades y juzgadores atendiendo a su naturaleza y características específicas, sin que sea válido dejar de otorgarles valor y eficacia con motivo del medio en que se aportaron, ya sea de forma electrónica, óptica o de cualquier tecnología.

---

que eventualmente se puedan generar, no tendrían eficacia probatoria en el proceso penal, ya sea por la ilicitud de su obtención o por la falta de fiabilidad en ésta. Segundo tribunal colegiado en materia penal del primer circuito. Amparo directo 97/2016. 11 de agosto de 2016. Unanimidad de votos. Ponente: Alejandro Gómez Sánchez. Secretario: Fernando Emmanuelle Ortiz Sánchez.
Tribunales colegiados de circuito. Décima época. *Gaceta del Semanario Judicial de la Federación*. Libro 38, enero de 2017, p. 2609. Disponible en: https://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/2013/2013524.pdf

1924 Norma Oficial Mexicana NOM-151-SCFI-2016. Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos (cancela la NOM-151-SCFI-2002). Disponible en: http://www.dof. gob.mx/normasOficiales/6499/seeco11_C/seeco11_C.html

1925 Código de Comercio, última reforma DOF 28/03/2018. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_280318.pdf
Artículo 49. Los comerciantes están obligados a conservar, por un plazo mínimo de diez años, los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones.
Para efectos de la conservación o presentación de originales, en el caso de mensajes de datos, se requerirá que la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta. La Secretaría de Economía emitirá la norma oficial mexicana que establezca los requisitos que deberán observarse para la conservación de mensajes de datos.

1926 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el DOF 21/12/2011. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Prueba de daño

Jimena Moreno González

El derecho a la información está garantizado por la Constitución Política de los Estados Unidos Mexicanos (CPEUM) en su artículo 6 para cualquier persona, sin acreditar interés jurídico o destino de la información (fracción III), y es un elemento fundamental de la democracia. Este artículo también establece las bases para el ejercicio del derecho a la información y señala lo siguiente:

> Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y solo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.[1927]

Derivado de lo anterior, podemos establecer dos elementos importantes para abordar este tema: i) la información solo puede ser reservada temporalmente por razones de interés público y seguridad nacional y ii) deberá prevalecer el principio de máxima publicidad.

La Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) señala la obligación de aplicar una prueba de daño para los casos en que se deba motivar la clasificación de la información y la ampliación del plazo de reserva.[1928]

Es importante señalar que el artículo 68 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) remite al artículo 104 de la LGTAIP para la aplicación de la prueba de daño para el caso de que se requiera reservar la información.[1929]

En el artículo 104 de la mencionada ley se establecen los requisitos para aplicar la prueba de daño y señala:

> Artículo 104. En la aplicación de la prueba de daño, el sujeto obligado deberá justificar que:
>
> I. la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional;
>
> II. el riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda y
>
> III. la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio.

1927 Constitución Política de los Estados Unidos Mexicanos. Disponible en: https://www.juridicas.unam.mx/legislacion/ordenamiento/constitucion-politica-de-los-estados-unidos-mexicanos#10541

1928 Artículo 103 de la Ley General de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 4 de mayo del 2015.

1929 Ley Federal de Transparencia y Acceso a la Información Pública.
Artículo 68. Los sujetos obligados en el ámbito federal deberán cumplir con las obligaciones de transparencia y poner a disposición del público y mantener actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas e información señalados en el título quinto de la Ley General. Al respecto, aquella información particular de la referida en el presente artículo que se ubique en alguno de los supuestos de clasificación señalados en los artículos 110 y 113 de la presente Ley no será objeto de la publicación a que se refiere este mismo artículo; salvo que pueda ser elaborada una versión pública. En todo caso se aplicará la prueba de daño a que se refiere el artículo 104 de la Ley General.
En sus resoluciones el Instituto podrá señalar a los sujetos obligados que la información que deben proporcionar sea considerada como obligación de transparencia de conformidad con el capítulo II del título quinto de la Ley General y el capítulo I del título tercero de esta Ley, atendiendo a la relevancia de la información, la incidencia de las solicitudes sobre la misma y el sentido reiterativo de las resoluciones, publicada en el *Diario Oficial de la Federación* el 9 de mayo de 2016.

En los artículos 113 fracción I y 114 de la LGTAIP y 110 fracción I de la Ley Federal de Transparencia ya Acceso a la Información Pública (LFTAIP) se establecen las causas que proceden para clasificar la información como reservada y señala que, tratándose de las causales de reserva, éstas deberán fundarse y motivarse a través de la aplicación de la prueba de daño en la que los sujetos obligados demuestren, caso por caso,[1930] que su divulgación pudiera afectar los supuestos del artículo 113. Así también lo señaló a Suprema Corte de Justicia de la Nación (SCJN) al indicar que, "… puede considerarse reservada mediante la aplicación de la prueba de daño, si éstos demuestran que con su divulgación se actualizaría alguno de los supuestos legales en que se juzga preferible aplazar su acceso".[1931]

En los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de las versiones públicas para los sujetos obligados se define la prueba de daño como "la argumentación fundada y motivada que deben realizar los sujetos obligados tendiente a acreditar que la divulgación de la información lesiona el interés jurídicamente protegido, por la normativa aplicable y que el daño que puede producirse con la publicidad de la información es mayor que el interés de conocerla".[1932]

En el lineamiento 33 se establecen los requisitos que deberá contener la prueba de daño de acuerdo con el artículo 104 de la LGAIP que son los siguientes:

> Trigésimo tercero. Para la aplicación de la prueba de daño a la que hace referencia el artículo 104 de la Ley General, los sujetos obligados atenderán lo siguiente:
>
> I. se deberá citar la fracción y en su caso, la causal aplicable del artículo 113 de la Ley General, vinculándola con el Lineamiento específico del presente ordenamiento y, cuando corresponda, el supuesto normativo que expresamente le otorga el carácter de información reservada;
>
> II. mediante la ponderación de los intereses en conflicto, los sujetos obligados deberán demostrar que la publicidad de la información solicitada generaría un riesgo de perjuicio y por lo tanto, tendrán que acreditar que este último rebasa el interés público protegido por la reserva;
>
> III. se debe de acreditar el vínculo entre la difusión de la información y la afectación del interés jurídico tutelado de que se trate;
>
> IV. precisar las razones objetivas por las que la apertura de la información generaría una afectación, a través de los elementos de un riesgo real, demostrable e identificable;
>
> V en la motivación de la clasificación, el sujeto obligado deberá acreditar las circunstancias de modo, tiempo y lugar del daño, y
>
> VI. deberán elegir la opción de excepción al acceso a la información que menos lo restrinja, la cual será adecuada y proporcional para la protección del interés público, y deberá interferir lo menos posible en el ejercicio efectivo del derecho de acceso a la información.[1933]

1930 Artículo108 de la LGAIP y artículo 97 de la LFTAIP.

1931 "DATOS PERSONALES. LA PUBLICACIÓN DE LOS RELATIVOS AL NOMBRE O DENOMINACIÓN DE LAS PARTES EN LAS LISTAS DE LOS ASUNTOS VENTILADOS ANTE LOS ÓRGANOS JURISDICCIONALES, NO IMPLICA LA DIVULGACIÓN DE INFORMACIÓN CONFIDENCIAL NI PRECISA, POR ENDE, DE LA ANUENCIA DE AQUÉLLAS". Semanario Judicial de la Federación. Tesis: I.1o.A.E.229 A (10a.). Tesis Aislada (constitucional, administrativa).Tribunales colegiados de circuito. Décima época. Registro número 2016812. Publicada el 04 de mayo de 2018.

1932 Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales por el que se aprueban los Lineamientos Generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas. Publicado en el *Diario Oficial de la Federación* el 15 de abril de 2018. Disponible en: http://diariooficial.gob.mx/nota_detalle.php?codigo=5433280&fecha=15/04/2016

1933 Lineamiento 33 de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

De conformidad con el lineamiento anterior, para la aplicación de la prueba de daño es indispensable vincular algunas de las excepciones establecidas en el artículo 113 de la LGAIP referentes a la información reservada con el supuesto normativo correspondiente. Los sujetos obligados, al ponderar los intereses en conflicto, deberán demostrar que la reserva de la información en cuestión genera un mayor beneficio que su publicidad señalando el interés jurídico tutelado, tomando en cuenta la proporcionalidad de la medida y buscando en todo momento no interferir en el ejercicio del derecho de acceso a la información. Además, deberá acreditar que existe un riesgo real, demostrable e identificable.

La Primera Sala de la SCJN determinó que la prueba de daño consiste "en la facultad de la autoridad que posee la información solicitada para ponderar y valorar mediante la debida fundamentación y motivación, el proporcionarla o no, en tanto que su divulgación ponga en riesgo o pueda causar un perjuicio real al objetivo o principio que trata de salvaguardar, y de manera estricta debe demostrarse que el perjuicio u objetivo reservado, resulta mayormente afectado que los beneficios que podrían lograrse con la difusión de la información".[1934]

El sujeto obligado que ostenta la información deberá ponderar y evaluar de manera fundada y motivada si al reservar la información solicitada se obtienen mayores beneficios y menores afectaciones que la difusión de la misma ya que la difusión de información lesionaría el interés jurídico tutelado. Para declarar la reserva de la información, el sistema normativo establece un método de ponderación para los sujetos obligados que parte de la premisa de la a existencia de una colisión entre derechos cuya valoración se basa en los intereses en juego.[1935]

El desafío que tienen los sujetos obligados para motivar y fundar adecuadamente la prueba de daño y poder cumplir con los requisitos establecidos en los Lineamientos es grande, ya que se requiere generar capacidades institucionales y profesionales del personal a cargo y una capacitación continua. Debido a que la reserva de la información pública es una excepción al principio de máxima publicidad consagrado en la Constitución, el estándar de ponderación para hacerlo efectivo es alto por lo que el fortalecimiento de las capacidades del personal a cargo debe convertirse en una prioridad institucional.

Puesta a disposición del aviso de privacidad

Jorge Antonio Orta Villar

Resulta indudable que el aviso de privacidad[1936] es punto de partida y eje central sobre el cual versan los derechos y obligaciones de los sujetos involucrados en la relación jurídica que se origina a partir de los datos personales.

No contar con el soporte de un aviso de privacidad será causa de sanción por incumplimiento de las obligaciones establecidas en la normatividad de la materia.

1934 AVERIGUACIÓN PREVIA. LA PRUEBA DE DAÑO PREVISTA EN LAS LEYES FEDERAL Y GENERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA, INSTITUIDA PARA DETERMINAR SI SE PERMITE EL ACCESO A INFORMACIÓN RESERVADA, ES INAPLICABLE PARA QUIENES SON PARTE EN LA INDAGATORIA, POR LO QUE UTILIZARLA PARA RESTRINGIRLES EL ACCESO A LAS CONSTANCIAS QUE LA INTEGRAN, CONSTITUYE UNA CARGA DESPROPORCIONADA, INCOMPATIBLE CON EL DERECHO DE DEFENSA ADECUADA. *Semanario Judicial de la Federación*. Tesis: I.9o.P.183 P (10a.). Tesis aislada (constitucional). Tribunales colegiados de circuito. Décima época. Registro número: 2016501. Publicación: 23 de marzo de 2018.

1935 Upegui, J. (2018). *Crítica a la ponderación como test de proporcionalidad para decidir sobre la publicidad de la información personal en poder del Estado en México.* Instituto de Investigaciones Jurídicas-UNAM, p. 40. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-informacion/issue/archive

1936 Artículo 3, fracción II de la LGPDPPSO.

Se debe recordar que para efectos de demostrar la puesta a disposición del aviso de privacidad al titular, la carga de la prueba recaerá, en todos los casos, en el responsable del tratamiento.

Mediante la puesta a disposición del aviso de privacidad, el responsable cumple con el principio de información, el cual consiste en informar a los titulares sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales.

La expresión "puesta a disposición" implica la obligación del responsable del tratamiento de hacer del conocimiento del titular de quien recaba datos personales el aviso de privacidad. El "hacer del conocimiento" el aviso de privacidad no significa realizar su entrega física o proporcionar una copia al titular, sino dárselo a conocer.

El responsable podrá cumplir con esta obligación a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, en un lugar visible y de fácil consulta, utilizando alguna de las modalidades que la normatividad prevé.

La normatividad del sector privado establece tres modalidades o tipos de avisos de privacidad: el integral, el simplificado y el corto. En cambio, en la esfera pública únicamente se regulan dos modalidades: la integral y la simplificada.

En el sector privado, la modalidad en la que deberá ponerse a disposición del titular el aviso de privacidad estará condicionada por la manera en que el responsable obtenga los datos personales del titular.

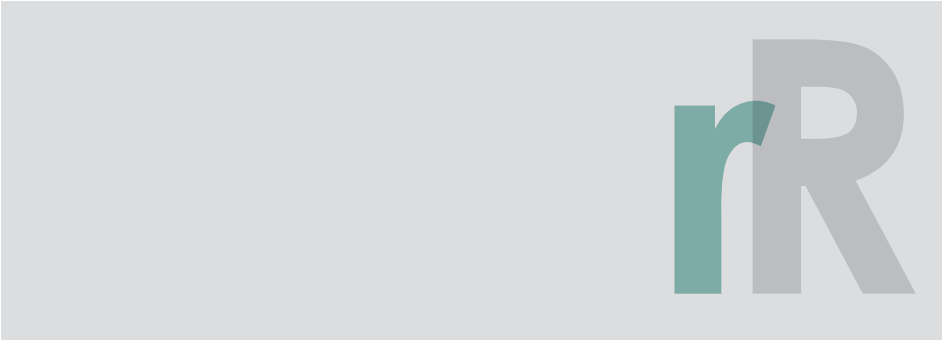
Por su parte, en el sector público las reglas respecto de la modalidad que deberá utilizarse para poner a disposición del titular el aviso de privacidad son que en un primer momento será la modalidad "simplificada" que deberá utilizar el responsable, no obstante, si el responsable lo cree conveniente, se podrá poner a disposición en su modalidad "integral". En todo caso, el aviso de privacidad integral deberá estar publicado, de manera permanente, en el medio señalado en el aviso de privacidad simplificado.

Podemos afirmar que en términos de la normatividad aplicable de datos personales en México, el principio de información se materializa físicamente a través de la puesta a disposición del aviso de privacidad al titular de los datos personales, quien será sujeto a tratamiento. De este punto reviste el rol protagónico que tiene el concepto de "puesta a disposición del aviso de privacidad" en la normatividad de datos personales en México, ya que la única manera que un responsable puede cumplir con el principio de información es acreditando la puesta a disposición del titular de su aviso de privacidad.

NOTAS

NOTAS

NOTAS



Recomendaciones de Seguridad

Christian Paredes González

Las Recomendaciones en Materia de Seguridad de Datos Personales (Recomendaciones de Seguridad)[1937] fueron publicadas por el otrora Instituto Federal de Acceso a la Información y Protección de Datos (actual Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales o INAI) el 30 de octubre de 2013. La fracción IV del artículo 39 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) le otorga la facultad para emitir criterios y recomendaciones para el funcionamiento y operación de la LFPDPPP.

1. Objeto

Las Recomendaciones de Seguridad emitidas tienen por objeto que los responsables y encargados tengan un marco de referencia de las acciones que se consideran como las mínimas necesarias para la seguridad de los datos personales. Es decir, las Recomendaciones de Seguridad pretenden servir como orientación y, eventualmente, como criterios a los particulares para determinar los procedimientos y mecanismos a aplicar para la seguridad de los datos personales.

En las Recomendaciones de Seguridad, la autoridad de protección de datos personales de manera general recomienda para la seguridad de los datos personales, la adopción de un sistema de gestión de seguridad de datos personales (SGSDP) basado en el ciclo PHVA (planear-hacer- verificar-actuar).

2. Alcance

En cuanto a su alcance, se señala en el texto de las Recomendaciones de Seguridad, que son de carácter voluntario, por lo que los responsables y encargados podrán decidir libremente qué metodología conviene más aplicar en su negocio para la seguridad de los datos personales.

El seguimiento de las Recomendaciones no exime a los responsables y encargados de su responsabilidad en relación con cualquier vulneración que pudiera ocurrir a sus bases de datos, ya que la seguridad de dichas bases depende de una correcta implementación de las medidas o controles de seguridad.

1937 Recomendaciones en materia de seguridad de datos personales. Disponible en: http://inicio.ifai.org.mx/MarcoNormativo-Documentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf

De acuerdo con el texto de las Recomendaciones, el alcance del SGSDP es la protección de los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Por lo cual, el análisis de riesgos y las medidas de seguridad implementadas como resultado del seguimiento de las Recomendaciones se deberán enfocar en la protección de datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, así como en evitar las vulneraciones descritas en el artículo 63 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).

3. Contenido de las Recomendaciones

De acuerdo con las Recomendaciones de Seguridad, las acciones mínimas a realizar en el SGSDP son las siguientes:

Fase 1. Planear el SGSDP	
Paso 1	Alcance y objetivos. Consideraciones respecto al tratamiento de datos personales y al modelo de negocios de la organización.
Paso 2	Política de gestión de datos personales. El compromiso formal documentado de la alta gerencia hacia el tratamiento adecuado de datos personales en la organización.
Paso 3	Funciones y obligaciones de quienes traten datos personales. Asignación de responsabilidades para la implementación del SGSDP.
Paso 4	Inventario de datos personales. Identificación de los tipos de datos y su flujo.
Paso 5	Análisis de riesgo de los datos personales. a) Factores para determinar las medidas de seguridad. Conjunto de consideraciones que las organizaciones deben plantear como directrices para tratar el riesgo en función de sus alcances y objetivos. b) Valoración respecto al riesgo. Proceso de ponderación para identificar los escenarios de riesgo prioritarios y darles tratamiento proporcional.
Paso 6	Identificación de las medidas de seguridad y análisis de brecha. Proceso de evaluación de las medidas de seguridad que ya existen en la organización contra las que sería conveniente tener. Los controles de seguridad, sin que sean limitativos, deben considerar los siguientes dominios: a) políticas del SGSDP b) cumplimiento legal c) estructura organizacional de la seguridad d) clasificación y acceso de los activos e) seguridad del personal f) seguridad física y ambiental g) gestión de comunicaciones y operaciones h) control de acceso i) desarrollo y mantenimiento de sistemas j) vulneraciones de seguridad

Fase 2. Implementar y operar el SGSDP	
Paso 7	Implementación de las medidas de seguridad aplicables a los datos personales. Cumplimiento cotidiano de medidas de seguridad. Consideraciones para el trabajo cotidiano con datos personales, así como el plan de tratamiento del riesgo de los activos relacionados a los mismos. Plan de trabajo para la implementación de las medidas de seguridad faltantes. Proceso en el que se decide y se implementa el tratamiento adecuado para un riesgo o grupo de riesgos respecto al contexto de la organización.
Fase 3. Monitorear y revisar el SGSDP	
Paso 8	Revisiones y auditoría. Proceso de revisión del funcionamiento del SGSDP respecto a la política establecida, cada vez que exista un cambio en el contexto del alcance y objetivos del SGSDP. Revisión de los factores de riesgo. Consideraciones para monitorear el estado del riesgo y aplicar las modificaciones pertinentes para mejorar el SGSDP. Auditoría. Requerimientos para los procesos de auditoría interna/externa. Vulneraciones a la seguridad de la información. Consideraciones en caso de un incidente de seguridad.
Fase 4. Mejorar el SGSDP	
Paso 9	Mejora continua y capacitación. Consideraciones para incluir la protección de datos en la cultura de la organización y mantener siempre actualizado el SGSDP. Mejora continua. La aplicación de medidas preventivas y correctivas sobre el SGSDP. Capacitación. Programas de mejora en la capacitación al personal para mantener la vigencia del SGSDP.

Finalmente, no debe obviarse que las Recomendaciones de Seguridad tienen plena correspondencia con las medidas de seguridad exigidas por el capítulo III del RLFPDPPP para garantizar la seguridad de los datos personales sujetos a tratamiento.

Reconducción de la denuncia

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La reconducción del procedimiento es un acto procesal mediante el cual la unidad administrativa que recibió la denuncia o, en su caso, la solicitud de protección de derechos, turna a la unidad administrativa competente la denuncia o solicitud de protección de derechos recibida, al no ser la unidad administrativa receptora la competente para sustanciar el procedimiento que en términos de la normatividad corresponde iniciarse derivado de los hechos denunciados.

1. Particularidades

La reconducción del procedimiento, como acto jurídico procesal, suele ser consecuencia de una confusión por parte de la persona que acude ante la autoridad para presentar una inconformidad al no saber distinguir si los hechos ocurridos son materia de un procedimiento de protección de derechos, o bien de un procedimiento de investigación y verificación. Pueden presentarse dos supuestos en los que opera la figura de reconducción del procedimiento:

El primero de ellos es cuando la denuncia presentada no refiere a los procedimientos de investigación y verificación, sino que actualiza alguna de las causales de procedencia del procedimiento de protección de derechos. Las causales de procedencia del procedimiento de protección de derechos están previstas en el artículo 115 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), el cual para pronta referencia citamos a continuación:

> Artículo 115. El procedimiento de protección de derechos procederá cuando exista una inconformidad por parte del titular, derivada de acciones u omisiones del responsable con motivo del ejercicio de los derechos ARCO cuando:
>
> I. el titular no haya recibido respuesta por parte del responsable;
>
> II. el responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;
>
> III. el responsable se niegue a efectuar las rectificaciones a los datos personales;
>
> IV. el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;
>
> V. el responsable se niegue a cancelar los datos personales;
>
> VI. el responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición y
>
> VII. por otras causas que a juicio del Instituto sean procedentes conforme a la Ley o al presente Reglamento.

El segundo de ellos es cuando la solicitud de protección de derechos presentada no actualiza alguna de las causales de procedencia previstas en el artículo 115 del RLFPDPPP antes citado, sino que refiera al procedimiento de investigación y verificación.

2. Temporalidad

En cuanto a su temporalidad, según disponen el artículo 39 del RLFPDPPP y el artículo 54 de los Lineamientos de los Procedimientos, la reconducción de la denuncia debe realizarse en un plazo no mayor a 10 días contados a partir del día en que se recibió la solicitud (denuncia del titular).[1938]

Registro de los esquemas de autorregulación vinculante

Rosa María Franco Velázquez

El Registro de los Esquemas de Autorregulación Vinculante (REA) es la base de datos administrada por el Instituto Nacional de Transparencia, Acceso a la Información y Pro-

1938 Los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones señalan:
Artículo 54. Durante el estudio y análisis de la descripción de los hechos, así como a partir de la información presentada por el denunciante ante el Instituto, la Dirección General de Investigación y Verificación podrá:
I. Reconducir la denuncia, conforme a lo dispuesto por el artículo 139 del Reglamento, si se ubica en uno de los supuestos señalados por el diverso artículo 115 del mismo ordenamiento legal, en un plazo no mayor a diez días hábiles a partir de que se tuvo por presentada la denuncia.
II. Orientar al denunciante sobre las instancias legales a las que puede acudir en defensa de sus derechos, en un plazo no mayor a diez días hábiles a partir de que se haya tenido por presentada la denuncia.
III. Prevenir al denunciante, en caso de que su denuncia no sea clara, o bien, no cumpla con los elementos que señala el artículo 51 de los presentes Lineamientos.
Si el denunciante no diera contestación a la prevención de referencia, en un término no mayor a cinco días hábiles, se tendrá por desechada la misma.

tección de Datos Personales (INAI), conformada por expedientes y documentos físicos y electrónicos, la cual tiene la función de organizar, administrar, gestionar, facilitar el acceso y difundir información de los esquemas de autorregulación vinculante[1939] en materia de protección de datos personales, así como transparentar información relacionada con:

a) las reglas emitidas para adaptar la normativa en materia de protección de datos personales, a las que refiere el capítulo II de los Parámetros (reglas para adaptar la normativa o buenas prácticas), cuando el INAI y los interesados así lo consideren pertinente;
b) el listado de esquemas de autorregulación validados por el INAI o con certificación reconocida, e información relacionada con ellos que sea relevante para el público interesado;
c) aquellas entidades de acreditación autorizadas por la Secretaría de Economía en términos de la Ley Federal sobre Metrología y Normalización, y reconocidas por el INAI.
d) los organismos de certificación con acreditación reconocida por el INAI;
e) los responsables y encargados que se hayan adherido a algún esquema, y
f) los esquemas de autorregulación internacionales reconocidos fuera del territorio mexicano, con su respectiva equivalencia con la normativa mexicana en la materia, que hayan sido admitidos por el INAI.[1940]

La información anterior deberá publicarse de forma tal que facilite el acceso a la misma, su uso y comprensión. Con excepción de la información que se encuentre clasificada como reservada o confidencial con fundamento en la Ley Federal de Transparencia y Acceso a la Información Pública, el INAI podrá determinar procedente el acceso y difusión a otra información no prevista anteriormente que forme parte del REA.[1941]

Las reglas para la operación del REA se establecieron a través del acuerdo del Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, por el que se aprueba el Proyecto de Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante y se instruye su publicación oficial.[1942]

Reglamento General de Protección de Datos

Alejandro Alday González

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD o GDPR por sus siglas en inglés) es aplicable a partir del 25 de mayo de 2018, y constituye una norma de aplicación directa en el territorio de la Unión Europea que tiene por objeto establecer las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de tales datos, así como proteger

1939 Numeral 84 de los Parámetros de Autorregulación en materia de Protección de Datos Personales, publicados en el *Diario Oficial de la Federación* el 29 de mayo de 2014. (Los Parámetros).

1940 Preguntas frecuentes. Registro de Esquemas de Autorregulación Vinculante (REA), mismas que pueden ser consultadas en la siguiente liga: http://rea.inai.org.mx/_catalogs/masterpage/Sec1_3.aspx

1941 En la página de internet del REA, www.rea.ifai.org.mx, se podrá encontrar información relativa a los certificados otorgados, las oficinas de los responsables o encargados certificados, el alcance de sus certificaciones, así como los vínculos a los sitios de internet de las personas morales que han sido certificadas en materia de protección de datos personales.

1942 Acuerdo del Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, por el que se aprueba el Proyecto de Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante y se instruye su publicación oficial; publicado en el *Diario Oficial de la Federación* el 18 de febrero de 2015.

los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de datos personales.[1943]

1. Antecedentes

El RGPD[1944] es resultado de un amplio proceso deliberativo iniciado en 2010 con la invitación que el Consejo Europeo extendió a la Comisión Europea (CE) para evaluar el funcionamiento de los diversos instrumentos relativos a la protección de datos personales y presentar propuestas tendentes a reformar el régimen existente. Anteriormente, en la resolución de 2009 sobre el Programa de Estocolmo,[1945] el Parlamento Europeo sostuvo una postura favorable en torno a la elaboración de un régimen general de protección de datos para la Unión Europea (UE), y más tarde, hacia finales de 2010, la CE reconoció la necesidad de garantizar que el derecho fundamental a la protección de datos de carácter personal se aplicara de manera congruente en todas las políticas de la UE.[1946]

Como resultado de las discusiones y consultas con los interesados, el 6 de julio de 2011, el Parlamento Europeo adoptó una resolución[1947] que coincidía con el enfoque de la CE para efectuar una revisión y armonización del marco normativo de la UE en materia de protección de datos. Ello consideró el apoyo que el Consejo de la Unión Europea manifestó a la CE el 24 de febrero de 2011 para modificar el régimen de protección de datos, posición que fue avalada también por el Comité Económico y Social Europeo en su dictamen del 16 de junio de 2011.[1948]

El 27 de enero de 2012, la CE elaboró una propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.[1949]

La propuesta de reglamento general de protección de datos fue sometida a diversas modificaciones por más de tres años, hasta que el Consejo de la Unión Europea, el Parlamento Europeo y la CE consensuaron el contenido del RGPD el 15 de diciembre de 2015. El 17 de diciembre de 2015 la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del

1943 Artículo 1
Objeto
1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.
2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.
3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

1944 La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, es el antecedente normativo inmediato cuyo objeto consistía en garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

1945 Resolución del Parlamento Europeo, de 25 de noviembre de 2009, sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada "Un espacio de libertad, seguridad y justicia al servicio de los ciudadanos - Programa de Estocolmo", [P7_TA (2009)0090].

1946 Comunicación titulada "Un enfoque global de la protección de los datos personales en la Unión Europea", COM (2010) 609 final.

1947 Resolución del Parlamento Europeo, de 6 de julio de 2011, sobre un enfoque global de la protección de los datos personales en la Unión Europea, [P7TA(2011)0323].

1948 Dictamen del Comité Económico y Social Europeo sobre la "Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Un enfoque global de la protección de los datos personales en la Unión Europea". [COM(2010) 609 final].

1949 Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF

Parlamento Europeo aprobó el texto emanado de los diálogos tripartitas, y posteriormente el Comité de Representantes Permanentes de los Gobiernos de los Estados miembros (Coreper) confirmó que el documento se presentaría para su adopción por parte del Consejo de la Unión Europea, y subsecuentemente, del Parlamento Europeo.

El 8 de abril de 2016, el Consejo de la Unión Europea adoptó su posición en primera lectura sobre la propuesta de reglamento general de protección de datos.[1950] Por su parte, el Parlamento Europeo aprobó el texto el 14 de abril de 2016.[1951]

Finalmente, el 4 de mayo de 2016 se publicó en el *Diario Oficial de la Unión Europea* el RGPD. El RGPD es de aplicación obligatoria desde el 25 de mayo de 2018.

2. Ámbito de aplicación material

De conformidad con el artículo 2, el RGPD se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Esto significa que la protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él (considerando 15 del RGPD).

Conforme al párrafo 2 del artículo 2, el RGPD no es aplicable al tratamiento de datos personales:

a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del derecho de la UE.[1952]

b) Por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del Tratado de la Unión Europea.

c) Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas.[1953]

d) Por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.[1954]

1950 Posición del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo Y Del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). [Documento 52016AG0006(01)].

1951 Resolución legislativa del Parlamento Europeo, de 14 de abril de 2016, respecto de la posición del consejo en primera lectura con vistas a la adopción del Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. (Reglamento General de Protección de Datos). (05419/1/2016 – C8-0140/2016 – 2012/0011 COD). (Procedimiento legislativo ordinario: segunda lectura). [P8TA(2016)0125].

1952 En este sentido, el considerando 16 dispone que el RGPD no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con actividades excluidas del ámbito del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

1953 En este sentido, el considerando 18 del RGPD dispone lo siguiente: "El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas".

1954 El considerando 19 del RGPD indica:
La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación

De la misma forma, es pertinente precisar que el RGPD tampoco se aplica a la protección de datos personales de personas fallecidas (considerando 27).

3. Ámbito de aplicación territorial

De conformidad con el párrafo 1 del artículo 3, el RGPD se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la UE, independientemente de que el tratamiento tenga lugar en la UE o no.

Asimismo, según dispone el párrafo 2 del artículo 3, el RGPD también es aplicable al tratamiento de datos personales de interesados que residan en la UE por parte de un responsable o encargado no establecido en la Unión,[1955] cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la UE, independientemente de si a estos se les requiere su pago o b) el control de su comportamiento, en la medida en que este tenga lugar en la UE.[1956]

Finalmente, en consonancia con lo dispuesto en el apartado 3 del artículo tercero, el RGPD también se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la UE sino en un lugar en que el derecho de los Estados miembros sea de aplicación en virtud del derecho internacional público.

---

de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo. Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

1955 En este respecto, el considerando 22 del RGPD precisa lo siguiente:
Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

1956 En este sentido el considerando 23 del RGPD dispone lo siguiente:
Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que residen en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio *web* del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

4. Contenido

El RGPD se compone de 173 considerandos y 99 artículos distribuidos en 11 capítulos. Los capítulos del RGPD tienen el siguiente orden y contenido:

a) Capítulo I. Disposiciones generales: se establece el objeto, ámbito de aplicación material, ámbito territorial y definiciones (datos personales, tratamiento, limitación del tratamiento, elaboración de perfiles, seudonimización, responsable del tratamiento, encargado del tratamiento, destinatario, tercero, consentimiento del interesado, violación de la seguridad de los datos personales, datos genéticos, datos biométricos, datos relativos al a salud, establecimiento principal, representante, empresa, grupo empresarial, normas corporativas vinculantes, autoridad de control, autoridad de control interesada, tratamiento transfronterizo, objeción pertinente y motivada, servicio de la sociedad de la información, organización internacional).

b) Capítulo II. Principios: se establecen como principios aplicables al tratamiento: licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del plazo de conservación, integridad y confidencialidad y responsabilidad proactiva.

c) Capítulo III. Derechos del interesado: se reconoce el derecho de transparencia y las modalidades de ejercicio de los derechos del interesado, el derecho de información y acceso a los datos personales, el derecho de rectificación y supresión, el derecho a la limitación del tratamiento, el derecho a la portabilidad de los datos, el derecho de oposición y decisiones individuales automatizadas y las limitaciones a tales derechos anteriores.

d) Capítulo IV. Responsable del tratamiento y encargado del tratamiento: se establecen las obligaciones generales del responsable y de los corresponsables del tratamiento, obligaciones de seguridad de datos personales, aspectos relacionados con las evaluaciones de impacto en la protección de datos y consulta previa, la figura del delegado de protección de datos y los códigos de conducta y esquemas certificación.

e) Capítulo V. Transferencias de datos personales a terceros países u organizaciones internacionales: se establece, entre otras cosas, que solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del RGPD, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el dicho capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional.

f) Capítulo VI. Autoridades de control independientes: entre otros aspectos, establece la obligación de cada Estado de fijar como responsabilidad de una o varias autoridades públicas independientes (autoridad de control) la supervisión de la aplicación del RGPD, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la UE.

g) Capítulo VII. Cooperación y coherencia: sienta las bases para la colaboración entre la autoridad de control principal y las demás autoridades de control interesadas y prevé que la autoridad de control principal coopere con las demás autoridades de control interesadas esforzándose en alcanzar consensos bajo las condiciones establecidas en el propio RGPD.

h) Capítulo VIII. Recursos, responsabilidad y sanciones: se establece que todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de

trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el RGPD. De la misma forma, se prevé la responsabilidad derivada del incumplimiento al RGPD y las sanciones.

i) Capítulo IX. Disposiciones relativas a situaciones específicas de tratamiento: se incorporan disposiciones específicas para regular cuestiones relacionadas con el tratamiento y la libertad de expresión y de información, el tratamiento y acceso del público a documentos oficiales, el tratamiento del número nacional de identificación, el tratamiento en el ámbito laboral, las garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, las obligaciones de secreto, y las normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.

j) Capítulo X. Actos delegados y actos de ejecución: contempla las condiciones a las que se sujetan los actos delegados otorgados a la CE.

k) Capítulo XI. Disposiciones finales: borda la derogación de la Directiva 95/46/CE, la relación del RGPD con la Directiva 002/58/CE (directiva sobre la privacidad y las comunicaciones electrónicas), la relación con los acuerdos celebrados anteriormente, los informes de la CE, la revisión de actos jurídicos de la UE en materia de protección de datos, así como la entrada en vigor y aplicación.

El RGPD es la norma de protección de datos más avanzada hasta el momento para proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

Reglamento interior del IFAI (actualmente INAI)

Ángel Trinidad Zaldívar y
Marina San Martín Rebolloso

Un reglamento "es una norma que complementa y amplía el contenido de una ley, por lo que jerárquicamente aquél está subordinado a ésta y corre la misma suerte; de tal manera que, si una ley es reformada, derogada o abrogada, el reglamento se verá afectado con las mismas consecuencias, a pesar de que no se hubiese reformado, derogado o abrogado expresamente por otro reglamento, ya que éste no goza de la autoridad formal de una ley, que sí requiere que toda modificación sea expresa".[1957]

La expedición de reglamentos interiores se especifica como una facultad del presidente de la República[1958] para establecer las atribuciones de las unidades administrativas de cada una de las secretarías de Estado de la administración pública federal,[1959] las leyes o decretos de creación de entidades de la administración pública paraestatal pueden conferir a su órgano de gobierno o similar la potestad de expedir su reglamento interior.

La posibilidad de que las entidades descentralizadas emitan la normativa que regule su organización y actividad al interior "deriva de la autonomía orgánica y jurídica que las

1957 Instituto de Investigaciones Jurídicas. (1997). *Diccionario Jurídico Mexicano*. 10ª ed. México. Porrúa-UNAM. Tomo P-Z, p. 2751.

1958 De acuerdo con el artículo 89, fracción I, constitucional, es facultad y obligación del presidente "promulgar y ejecutar las leyes que expida el Congreso de la Unión, proveyendo en la esfera administrativa a su exacta observancia". Véase, Constitución Política de los Estados Unidos Mexicanos, *Diario Oficial de la Federación*, 5 de febrero de 1917 (última reforma 15-09-2017).

1959 Artículo 18 de la Ley Orgánica de la Administración Pública Federal (LOAPF), *Diario Oficial de la Federación,* 29 de diciembre de 1976 (última reforma 15-06-2018).

caracteriza y que les permite gobernarse a sí mismas y expedir las normas internas necesarias para su adecuado funcionamiento y eficaz cumplimiento de su objeto social".[1960]

En el caso del Instituto Federal de Acceso a la Información Pública (IFAI), actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), de acuerdo con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) de 2002, y conforme a su decreto de creación,[1961] nació como un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio, parte de la administración pública federal; con autonomía operativa, presupuestaria y de decisión, para ser el encargado de promover el ejercicio del derecho de acceso a la información; resolver sobre la negativa de las solicitudes de información y proteger los datos personales en poder de las dependencias y entidades,[1962] otorgándole la facultad, a través de su órgano máximo de dirección,[1963] de la elaboración y expedición de su reglamento interior.[1964]

Un reglamento interior "no puede otorgar más atribuciones a la dependencia o entidad que las que expresamente le confiere la ley. Su función es distribuir las atribuciones legales entre sus distintas unidades administrativas",[1965] es decir, debe especificar y describir la organización interna de una institución, establecer sus áreas administrativas, el nivel jerárquico entre ellas, definir sus actividades acordes con las disposiciones que la regulan, así como prever los casos de suplencia de los servidores públicos.

En el propio decreto de creación del Instituto se previó que, en su reglamento interior se detallarían las facultades de los secretarios designados por el Pleno, encargados de las actividades administrativas, operativas y de sustanciación de los procedimientos, y en su caso, del personal de dirección y de apoyo; así como las demás competencias necesarias para su organización y funcionamiento.[1966]

1. Reglamentos interiores del Instituto y sus modificaciones

La normativa del IFAI que regula su organización y actuación al interior ha sufrido modificaciones diversas a lo largo de su existencia, en razón de que sus facultades se han transformado y ampliado en distintas materias, tanto por mandato constitucional como por nuevas leyes.

Los comisionados del Instituto aprobaron el primer reglamento interior el 5 de junio de 2003. En dicho reglamento se consideraban dos secretarías: una ejecutiva y otra de acuer-

1960 Reglamento interior es "el instrumento jurídico que expide el Ejecutivo Federal, en ejercicio de la facultad que le confiere el artículo 89, fracción I, de la Constitución, con el objeto de reglamentar las disposiciones legales que confieren atribuciones a las dependencias del Ejecutivo, determinando la distribución de dichas atribuciones entre las diferentes unidades administrativas de cada dependencia; así como para definir la forma en que los titulares podrán ser suplidos durante sus ausencias". Véase, Instituto de Investigaciones Jurídicas. (1997). *Diccionario Jurídico Mexicano*. 10ª ed. México. Porrúa-UNAM. Tomo P-Z, p. 2755.

1961 Artículos 1º y 2º del Decreto del Instituto Federal de Acceso a la Información Pública (Decreto del IFAI), *Diario Oficial de la Federación*, 24 de diciembre de 2002.

1962 Artículo 33 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), *Diario Oficial de la Federación*, 11 de junio de 2002.

1963 La administración de los organismos descentralizados estará a cargo de un órgano de gobierno que podrá ser una junta de gobierno o su equivalente y un director general, el cual estará integrado por no menos de cinco ni más de 15 miembros propietarios y de sus respectivos suplentes, y será presidido por el titular de la coordinadora de sector o por la persona que éste designe. Véase, artículos 17 y 18 de la Ley Federal de las Entidades Paraestatales (LFEP), *Diario Oficial de la Federación*, 14 de mayo de 1986 (última reforma 15-06-2018).

1964 Artículo 37, fracción XVI, y séptimo transitorio de la LFTAIPG.

1965 Instituto de Investigaciones Jurídicas. (1997). *Diccionario Jurídico Mexicano*. 10ª ed. México. Porrúa-UNAM. Tomo P-Z, p. 2756

1966 Artículo 6 del decreto del IFAI.

dos; así como diversas direcciones generales siendo una de ellas la de protección de datos personales adscrita a la segunda secretaría,[1967] en razón de que, desde la LFTAIPG de 2002, se planteaba entre sus objetivos, garantizar la protección de los datos personales en posesión de los sujetos obligados (se incluía una definición de éstos), se preveía un capítulo específico con seis artículos sobre su salvaguarda[1968] y contenía disposiciones para solicitar acceso y para su corrección, sobre la inconformidad en la atención a dichas peticiones, entre otras.

Cuatro años más tarde, un segundo reglamento interior, que abrogó al de 2003, fue publicado en el *Diario Oficial de la Federación* el 2 de mayo de 2007. En materia de datos personales, en este nuevo instrumento se unificaron las direcciones generales de clasificación y de datos personales en una sola.[1969] A diferencia del anterior reglamento, se desglosaron las funciones específicas de cada dirección general, correspondiendo a la mencionada, entre otras, apoyar en la sustanciación de los medios de impugnación interpuestos ante el Instituto a través de la elaboración de dictámenes, estudios y opiniones en materia de clasificación, datos personales y archivos, además de proponer los criterios para la organización y conservación de documentos, y para el manejo, mantenimiento, seguridad y protección de los datos personales.[1970]

En abril de 2009 se volvió a modificar el reglamento (desaparece la secretaría técnica del Pleno)[1971] y el 1 de junio de 2009 tiene lugar la reforma constitucional al artículo 16 que adiciona el derecho de las personas "a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros".[1972]

Esta reforma constitucional da lugar a que el 5 de julio de 2010 se expida la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que le encomendó nuevas atribuciones, cambiando la denominación del Instituto Federal de Acceso a la Información Pública por Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).[1973]

En razón de lo anterior, en el año 2011 ocurrieron dos modificaciones al reglamento interior del IFAI en su estructura orgánica y operación. La primera crea una secretaría de protección de datos personales, encargada de desarrollar las temáticas, normativas y procedimientos en esta materia derivados de la LFPDPPP y de la LFTAIPG. Además, se ampliaron las direcciones generales añadiendo la de asuntos internacionales, autorregulación, de normatividad y estudios, sanciones, de protección de derechos y de verificación.[1974]

1967 Artículos 6, fracciones IV, V y VI inciso j, y 26, fracción I, del Reglamento Interior del Instituto Federal de Acceso a la Información Pública (Reglamento Interior del IFAI 2003), *Diario Oficial de la Federación*, 11 de junio de 2003.

1968 Artículos 3, fracción II, 4, fracción III y capítulo IV "Protección de Datos Personales" de los artículos 20 al 26 de la LFTAIPG.

1969 Artículos 6, fracción VII, inciso d y 36, fracción I, del Reglamento Interior del Instituto Federal de Acceso a la Información Pública (Reglamento Interior del IFAI 2007), *Diario Oficial de la Federación*, 2 de mayo de 2007.

1970 Artículo 30, fracciones I y V, del Reglamento Interior del IFAI 2007.

1971 Se deroga la fracción VIII del artículo 6 y el capítulo octavo "De la Secretaría Técnica del Pleno". Véase: modificación al reglamento interior del instituto federal de acceso a la información pública (modificación al reglamento interior del IFAI 2009), *Diario Oficial de la Federación*, 8 de abril de 2009.

1972 Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, *Diario Oficial de la Federación*, 1º de junio de 2009.

1973 Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II, del título segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, *Diario Oficial de la Federación*, 5 de julio de 2010.

1974 Artículo 6, fracciones V bis y VII, y capítulo sexto "De la Secretaría de Protección de Datos Personales". Véase: modificación al reglamento interior del instituto federal de acceso a la información pública (modificación al reglamento interior del IFAI 2011), *Diario Oficial de la Federación*, 28 de abril de 2011.

El segundo cambio implicó diversos ajustes entre los que destacan el cambio de la Secretaría Ejecutiva por una secretaría general, la Secretaría de Acuerdos por Secretaría de Acceso a la Información o la Dirección General de Sanciones por Dirección General de Sustanciación y Sanción. También se creó la Dirección General de Políticas de Acceso, se agregó la parte de datos personales a la Dirección General de Clasificación, se recuperó la Secretaría Técnica del Pleno y se fortaleció la organización de la Secretaría de Protección de Datos Personales teniendo como brazos de actuación a cuatro direcciones generales que son de normatividad y estudios, autorregulación, de sustanciación y sanción y de verificación[1975] para dar un mejor cumplimiento a la legislación.

En diciembre de 2011 se publicó el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), y que en enero de 2012 se expidió la Ley Federal de Archivos, en octubre de 2012 se publicó un tercer reglamento interior del IFAI, con la finalidad de alinear la estructura, atribuciones, mecanismos y procedimientos del Instituto con estas nuevas normas.[1976] Dos años después, el 20 de febrero de 2014, se publicó una cuarta versión de reglamento interior del IFAI, posterior a la reforma constitucional en materia de transparencia del 7 de febrero de ese mismo año, que cambió la naturaleza jurídica del Instituto para dejar de ser parte del Poder Ejecutivo y convertirse en un organismo constitucional autónomo.[1977] Este cambio fue necesario aún a sabiendas que con posterioridad se tendría que expedir un nuevo ordenamiento adecuado a la legislación que emitiera el Congreso de la Unión con el objeto de establecer la estructura y regular el funcionamiento y operación del nuevo IFAI.[1978]

El reglamento interior de 2014 mantuvo la mayor parte de la estructura prevista en el anterior ordenamiento de 2012, con la eliminación de la figura del órgano de gobierno; y el establecimiento de una contraloría en sustitución del órgano interno de control, cuyo titular sería designado por el Pleno del Instituto.[1979]

A raíz de la reforma constitucional en materia de transparencia de febrero de 2014, que incrementó el número de miembros del Pleno del nuevo órgano autónomo de cinco a siete, el 14 de mayo del mismo año, el Senado de la República tomó protesta a los siete nuevos comisionados del Pleno del Instituto.[1980]

A partir de estos cambios estructurales en el máximo órgano de dirección, se rediseñó y ajustó la organización y operación de las actividades institucionales, a fin de responder a los nuevos retos y estar en posibilidad de ejercer las nuevas competencias. Ello implicó tres ajustes normativos: i) la modificación a la estructura orgánica y ocupacional del IFAI

1975 Se reforman los artículos 6, fracciones V, VI, VII incisos f y l, 23 fracción XI, 24, 24 bis fracciones II, IV a XXV, 25 fracciones II, XII y XXV, 26 fracción VI y el artículo 36 y se adicionan el artículo 6 fracción VII con el inciso o, el artículo 24 bis con un último párrafo y los artículos 34 bis, 34 ter y el capítulo noveno con el artículo 35. Véase: modificación al reglamento interior del IFAI 2011.

1976 Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), *Diario Oficial de la Federación*, 21 de diciembre de 2011 y Ley Federal de Archivos, *Diario Oficial de la Federación*, 23 de enero de 2012.

1977 Artículo 6, fracción VIII, del decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*, 7 de febrero de 2014.

1978 Artículo 1 del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos (Reglamento Interior del IFAI 2014), *Diario Oficial de la Federación*, 20 de febrero de 2014.

1979 Artículo 5º del Reglamento Interior del IFAI 2014.

1980 Comunicado-801, presidente del Senado toma protesta a comisionados del organismo garante de la transparencia. Senado de la República, 14 de mayo de 2014. Disponible en: http://comunicacion.senado.gob.mx/index.php/informacion/boletines/12673-presidente-del-senado-toma-protesta-a-comisionados-del-organismo-garante-de-la-transparencia.html

para integrar nuevas unidades administrativas,[1981] ii) la creación de comisiones permanentes como instancias colegiadas de colaboración con el Pleno en las labores de supervisión, coordinación y de propuestas de políticas, programas y acciones, así como para el seguimiento de las actividades de las distintas unidades administrativas del Instituto[1982] y iii) el Reglamento para la Organización y Funcionamiento de las Comisiones del Instituto Federal de Acceso a la Información y Protección de Datos con objeto de establecer las disposiciones para la organización y adecuado funcionamiento de las comisiones.[1983]

En mayo de 2015 se publicó la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) que identifica al organismo como Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) dejando de ser IFAI.[1984] El INAI aprobó modificaciones en su estructura orgánica que dio lugar a diversos cambios profundos, entre los que destacan los siguientes:[1985]

a) se creó la coordinación del secretariado ejecutivo del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT) y una nueva Dirección General Técnica, Seguimiento y Normatividad del SNT;
b) se constituyó una coordinación técnica del Pleno, y se creó la Dirección General de Atención al Pleno;
c) dentro de la estructura de ponencias se modificó el nombre de la Dirección de Análisis y Estudios por Jefatura de Ponencia;
d) la Coordinación de Acceso a la Información se reestructura, de tal suerte que la Dirección General de Coordinación y Vigilancia de la Administración Pública Federal se rediseña en tres direcciones generales que son la de evaluación, la de enlace con sujetos obligados de la administración pública centralizada y la de enlace con organismos públicos autónomos, empresas paraestatales, entidades financieras, fondos y fideicomisos y
e) la Coordinación de Protección de Datos Personales tendrá adscritas a la Dirección General de Prevención y Autorregulación, a la de protección de derechos y sanción, a la de investigación y verificación, y a la de normatividad y consulta.

1981 Por acuerdo ACT/EXT-PLENO/PA/12/05/14.0 se integraron nuevas unidades administrativas como las direcciones generales de capacitación; de promoción y de vinculación con la sociedad; de estados y municipios; de relaciones con nuevos sujetos obligados y de asesoría y consulta; de planeación estratégica, evaluación e innovación del desempeño institucional; y de gobierno abierto y transparencia. Asimismo, el Pleno aprobó el acuerdo ACT/ORD-PLENO/PA/03/06/14.04, que modificó la estructura orgánica y ocupacional de las ponencias de los comisionados, así como la restructuración de secretarías a coordinaciones, con la modificación de su denominación de Secretaría General por Coordinación Ejecutiva, de Secretaría de Acceso a la Información por Coordinación de Acceso a la Información y de Secretaría de Protección de Datos por Coordinación de Protección de Datos Personales. Véase, acuerdo por el que se aprueba la modificación a la estructura orgánica y ocupacional del Instituto Federal de Acceso a la Información y Protección de Datos, autorizada mediante el acuerdo ACT/EXT-PLENO/PA/12/05/14.02, *Diario Oficial de la Federación*, 10 de septiembre de 2014.

1982 Las comisiones permanentes estarán conformadas por tres comisionados y son las siguientes: políticas de acceso a la información; asuntos internacionales; normativa de acceso a la información; capacitación y cultura de la transparencia; gestión documental y archivos; indicadores y evaluación; normatividad de datos personales; supervisión, vigilancia, verificación y sanciones; tecnologías de la información; gobierno abierto y transparencia; vinculación con estados y municipios; vinculación con nuevos sujetos obligados; y vinculación y promoción del derecho. Véase artículos primero y segundo del Acuerdo por el que el Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, aprueba la creación de las Comisiones Permanentes, *Diario Oficial de la Federación*, 10 de septiembre de 2014.

1983 Artículo 1 del Reglamento para la Organización y Funcionamiento de las Comisiones del Instituto Federal de Acceso a la Información y Protección de Datos, *Diario Oficial de la Federación*, 10 de septiembre de 2014.

1984 Artículo 3, fracción XIII, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), *Diario Oficial de la Federación*, 4 de mayo de 2015.

1985 Acuerdo ACT-PUB-24-06-2015.04 mediante el cual se aprueban las modificaciones a la estructura orgánica del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Diario Oficial de la Federación*, 1 de julio de 2015.

2. Estatuto Orgánico del INAI y sus reformas

En mayo de 2016 se emitió la nueva Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) en la cual se establece, entre otros aspectos, el mandato al Instituto de expedir su estatuto orgánico y los lineamientos necesarios para el ejercicio de sus atribuciones, de conformidad con lo previsto en la misma.[1986]

En ese tenor, el 17 de enero de 2017 se publicó el Estatuto Orgánico del INAI, que abroga al Reglamento Interior del IFAI de 2014,[1987] en el cual se mantiene el Pleno, los comisionados con su presidente y las comisiones. No obstante, en el caso de las coordinaciones de acceso a la información; ejecutiva; del secretariado ejecutivo del SNT; de protección de datos personales y técnica del Pleno cambian su denominación para llamarse, respectivamente, Secretaría de Acceso a la Información, Secretaría Ejecutiva, Secretaría Ejecutiva del SNT, Secretaría de Protección de Datos Personales y Secretaría Técnica del Pleno. De igual manera, la contraloría interna pasó a ser órgano interno de control.[1988] Se mantuvieron diversas direcciones generales y otras cambiaron de denominación.[1989]

El 26 de enero de 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que establece las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.[1990]

Con motivo de la expedición de dicha Ley, en febrero de 2018, se modificó el estatuto orgánico del INAI para que las unidades administrativas cuenten con las atribuciones necesarias para dar cumplimiento a las obligaciones previstas en dicho ordenamiento. En ese sentido, se hacen ajustes en la Secretaría de Protección de Datos Personales incrementando sus atribuciones legales, se creó la Dirección General de Evaluación, Investigación y Verificación del Sector Público, se modificó el nombre de la Dirección General de Investigación y Verificación por Dirección General de Investigación y Verificación del Sector Privado y se concedieron facultades diversas a la Dirección General de Prevención y Autorregulación y a la Dirección General de Normatividad y Consulta.[1991]

Las modificaciones a la normativa interior del antes IFAI, hoy INAI, son reflejo del proceso de desarrollo y garantía de los derechos humanos de acceso a la información y protección de datos personales que a lo largo de los años de su trayectoria seguramente seguirá transformándose hasta alcanzar su consolidación y su pleno ejercicio en todo el país.

1986 Sexto transitorio de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), *Diario Oficial de la Federación*, 9 de mayo de 2016.

1987 Artículos 1 y segundo transitorio del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Estatuto Orgánico del INAI), *Diario Oficial de la Federación*, 17 de enero de 2017.

1988 Artículo 5, fracciones de la I a la IX, y último párrafo del Estatuto Orgánico del INAI.

1989 Artículo 5, fracción X del Estatuto Orgánico del INAI.

1990 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), *Diario Oficial de la Federación*, 26 de enero de 2017.

1991 Acuerdo mediante el cual se aprueban las modificaciones al Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Diario Oficial de la Federación*, 13 de febrero de 2018.

Reincidencia

Gabriel López López

Constituye una agravante de la responsabilidad por virtud del cual un mismo individuo que ha sido condenado por un delito o una infracción, comete otra conducta que se considera de naturaleza similar a la cometida y sancionada previamente.

Desde la antigüedad, la reincidencia como institución jurídica ha estado relacionada con el derecho penal. Actualmente, en la legislación mexicana se encuentra regulada dentro de los artículos 20, 21, 22, 23 y 65 del Código Penal Federal (CPF).[1992]

Conforme al CPF, la reincidencia se configura cuando existe una sentencia ejecutoria y se comete una nueva infracción sin que haya transcurrido un plazo igual al de la prescripción de la pena del primer delito. De tal manera que si el reincidente comete tres infracciones del mismo género y de la misma pasión o inclinación viciosa en un periodo que no exceda los 10 años, será considerado como delincuente habitual.

Partiendo de esta definición y tomando en cuenta la relación que mantiene el derecho penal con el derecho administrativo sancionador, se analizará la naturaleza de la reincidencia como agravante de la sanción y su alcance en la materia de protección de datos personales.

En materia de protección de datos, tanto la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados (LFPDPPP), Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos de los Procedimientos de Protección de Derechos de Investigación y Verificación y de Imposición de Sanciones (Lineamientos de Procedimiento) señalan criterios para determinar la gravedad de la sanción o las medidas de apremio por el incumplimiento de las disposiciones normativas o el indebido tratamiento de los datos personales.

En términos de lo previsto por el artículo 65, de la LFPDPPP y por el cuarto párrafo del artículo 73 de los Lineamientos de Procedimiento las resoluciones sancionatorias deberán tomar en cuenta la naturaleza del dato, la notoria improcedencia de la negativa del responsable para realizar los actos solicitados por el titular, la intencionalidad de la acción u omisión constitutiva de la infracción, la capacidad económica del responsable y la reincidencia.

Conforme a lo establecido en el artículo 157 de la LGDPPSO, la gravedad de la falta del responsable será determinada por elementos tales como el daño causado, los indicios de intencionalidad, la duración del incumplimiento de las determinaciones del Instituto o los organismos garantes y la afectación al ejercicio de sus atribuciones, la condición

1992 Artículo 20. Hay reincidencia siempre que el condenado por sentencia ejecutoria dictada por cualquier tribunal de la República o del extranjero cometa un nuevo delito, si no ha transcurrido, desde el cumplimiento de la condena o desde el indulto de la misma, un término igual al de la prescripción de la pena, salvo las excepciones fijadas en la ley. La condena sufrida en el extranjero se tendrá en cuenta si proviniere de un delito que tenga este carácter en este Código o leyes especiales.
Artículo 21. Si el reincidente en el mismo género de infracciones comete un nuevo delito procedente de la misma pasión o inclinación viciosa, será considerado como delincuente habitual, siempre que las tres infracciones se hayan cometido en un período que no exceda de diez años.
Artículo 22. En las prevenciones de los artículos anteriores se comprenden los casos en que uno solo de los delitos, o todos, queden en cualquier momento de la tentativa, sea cual fuere el carácter con que intervenga el responsable.
Artículo 23. No se aplicarán los artículos anteriores tratándose de delitos políticos y cuando el agente haya sido indultado por ser inocente.
Artículo 65. La reincidencia a que se refiere el artículo 20 será tomada en cuenta para la individualización judicial de la pena, así como para el otorgamiento o no de los beneficios o de los sustitutivos penales que la ley prevé. En caso de que el imputado por algún delito doloso calificado por la ley como grave o que amerite prisión preventiva oficiosa, según corresponda, fuese reincidente por delitos de dicha naturaleza, la sanción aplicable por el nuevo delito cometido se incrementará en dos terceras partes y hasta en un tanto más de la pena máxima prevista para éste, sin que exceda del máximo señalado en el título segundo del libro primero.

económica del infractor y la reincidencia. De los criterios normativos anteriores se desprende, en primer lugar, que la reincidencia es un factor determinante para establecer la gravedad de la conducta del responsable y se sanciona con mayor dureza al infractor que hubiese cometido múltiples infracciones en un corto periodo de tiempo dentro del mismo ámbito. Esto es así con el propósito de prevenir o evitar que la conducta punible se repita. En segundo lugar, puede verificarse que la reincidencia, calificada como un criterio agravante para graduar la sanción por la LFPDPPP, ha sido igualmente recogida por la nueva LGDPPSO y por los Lineamientos de Procedimiento materia del presente análisis.

La potestad sancionadora del INAI, como autoridad garante del derecho a la protección de datos personales, tiene su justificación en la necesidad de garantizar a las personas el derecho a la protección de su información personal, es decir, a decidir quién puede tratar sus datos personales, cómo y para qué fines. Por lo tanto, la reincidencia, como elemento para determinar la gravedad de una sanción, pretende enviar un mensaje a los sujetos obligados y particulares de que la repetición de una infracción constituye una causa para justificar una multa más grave. Se espera que esta situación jurídica desaliente la comisión de nuevas infracciones en materia de protección de datos personales.

En ese mismo sentido, resulta evidente que la reincidencia tiene una naturaleza de carácter personal al colocar al sujeto sancionado en una condición de inferioridad o desventaja comparativamente con los demás sujetos que pudieran llegar a cometer una nueva infracción. Sin embargo, no debemos pasar por alto que la reincidencia también descansa sobre bases objetivas indudables, como a) la existencia previa de una resolución que de manera fundada y motivada sanciona una determinada conducta y b) la comisión de otra infracción dentro del mismo ámbito por parte del sujeto que ha sido sancionado.

1. Delimitación conceptual y conceptos relacionados

Como se ha podido observar, la reincidencia se ha considerado normativamente como un criterio para graduar la gravedad, repetición y/o continuidad de la sanción en la comisión de una infracción. Al respecto, es preciso mencionar que la doctrina ha señalado diversos fundamentos que refuerzan este argumento.

Guillermo Cabanellas sostiene que la reincidencia es la repetición de la misma falta, culpa o delito, insistencia en los mismos. Estrictamente hablando se dice que reincidencia es la comisión de igual o análogo delito por el reo ya condenado. Agrava la responsabilidad criminal por demostrar la peligrosidad del sujeto, la ineficacia o desprecio de la sanción y la tendencia a la habitualidad.[1993] Mientras que José Alberto Garrone establece que la reincidencia es el hecho de un individuo que luego de haber sido condenado por un delito o una infracción, comete otro de igual (reincidencia especial) o de distinta naturaleza (reincidencia general).[1994] La definición más aceptada y que más fuerza adoptó al momento de legislar es aquella que se basa en el mayor reproche a quien ya conoce, a partir de su propia experiencia, el sentido de las prohibiciones jurídicas, así como las razones de prevención especial, para aquel sujeto que ha demostrado peligrosa predisposición para trasgredir el ordenamiento jurídico.[1995]

La doctrina clasifica la reincidencia en dos clases: la genérica y la específica.

a) Reincidencia genérica: existe reincidencia genérica cuando el delincuente, luego de haber cumplido la condena en todo o en parte, vuelve a recaer en la comisión de un

1993 Cabanellas de Torres, G. (2008). *Diccionario Jurídico Elemental.* Heliasta. México.

1994 Garrone, J. (1993). *Diccionario Jurídico Abeledo-Perrot.* Vol. II. Abeledo-Perrot. Argentina.

1995 Sánchez, J. (2007). *Los criterios de graduación de las sanciones administrativas en el orden social,* Lex Nova. España, p. 324.

nuevo delito diferente al cometido en la primera ocasión, es decir, que los delitos que se cometan con posterioridad no son de la misma especie que el primer delito, la reiteración está en la insistencia o repetición en una variedad o diversificación de hechos o delitos.

b) Reincidencia específica: cuando la recaída se da con la comisión del mismo delito, es decir el nuevo delito cometido posteriormente es el mismo que el primero. Aunque algunos autores señalan que también puede ser un delito análogo o uno de igual o semejante naturaleza.[1996]

2. La reincidencia y el principio constitucional non bis in idem

El Principio *non bis in idem* (no dos veces por igual causa) se traduce en que no se debe aplicar doble sanción o a un mismo hecho. En este caso, nos referimos a la palabra "hecho" cuando existe identidad en la persona, en el objeto y la causa o fundamento de persecución. En nuestra legislación, este principio se encuentra regulado en el artículo 23 de la CPEUM, que establece que ningún juicio criminal deberá tener más de tres instancias. Nadie puede ser juzgado dos veces por el mismo delito, ya sea que en el juicio se le absuelva o se le condene. Queda prohibida la práctica de absolver de la instancia.[1997]

Como se observa, este principio constitucional —que deriva del principio de legalidad— busca salvaguardar y proteger las garantías individuales de seguridad y certeza jurídica. Durante muchos años se ha criticado la incorporación de la reincidencia dentro de la normatividad penal mexicana por ser contraria al principio de *non bis idem*. Sin embargo, la reincidencia no busca generar la duplicidad de la pena en mismo hecho, por el contrario, busca evitar la comisión de un segundo delito o una infracción, agravándola. En pocas palabras, la aplicación de la reincidencia ocurre con la comisión de una segunda falta, en donde no solamente se deberá valorar el tipo de infracción cometida, sino además deberá considerarse al momento de determinar la gravedad, la existencia de una falta previa dentro del mismo ámbito. En estricto sentido, no se trata de una doble sanción por un mismo hecho, sino de una doble valoración.

Sirve de apoyo a lo anterior la siguiente tesis aislada del Poder Judicial de la Federación que a continuación se transcribe:

> REINCIDENCIA. EL ARTÍCULO 33 DEL CÓDIGO PENAL PARA EL ESTADO DE VERACRUZ QUE ESTABLECE CUÁNDO SE ACTUALIZA, NO VIOLA EL DERECHO FUNDAMENTAL *NON BIS IN IDEM.* El citado precepto, al establecer que hay reincidencia siempre que el condenado por sentencia ejecutoria, dictada por cualquier tribunal de la República Mexicana o del extranjero, cometa otro delito en la entidad, no contraviene el derecho fundamental *non bis in idem* contenido en el numeral 23 de la Constitución Política de los Estados Unidos Mexicanos, conforme al cual nadie puede ser juzgado dos veces por los mismos hechos delictivos, toda vez que, con tal definición, no se ejerce un doble enjuiciamiento al individualizar la pena en un asunto posterior seguido contra un justiciable que cometió un delito con antelación, ya que al actualizarse la reincidencia no está sujetándose nuevamente al procesado a una causa por los mismos hechos delictivos por los que anteriormente había sido sentenciado.[1998]

1996 Cabrera, R. (2011). "La reincidencia vulnera el *non bis in ídem*", en *Revista Ciencia Amazónica (Iquitos)*. Facultad de Derecho y Ciencias Políticas, Universidad Científica del Perú. No. 1. Vol. 1. Perú, pp. 81-92.

1997 Artículo 23. Ningún juicio criminal deberá tener más de tres instancias. Nadie puede ser juzgado dos veces por el mismo delito, ya sea que en el juicio se le absuelva o se le condene. Queda prohibida la práctica de absolver de la instancia.

1998 Tesis 1a. CXLIII/2013 (10a.). *Semanario Judicial de la Federación y su Gaceta.* Décima época. Libro XX. Tomo 1, mayo de 2013, p. 573.

De igual manera, reafirma lo anterior la siguiente tesis aislada:

> AGRAVANTES. NO SON VIOLATORIAS DEL PRINCIPIO *NON BIS IN IDEM.* El principio de *non bis in idem* o de prohibición de doble punición se actualiza únicamente cuando el Estado juzga dos veces a una persona con motivo de los mismos hechos delictivos, pero no en aquellos casos en que el legislador establece una penalidad agravada diversa a la del tipo básico. El hecho de ser juzgado por un delito y además que se le aplique una agravante no actualiza el supuesto del principio *non bis in idem*.[1999]

Finalmente, resta señalar que en aquellos casos en que no exista identidad en la persona, objeto y causa o fundamento de la eventual sanción, no se actualiza violación al principio referido, en tanto que su origen proviene de diversas hipótesis que puedan ser sancionables al actualizarse diversas conductas infractoras.

Relación jurídica

Luis Manuel C. Meján

El concepto "relación" implica la presencia de una pluralidad de elementos, la Real Academia de la Lengua Española (RAE) lo define como: "conexión, correspondencia de algo con otra cosa. Conexión, correspondencia, trato, comunicación de alguien con otra persona".[2000]

No basta que haya una pluralidad de elementos, sino que entre ellos debe existir un vínculo, un nexo, algo que los une y conecta al uno con el otro. En la vida ordinaria, todos los seres humanos desarrollan relaciones, es decir, vínculos con otras personas (amistad, cariño, contrato, empleo, etc.), con las cosas (atesoradas, poseídas, etc.) o con entidades más abstractas (la sociedad, los necesitados, el público).

La diferencia específica que se añade al concepto "vínculo" es que la conexión entre los elementos de la relación debe ser jurídica, es decir, una regida por el derecho. Savigny explicaba que en todas las relaciones humanas hay unas regidas y determinadas por el derecho, como es el caso de la propiedad, otras en el que el derecho las regula solo en parte, como el matrimonio y otras en donde el derecho está fuera de la relación, es el caso de la amistad.[2001]

La relación jurídica puede nacer de la ley, de la voluntad de las personas, de actos de autoridad o de disposiciones judiciales, y se integra con un elemento subjetivo: los sujetos, un elemento material: un objeto, y un elemento formal: una fuente de derecho.[2002]

El vínculo fuerza a la persona a dar cumplimiento a algo, hay siempre un objeto en la relación jurídica que constriñe a los sujetos a desplegar una determinada conducta "en vista de cuya inejecución el poder público se apoderará de la persona o del patrimonio del deudor para obligarlo a ejecutar la obligación" (Kohler).[2003]

1999 Tesis 1a. CI/2011. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XXXIII, junio de 2011, p.169.

2000 RAE. (2017). Relación en *Diccionario de la lengua española.* Disponible en: http://dle.rae.es/?id=VoYtQP9

2001 Savigny explicado por De Cossío, A. (1975-1977). *Instituciones de derecho civil (parte general, derecho de las obligaciones).* Primera edición. Editorial Alianza. Madrid, p. 75-77.

2002 Una explicación dada por la teoría pura del derecho de Kelsen, dice que se trata de una "unión normativa de los elementos que integran el contenido del precepto: la unión de una consecuencia (sanción normativa) a un determinado supuesto o condición (el acto) y la imputación de cierta conducta, a una determinada persona. Estos elementos que integran la norma no están, pues, unidos o ligados por relaciones de causalidad, sino por el deber ser establecido en el precepto jurídico". Ramírez, J. (1988). *Diccionario Jurídico.* Décima edición. Editorial Claridad. Argentina, p. 266.

2003 Borja, M. (2012). *Teoría general de las obligaciones*. 21 edición. Editorial Porrúa. México, p. 72.

La típica relación jurídica es la que se establece entre dos personas, de las cuales, una tiene el deber de cumplir con una determinada prestación en favor de la otra a quien le asiste el derecho de exigir su cumplimiento. Esta es la típica relación estudiada por la teoría general de las obligaciones. Luis Díez-Picaso y Robles Farías la llaman "relación jurídica obligatoria" y comúnmente es designada simplemente por el término "obligaciones".

Sin duda, esa es una relación jurídica pues establece un vínculo entre sus partes respecto de un hecho, cosa o prestación que es sancionada por las normas jurídicas. Esta es la relación que nace de un contrato, de una declaración unilateral de la voluntad, de los cuasicontratos, de la responsabilidad civil, contractual o extracontractual, de los hechos de las cosas o de terceros. Sin embargo, no es la única vinculación posible.

Puede existir una vinculación regida por el derecho entre las personas y las cosas, es el caso de la propiedad en el que una persona ejerce un poder de dominio sobre una cosa y a todos los demás se les impone un deber de respeto hacia ese dominio. En el caso de la copropiedad se establecen, además del vínculo hacia la cosa, relaciones entre las personas que detentan la copropiedad. Los derechos reales importan esta clase de relación jurídica.

Otro caso de relación jurídica es el que se establece entre el Estado y el ciudadano cuando se produce un acto administrativo que impone al sujeto la obligación de cumplir una obligación. Similar situación es la que se produce cuando un juez o tribunal impone una carga a un justiciable.

Una peculiar forma de relación jurídica es la derivada de las leyes laborales en las que, a manera de las relaciones jurídicas obligatorias, pero con una protección peculiar, se regulan los vínculos que nacen del vínculo laboral.

Hay leyes que imponen obligaciones y establecen un vínculo entre una persona y un grupo abstracto de personas: la sociedad. Tal es el caso de las relaciones que nacen derivadas de las leyes que protegen la propiedad intelectual, las leyes ecológicas, las de competencia económica, de procesos electorales y partidos políticos, las de explotación y uso de recursos naturales, etcétera.

En la normatividad que rige el trato a los datos personales se establecen vínculos en los que participan el titular de los mismos y el responsable de su captación y trato, sea entidad privada o entidad pública. Curiosamente, cuando los datos personales son requeridos para el ejercicio de un derecho o el cumplimiento de obligaciones derivados de una relación jurídica entre el titular y el responsable, no será requisito el exigir el consentimiento del titular.[2004]

Remisión de datos personales

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La remisión de datos personales se encuentra definida en la normatividad de protección de datos personales aplicable a los sectores público y privado en casi idénticos términos. El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) señalan:

2004 Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 22, fracción V. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículos 10, fracción IV y 37 fracción VII y artículo 6 de su Reglamento.

Definición de remisión	
Artículo 3, fracción IX, del RLFPDPPP	Artículo 3, fracción XXVII, de la LGPDPPSO
La comunicación de datos personales entre el responsable y el encargado dentro o fuera del territorio mexicano.	Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado dentro o fuera del territorio mexicano.

Del contenido de las definiciones legales anteriores se desprende que la remisión de datos personales implica lo siguiente:

a) La comunicación o divulgación de datos personales entre un responsable y un encargado.[2005] En virtud de la remisión el responsable comparte con el encargado determinados datos personales que serán sujetos a tratamiento según las instrucciones del responsable. Solo se considera remisión a esta comunicación.

b) La remisión puede realizarse dentro o fuera del territorio nacional. Es decir, pueden existir remisiones nacionales e internacionales de datos personales.

La remisión, en contraposición con otras comunicaciones de datos personales —como la transferencia— tal y como lo establecen el RLFPDPPP[2006] y la LGPDPPSO,[2007] no se encuentra sujetas al consentimiento del titular de los datos personales y tampoco requiere ser informadas en el aviso de privacidad.

Es decir, el tratamiento de las remisiones de datos personales, no está sujeto al cumplimiento de los principios de consentimiento e información, pero sí debe cumplir las formalidades relativas a la delimitación de su alcance y contenido a través de un instrumento jurídico específico (artículo 50 del RLFPDPPP y artículo 59 de la LGPDPPSO).

La remisión es, por tanto, el medio por el que el responsable y encargado se comunican los datos. El encargado, como se detalla en la definición pertinente a la que nos remitimos, sigue las instrucciones del responsable en el tratamiento objeto de la remisión, actuando por cuenta del mismo. Sin embargo, si el encargado incumple dichas instrucciones y destina o utiliza los datos personales con una finalidad distinta a la autorizada por el responsable, o efectúa una transferencia, incumpliendo las instrucciones del responsable, será considerado como un responsable del tratamiento con las obligaciones que resultan aplicable a este último (según el artículo 53 del RLFPDPPP y artículo 60 de la LGPDPPSO y, en consecuencia, deberá responder de forma íntegra e independiente sobre el cumplimiento de las obligaciones y responsabilidades establecidas en la normatividad de datos personales.

Además, debe precisarse que dicha responsabilidad no será asumible por el encargado cuando éste haya remitido datos personales a otro encargado designado de forma previa y expresa por el responsable (subcontratación)[2008] y al que se le hubiere encargado la prestación de un servicio o bien los haya transferido a otro responsable en cumplimiento de lo dispuesto en la normatividad de datos personales (artículo 53 del RLFPDPPP).

Finalmente, debe tenerse en cuenta que, en términos de la LGPDPPSO, cuando las remisiones de datos personales sean de carácter internacional será necesario que el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la dicha norma y las disposiciones que resulten aplicables.[2009]

2005 Para un estudio detallado de la figura del encargado del tratamiento, recomendamos al lector consultar la definición de "encargado del tratamiento" de este diccionario.

2006 Artículo 53 del RLFPDPPP.

2007 Artículo 71 de la LGPDPPSO.

2008 Para ulterior detalle, se recomienda consultar la definición de "subcontratación" contenida en la presente obra.

2009 Artículo 68 de la LGPDPPSO.

Requerimiento de información

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El requerimiento de información es un acto procesal por virtud del cual el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), mediante sus unidades administrativas competentes, requiere[2010] al titular de los datos, al responsable y/o a los organismos garantes que proporcionen determinada información y/o documentación que puede estar en su poder, para obtener información, datos y evidencia o medios de convicción suficientes para que le permitan dilucidar los hechos denunciados por el titular o aquellos que pudieran representar un incumplimiento a la normatividad de protección de datos personales aplicable.

1. Características

El requerimiento de información tiene diversas particularidades, entre las cuales se pueden identificar las siguientes:

a) Es un acto de molestia: en el ámbito privado, se trata de un acto de molestia realizado por el INAI que restringe —de manera provisional o preventiva— un derecho con el objeto de proteger determinados bienes jurídicos[2011] como es el derecho de protección de datos personales de los titulares. Como consecuencia de lo anterior, el requerimiento de información debe revestir los siguientes elementos:[2012]

   1) Debe expresarse por escrito y contener la firma original o autógrafa del respectivo funcionario. Esta exigencia tiene como propósito evidente que pueda haber certeza sobre la existencia del acto de molestia y para que el afectado pueda conocer con precisión de cuál autoridad proviene, así como su contenido y sus consecuencias.

   2) Debe provenir de autoridad competente. Significa que la autoridad emisora esté habilitada constitucional y legalmente, y tenga dentro de sus atribuciones la facultad de emitirlo.

   3) Se debe fundar y motivar la causa legal del procedimiento. La exigencia de fundamentación es entendida como el deber que tiene la autoridad de expresar, en el mandamiento escrito, los preceptos legales que regulen el hecho y las consecuencias jurídicas que pretenda imponer el acto de autoridad. Este presupuesto tiene su origen en el principio de legalidad que, en su aspecto imperativo, consiste en que las autoridades solo puedan hacer lo que la ley les permite, mientras que la exigencia de motivación se traduce en la expresión de las razones por las cuales la autoridad considera que los hechos en que basa su proceder se encuentran probados y son precisamente los previstos en la disposición legal que afirma aplicar. Los presupuestos de fundamentación y motivación deben

2010 Desde su acepción gramatical el requerimiento es, según el *Diccionario de la Lengua Española*, "un acto judicial por el que se intima que se haga o se deje de ejecutar algo". *Vid,* RAE. (2017).. Requerimiento en *Diccionario de la Real Academia Española.* Disponible en: http://dle.rae.es/?id=W6dALmQ Fecha de consulta: 5 de septiembre de 2018.

2011 Tesis: 2a./J. 151/2016 (10a.). Jurisprudencia. Décima época. *Gaceta del Semanario Judicial de la Federación*. Libro 35, octubre de 2016. Tomo I, p. 720.

2012 *Vid,* Tesis: I.3o.C.52 K. Aislada. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XVII, abril de 2003, p. 1050.

coexistir y se suponen mutuamente, pues no es posible citar disposiciones legales sin relacionarlas con los hechos de que se trate, ni exponer razones sobre hechos que carezcan de relevancia para dichas disposiciones. Esta correlación entre los fundamentos jurídicos y los motivos de hecho supone necesariamente un razonamiento de la autoridad para demostrar la aplicabilidad de los preceptos legales invocados a los hechos de que se trate, lo que en realidad implica la fundamentación y motivación de la causa legal del procedimiento.

b) Debe tener un objeto determinado. El requerimiento de información debe circunscribirse al objeto de la actuación procesal que lo motiva, es decir, debe referirse de forma concreta a los elementos que el INAI debe investigar y comprobar con motivo del ejercicio de sus atribuciones legales con motivo de la solicitud formulada por el titular de los datos.

c) Debe emitirse dentro de los plazos previstos en la normatividad. El requerimiento de información no puede emitirse en cualquier tiempo. Su emisión debe realizarse siempre dentro de los plazos legalmente establecidos para tal efecto en la normatividad de datos personales.

d) Debe ser debidamente notificado. El requerimiento de información debe ser notificado al titular, responsable y/o órgano garante correspondiente de forma personal, cuando así se hubiere solicitado, o bien mediante los medios electrónicos que las partes hubieren designado o acordado para tal efecto.

En relación con las notificaciones en los procedimientos regulados en el sector privado, el artículo 8 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de los Procedimientos) señala que las notificaciones, citatorios, emplazamientos, requerimientos, solicitud de informes o documentos y resoluciones definitivas podrán realizarse:

1) Personalmente con quien deba entenderse la diligencia, en el domicilio del interesado.
2) Mediante oficio entregado por mensajero o, correo certificado con acuse de recibo.
3) A través de medios de comunicación electrónica o cualquier otro medio, cuando así lo haya aceptado expresamente el interesado y siempre que pueda comprobarse fehacientemente la recepción de estos.
4) Por edictos, cuando se desconozca el domicilio del interesado, o en el caso de que la persona a quien deba notificarse haya desaparecido o no tenga domicilio fijo.
5) Por estrados, fijándose durante 15 días hábiles el documento que se pretenda notificar, en un sitio abierto al público ubicado en las oficinas del Instituto.

En lo concerniente a las notificaciones en los procedimientos de revisión e inconformidad regulados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), las notificaciones que emita el INAI podrán efectuarse:

a. Personalmente en los siguientes casos:
    i. se trate de la primera notificación;
    ii. se trate del requerimiento de un acto a la parte que deba cumplirlo;
    iii. se trate de la solicitud de informes o documentos;
    iv. se trate de la resolución que ponga fin al procedimiento de que se trate y
    v. en los demás casos que disponga la ley.

b. Por correo certificado con acuse de recibo o medios digitales o sistemas autorizados por el Instituto o los organismos garantes, según corresponda, y publicados mediante acuerdo general en el *Diario Oficial de la Federación* o diarios o gacetas oficiales de las entidades federativas, cuando se trate de requerimientos, emplazamientos, solicitudes de informes o documentos y resoluciones que puedan ser impugnadas.

c. Por correo postal ordinario o por correo electrónico ordinario cuando se trate de actos distintos de los señalados en las fracciones anteriores.

d. Por estrados, cuando la persona a quien deba notificarse no sea localizable en su domicilio, se ignore éste o el de su representante.

2. Requerimiento de información en el sector privado

El requerimiento de información en el sector privado se da dentro de los Procedimientos de Investigación (PI) y Verificación (PV) con base en lo siguiente:

a) PI: los Lineamientos de los Procedimientos precisan, en su artículo 55, que cuando el denunciante haya cumplido con las formalidades establecidas en el artículo 51 de los referidos Lineamientos,[2013] la Dirección General de Investigación y Verificación (DGIV) expedirá un requerimiento de información al denunciado (responsable) o a cualquier tercero, solicitando que se proporcione la información que se estime oportuna, que se manifieste respecto de los hechos vertidos en la denuncia, así como que aporte la información y documentación que acredite su dicho, dentro de un plazo máximo de cinco días hábiles, contados a partir de que surta efectos la notificación de dicho requerimiento.

b) PV: los Lineamientos de los Procedimientos, en su artículo 62,[2014] indican que el PV se podrá llevar a cabo mediante requerimientos de información a través de los cuales la DGIV emitirá los oficios correspondientes y el responsable dará respuesta a los mismos dentro del plazo máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del requerimiento respectivo.

3. Requerimiento de información en el sector publico

En la normatividad del sector público, la figura del requerimiento de información se encuentra prevista con claridad en el artículo 135 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales) en relación con el recurso de revisión, al señalar que el Instituto podrá solicitar al titular, responsable,

2013 Artículo 55. Cuando el denunciante haya cumplido con las formalidades establecidas en el artículo 51 de los presentes Lineamientos, la Dirección General de Investigación y Verificación expedirá un requerimiento de información al denunciado o a cualquier tercero, solicitando que se proporcione la información que se estime oportuna, que se manifieste respecto de los hechos vertidos en la denuncia, así como que aporte la información y documentación que acredite su dicho, dentro de un plazo máximo de cinco días hábiles, contados a partir de que surta efectos la notificación de dicho requerimiento.

2014 Artículo 62. El desarrollo del Procedimiento de Verificación se podrá llevar a cabo de la siguiente manera:

I. Mediante requerimientos de información. La Dirección General de Investigación y Verificación emitirá los oficios correspondientes, y al dar respuesta, dentro del plazo máximo de cinco días hábiles, contados a partir de que surta efectos la notificación del requerimiento respectivo, el responsable podrá presentar las pruebas que considere pertinentes sobre el tratamiento que brinda a los datos personales, así como manifestar lo que a su derecho convenga respecto de la denuncia y el procedimiento de verificación instaurado en su contra, y

II. A través de visitas de verificación. Se realizarán en el establecimiento del responsable, o bien en donde se encuentren las bases de datos objeto de la verificación, y tendrán una duración máxima de diez días hábiles cada una, para que el Instituto se allegue de diversos elementos de convicción sobre el tratamiento que el responsable da a los datos personales tanto de titulares como del denunciante.

tercero interesado y/o organismos garantes cualquier información y demás documentos que estime pertinentes, guardando la confidencialidad respectiva sobre la información a la que tenga acceso.

Por otra parte, en relación con el PV regulado en la LGPDPPSO, el artículo 195 de los Lineamientos Generales señala que, cumplidos los requisitos que debe contener la denuncia, o una vez iniciada de oficio la investigación previa, el Instituto, a través de la unidad administrativa competente conforme a su estatuto orgánico vigente podrá:

a) expedir requerimientos de información dirigidos al responsable, al encargado o a cualquier tercero, solicitando que se proporcione la información y documentación que se estime oportuna;
b) que se manifieste respecto de los hechos vertidos en la denuncia y
c) que aporte la información y documentación que acredite su dicho, dentro de un plazo máximo de cinco días contados a partir de que surta efectos la notificación de dicho requerimiento.

En definitiva, el requerimiento de información es un acto jurídico emitido por las unidades administrativas competentes del INAI para abastecerse de los elementos necesarios para la resolución de un determinado procedimiento en materia de protección de datos personales.

Resolución de Madrid de Estándares Internacionales de Privacidad

Jacobo Esquenazi Franco

1. Introducción

En 2009, como parte de los trabajos en las sesiones cerradas de la trigésimo primera Conferencia de Autoridades de Protección de Datos Personales y Privacidad, se emitió la Resolución de Madrid de Estándares Internacionales de Privacidad,[2015] también conocida como la Resolución de Madrid de Privacidad y Protección de Datos (Resolución de Madrid).[2016]

La resolución buscó establecer un conjunto de principios, derechos y obligaciones que cualquier sistema jurídico de protección de la privacidad debería esforzarse por alcanzar. La propuesta se pensó como la base para el desarrollo de un instrumento vinculante a escala internacional, que contribuya a una mayor protección de los derechos y libertades individuales a nivel global.

2. Estructura y contenido

La Resolución de Madrid tiene por objeto definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal y facilitar su flujo a escala internacional, necesarios en un mundo globalizado.[2017]

2015 Consultada en *International Conference of Data Protection and Privacy Commissioners* el 14 de noviembre del 2018. Disponible en: https://icdppc.org/wp-content/uploads/2015/02/The-Madrid-Resolution.pdf

2016 No confundir la Declaración de Privacidad de Madrid, que es un documento firmado por organizaciones de la sociedad civil en los márgenes de la 31ª Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad con el fin de promover la protección de la privacidad y los datos personales. Entre otras cosas la Declaración urge a los países a contar con legislación para la protección de datos y a firmar el Convenio 108 del Consejo de Europa.

2017 Artículo 1 de la Resolución de Madrid de Privacidad y Protección de Datos.

La citada resolución pretende aplicarse a todo tratamiento de datos de carácter personal, total o parcialmente automatizado o, en caso contrario, realizado de forma estructurada, que sea llevado a cabo por el sector público o privado.[2018]

En la parte II, la Resolución de Madrid establece principios y derechos sobre el tratamiento de datos para garantizar la efectiva protección de la privacidad a nivel internacional, así como para hacer más fácil el flujo internacional de datos personales, reconociendo que son imprescindibles en un mundo globalizado. Entre los principios básicos se incluyen:

a) Lealtad y legalidad (artículos 6.1 y 6.2)
b) Finalidad (artículos 7.1 y 7.2)
c) Proporcionalidad (artículos 8.1 y 8.2)
d) Calidad (artículos 9.1 y 9.2)
e) Transparencia (artículos 10.1, 10.2, 10.3, 10.4, 10.5 y 10.6)
f) Responsabilidad (artículo 11)

En la parte III, la Resolución de Madrid, en su artículo 12, establece las bases jurídicas para la legitimación del tratamiento y señala que, como regla general, los datos de carácter personal solo podrán ser tratados cuando concurra alguno de los siguientes supuestos:

a) previa obtención del consentimiento libre, inequívoco e informado del interesado;
b) cuando un interés legítimo de la persona responsable justifique el tratamiento, siempre y cuando no prevalezcan los intereses legítimos, derechos o libertades de los interesados;
c) cuando el tratamiento sea preciso para el mantenimiento o cumplimiento de una relación jurídica entre la persona responsable y el interesado;
d) cuando el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable, o se lleve a cabo por una administración pública que lo precise para el legítimo ejercicio de sus competencias y
e) cuando concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del interesado o de otra persona.

El documento también define a los datos sensibles como aquellos que afectan a "la esfera más íntima de la persona o cuya utilización indebida pueda dar origen a una discriminación ilegal o arbitraria, o conllevar un riesgo grave para la misma". En la misma sección se habla también de la utilización de prestadores de servicio para el tratamiento de datos. Establece que en en su uso se debe asegurar que los mismos establezcan las medidas de protección y la necesidad de establecer un documento jurídico que obligue a los prestadores de servicios a cumplir con estos principios.[2019]La Resolución plantea la necesidad de la existencia de autoridades de supervisión, que velen por un conjunto de derechos, como el de acceso, rectificación, cancelación y oposición y la forma de ejercerlos. También incluye deberes como el de seguridad de los datos personales, plantea los requisitos que deben cumplirse para la legítima recolección, conservación, utilización, revelación o supresión de datos personales, como, por ejemplo, la previa obtención del consentimiento libre, inequívoco e informado por parte de la persona que facilita los datos.

2018 Artículo 3.1 de la Resolución de Madrid de Privacidad y Protección de Datos.

2019 Artículo 13 de la Resolución de Madrid de Privacidad y Protección de Datos.

En la parte IV, de los artículos 16 al 19, la Resolución de Madrid reconoce y regula como derechos del interesado los derechos de acceso, rectificación, cancelación y oposición, mientras que en la parte V reconoce los deberes de seguridad y confidencialidad y obliga a todo sujeto que realice el tratamiento de los datos a prever medidas de seguridad físicas, técnicas y administrativas para garantizar la seguridad y confidencialidad de los datos personales.[2020]

3. Flujo transfronterizo de datos

La Resolución, en su artículo 15, trata el tema de las transferencias internacionales de datos y plantea que, como regla general, podrán realizarse transferencias internacionales de datos personales cuando el Estado al que se transfieran los datos ofrezca, al menos, el nivel de protección previsto en el documento. Sin embargo, también reconoce que en los casos en los que se pretenda transferir los datos no cuente con el nivel de protección previsto en la resolución, quién pretenda transferir los datos, garantice que el destinatario ofrecerá el nivel de protección requerido, utilizando, por ejemplo, las cláusulas contractuales apropiadas

4. Cooperación entre autoridades de protección

El documento plantea en su sexta y última parte la necesidad de cooperación entre las autoridades de protección de datos a nivel local e internacional y establece los mecanismos para lograrlo.[2021]

5. Apoyo Empresarial

Un grupo de 10 grandes empresas (Oracle, Walt Disney, Accenture, Microsoft, Google, Intel, Procter & Gamble, General Electric, IBM y Hewlett-Packard) firmaron una declaración en la que expresan su satisfacción por la iniciativa de la trigésimo primera Conferencia Internacional por explorar marcos para una mejor coordinación global de los distintos regímenes de privacidad.[2022]

Resolución del Pleno del INAI

Ángel Trinidad Zaldívar,
Marina San Martín Rebolloso

Una resolución es un acto de autoridad que define o da certeza a una situación legal, la cual goza de la presunción de legitimidad, es decir, parte de la premisa de su cumplimiento a la garantía de legalidad.[2023]

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) es un organismo autónomo que garantiza, en el ámbito federal, el ejercicio de los derechos de acceso a la información y la protección de datos personales, por tanto, conoce, sustancia y resuelve:

2020 Artículos 20 y 21 de la Resolución de Madrid de Privacidad y Protección de Datos.

2021 Artículos 22 al 25de la Resolución de Madrid de Privacidad y Protección de Datos.

2022 Citado por Abu Bakar Munir en: Bakar, A. (2009, diciembre 29). *Madrid Resolution: a Step Towards a Privacy Treaty?* Disponible en: http://profabm.blogspot.com/2009/12/another-privacy-standard.html Fecha de consulta: 14 de noviembre 2018.

2023 Concepto elaborado con base en la definición de "resolución administrativa". Véase, Instituto de Investigaciones Jurídicas. (1997). *Diccionario Jurídico Mexicano.* Décima edición. Tomo P-Z. Porrúa-UNAM. México, p. 2820.

a) los recursos de revisión de acceso a la información y de protección de datos personales del sector público, interpuestos en contra de las resoluciones de los sujetos obligados en el ámbito federal;
b) los recursos de inconformidad de acceso a la información y de protección de datos personales del sector público promovidos en contra de las resoluciones emitidas por los organismos garantes de las entidades federativas que determinen, entre otros supuestos, la clasificación, la inexistencia o la negativa de la información;
c) los recursos de revisión y de acceso a la información o de protección de datos personales del sector público que, por su interés o trascendencia atraiga el INAI, de oficio o a petición de los organismos garantes de las entidades federativas;
d) las denuncias por incumplimiento a las obligaciones de transparencia;
e) los procedimientos de verificación en materia de protección de datos personales del sector público y
f) los procedimientos de protección de derechos en materia de datos personales en posesión de particulares y de verificación del sector privado, así como imponer las sanciones que correspondan.[2024]

El Pleno del Instituto se integra por siete comisionados, incluyendo a su presidente, que representa la instancia superior de dirección para vigilar, de forma colegiada, el cumplimiento en materia de transparencia, acceso a la información y protección de datos personales, cuidando que sus actividades garanticen los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.[2025]

Las sesiones del Pleno son válidas siempre que se cuente con la asistencia de cinco comisionados, incluyendo al comisionado presidente. En caso de existir empate, el presidente tiene voto de calidad; además, sus resoluciones son obligatorias para todos ellos, aunque estuviesen ausentes o sean disidentes al momento de tomarlas.[2026]

Una resolución del Pleno del INAI es el acto de autoridad que documenta la decisión que adopten los comisionados, ya sea por unanimidad o por mayoría, para dar solución a una controversia relacionada con el ejercicio del derecho de acceso a la información, con el derecho a la protección de los datos personales, o que involucren ambos, así como para definir una situación específica relativa a los diversos procedimientos de inconformidad previstos en las leyes generales, en la Ley Federal de Transparencia y Acceso a la Información Pública y en la legislación de protección de datos personales, tanto en posesión de particulares como gubernamentales.

Siendo una de las funciones del Pleno del Instituto adoptar determinaciones para definir conflictos sobre acceso a la información y protección de datos personales, dicha actividad debe regirse por diversos principios,[2027] entre los que destacan:

2024 Artículos 21, fracciones II, III y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP). *Diario Oficial de la Federación*, 9 de mayo de 2016; 89, fracciones III, IV, V y VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). *Diario Oficial de la Federación*, 26 de enero de 2017; y 39, fracción VI de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), *Diario Oficial de la Federación,* 5 de julio de 2010.

2025 Artículos 4, fracción VIII, y 33 de la LFTAIP.

2026 Artículos 33 de la LFTAIP.

2027 De los nueve principios de los organismos rectores, no se cita el de "máxima publicidad" porque aplica específicamente al derecho de acceso a la información en cuanto a que, por regla general, prevalece la apertura de alguna información clasificando por excepción, regla que no ocurre en protección de datos personales. Véase el artículo 8, fracciones I a la V y de la VII a la IX, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), *Diario Oficial de la Federación*, 4 de mayo de 2015.

1) Certeza: es el principio que concede seguridad y certidumbre jurídica a las personas porque permite asegurar que el actuar de las autoridades garantes es apegado a derecho y que los procedimientos son verificables, fidedignos y confiables.
2) Eficacia: consiste en la tutela efectiva de los derechos de acceso a la información y protección de datos personales.
3) Imparcialidad: es la cualidad que deben tener las instituciones garantes respecto de sus acciones para ser ajenos a los intereses de las partes en conflicto y de resolver sin favoritismo.
4) Independencia: se refiere a la cualidad que deben tener los organismos garantes para actuar sin someterse a los interéses de alguna autoridad o persona.
5) Objetividad: consiste en el deber de los organismos garantes de ajustar su actuación a los presupuestos de ley que deben ser aplicados al analizar el caso en concreto y resolver todos los hechos, prescindiendo de consideraciones y criterios personales.
6) Profesionalismo: se orienta a que los servidores públicos de los órganos garantes del derecho ejerzan sus funciones con base en conocimientos técnicos, teóricos y metodológicos que aseguren un desempeño eficiente y eficaz en el ejercicio de la función pública que tienen encomendada.
7) Transparencia: indica el deber del INAI y de los organismos garantes de dar publicidad a las deliberaciones y actos relacionados con sus atribuciones, así como permitir el acceso a la información que generen.
8) Legalidad:[2028] implica que el INAI funde y motive sus resoluciones y actos en las normas aplicables, es decir, justificando o dando razones por las que éstas deben aplicarse al supuesto en cuestión.

Ahora bien, el INAI es la autoridad que emite resoluciones ante impugnaciones presentadas relacionadas con el ejercicio del derecho a la protección de datos personales, en el marco de dos normativas:

a) La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que tiene por objeto salvaguardar los datos personales que se encuentren en posesión de particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.[2029]
b) La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) que es reglamentaria de los artículos 6, base "A" y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, que en materia de protección de datos personales en posesión de sujetos obligados incluyen a cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos de varios ámbitos de gobierno; con la precisión que su aplicación y observancia es directa para los sujetos obligados del orden federal.[2030]

2028 El principio de legalidad se prevé en el artículo 16 constitucional que señala que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento". Véase Constitución Política de los Estados Unidos Mexicanos, *Diario Oficial de la Federación*, 5 de febrero de 1917 (última reforma 15-09-2017).

2029 Artículo 1 de la LFPDPPP.

2030 Artículo 1 de la LGPDPPSO.

En lo que respecta a los datos personales de particulares, de conformidad con la LFPDPPP, al INAI le corresponde resolver los siguientes procedimientos:

1. Procedimiento de protección de derechos.
2. Procedimiento de verificación.
3. Procedimiento de imposición de sanciones.

El procedimiento de protección de derechos de datos personales se refiere a garantizar su acceso, rectificación, cancelación y oposición (derechos ARCO) y es detonado por el titular de los datos o su representante legal, cuando considere vulnerado su derecho.[2031] Las resoluciones pueden i) sobreseer[2032] o desechar[2033] la solicitud de protección de datos por improcedente o ii) confirmar, revocar o modificar la respuesta del responsable.[2034]

Si la resolución de protección de derechos favorece al titular de los datos, el responsable deberá hacer efectivo el ejercicio del derecho motivo de la queja en un plazo de 10 días siguientes a la notificación o en un tiempo mayor que se justifique en la propia resolución, debiendo dar cuenta por escrito del cumplimiento al Instituto dentro de los siguientes 10 días.[2035]

El procedimiento de verificación podrá ser a petición de parte, o de oficio cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos, o a petición de parte.[2036]

El procedimiento de imposición de sanciones ocurre cuando hay incumplimiento a los principios o disposiciones de la LFPDPPP derivado del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto.[2037]

Las resoluciones dictadas con base en la LFPDPPP son impugnables mediante el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.[2038]

Ahora bien, en materia de protección de datos personales en posesión del sector público, de acuerdo con la LGPDPPSO, el INAI decide sobre los procedimientos siguientes:

a) El recurso de revisión para el ejercicio de los derechos ARCO.
b) El recurso de inconformidad en segunda instancia contra resoluciones de los institutos de transparencia de las entidades federativas.

2031 Artículo 45 de la LFPDPPP.

2032 La solicitud de protección de datos será sobreseída cuando: i) el titular fallezca; ii) se desista de manera expresa; iii) una vez admitida, sobrevenga una causal de improcedencia y iv) quede sin materia. Véase el artículo 53 de la LFPDPPP.

2033 La solicitud de protección de datos será desechada por improcedente cuando: i) el Instituto sea incompetente; ii) el INAI haya conocido anteriormente de la solicitud contra el mismo acto y resuelto en definitiva respecto del mismo recurrente; iii) se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo; iv) se trate de una solicitud de protección de datos ofensiva o irracional o v) sea extemporánea. Véase el artículo 52 LFPDPPP.

2034 El plazo máximo para dictar la resolución es de 50 días contados a partir de la fecha de presentación de la solicitud de protección de datos y se puede extender por causa justificada por una vez por un período igual. Véase artículos 47 y 51 de la LFPDPPP.

2035 Artículo 48 de la LFPDPPP.

2036 Durará máximo 180 días, pudiendo prolongarse una vez y por un periodo igual, concluyendo con una resolución que establecerá las medidas a adoptar por el responsable en el plazo que la misma establezca. Véase artículos 59 de la LFPDPPP y 132 y 137 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), *Diario Oficial de la Federación*, 21 de diciembre de 2011

2037 El procedimiento de imposición de sanciones inicia con la notificación del INAI al presunto infractor otorgándole 15 días para rendir pruebas y manifestar lo que a su derecho convenga; desahogadas las pruebas, el presunto infractor tiene cinco días para rendir sus alegatos. El órgano garante de transparencia nacional resolverá en 50 días pudiendo ampliarse ese tiempo una vez por el mismo plazo. Véase artículos 61 y 62 de la LFPDPPP.

2038 Artículo 56 de la LFPDPPP y artículos 126, 138 y 144 del RLFPDPPP.

c) La facultad de atracción de los recursos de revisión de los órganos garantes de transparencia estatales.
d) El procedimiento de verificación a los sujetos obligados responsables del cumplimiento de la LGPDPPSO.

El recurso de revisión será interpuesto por el titular o por su representante para la protección de los derechos ARCO en un plazo de no más de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta y procederá cuando:

a) se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
b) se declare su inexistencia;
c) se declare la incompetencia del responsable;
d) se entreguen datos personales incompletos;
e) se entreguen datos personales que no correspondan con lo solicitado;
f) se niegue el acceso, rectificación, cancelación u oposición de dichos datos;
g) no se dé respuesta a una solicitud para el ejercicio de los derechos ARCO;
h) se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;
i) exista inconformidad con los costos de reproducción, envío o tiempos de entrega;
j) se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;
k) no se dé trámite a una solicitud de derechos ARCO y
l) en los demás casos que dispongan las leyes.[2039]

El INAI y los organismos garantes resolverán el recurso de revisión en un plazo no mayor a 40 días, el cual podrá ampliarse hasta por 20 días por una sola vez.[2040] Al resolver el recurso de revisión, el Instituto o los órganos garantes podrán emitir las resoluciones siguientes: i) sobreseerlas[2041] o desecharlas[2042] por improcedentes; ii) confirmar la respuesta, la cual también tendrá este sentido ante la falta de emisión de una resolución por parte de la autoridad; iii) revocar o modificar la respuesta u iv) ordenar la entrega de los datos personales, en caso de omisión.[2043]

2039 Artículos 103 y 104 de la LGPDPPSO.

2040 Artículo 108 de la LGPDPPSO.

2041 El recurso de revisión solo podrá ser sobreseído cuando: i) el recurrente se desista expresamente; ii) el recurrente fallezca; iii) admitido el recurso de revisión, se actualice alguna causal de improcedencia conforme a la ley; iv) el responsable modifique o revoque su respuesta de tal manera que el recurso de revisión quede sin materia o v) quede sin materia el recurso. Véase artículo 113 de la LGPDPPSO.

2042 El recurso de revisión podrá ser desechado por improcedente cuando: i) sea extemporáneo; ii) el titular o su representante no acrediten debidamente su identidad y personalidad; iii) el Instituto o los organismos garantes hayan resuelto anteriormente en definitiva sobre la materia del mismo; iv) no se actualice alguna de las causales del recurso de revisión previstas la propia ley; v) se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el recurrente, o en su caso, por el tercero interesado, en contra del acto recurrido; vi) el recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos o vii) el recurrente no acredite interés jurídico. Véase artículo 112 de la Ley LGPDPPSO.

2043 En las resoluciones se deberá precisar los plazos y términos para su cumplimiento y los procedimientos para su ejecución. Si durante el procedimiento se detecta una probable responsabilidad del sujeto obligado por el incumplimiento a las obligaciones de la ley, se informará al órgano interno de control o a la instancia competente para que inicie el procedimiento respectivo. Véase artículo 111 de la LGPDPPSO.

Las resoluciones del recurso de revisión serán vinculantes, definitivas e inatacables para los responsables, y solo podrán ser controvertidas por los titulares mediante recurso de inconformidad cuando se trata de decisiones de los organismos garantes de las entidades federativas, o bien, a través del juicio de amparo ante el Poder Judicial de la Federación, y en el caso de que la autoridad que conozca sea el INAI en relación a sujetos obligados federales, se podrá impugnar solamente mediante juicio de amparo.[2044]

El recurso de inconformidad es un medio de impugnación que permite controvertir ante el Instituto, en segunda instancia, una resolución del recurso de revisión emitida por el organismo garante de una entidad federativa, y procederá contra sus decisiones cuando:

a) clasifiquen los datos personales sin que se cumplan las características señaladas en las leyes aplicables;
b) determinen su inexistencia o
c) declaren la negativa de datos personales, porque: i) se entreguen incompletos; ii) no correspondan con los solicitados; iii) se niegue su acceso, rectificación, cancelación u oposición; iv) se entreguen o pongan a disposición en un formato incomprensible; v) exista desacuerdo con costos de reproducción, envío, o tiempos de entrega o vi) se oriente a un trámite específico que no garantice el ejercicio de los derechos ARCO.[2045]

Las resoluciones del INAI deberán dictarse en un plazo que no exceda 30 días a partir del día siguiente de la interposición del recurso de inconformidad, el cual podrá ampliarse por una sola vez y hasta por un periodo igual y adoptarán los sentidos siguientes: i) sobreseer[2046] o desechar[2047] el recurso de inconformidad; ii) confirmar la resolución del organismo garante de la entidad federativa, decisión que también ocurrirá en caso de que el Instituto omita dictar dicha resolución; iii) revocar o modificar la resolución del organismo garante estatal u iv) ordenar la entrega de los datos personales, en caso de omisión del responsable.[2048]

Si la resolución del recurso de inconformidad ordena la modificación o revocación de la decisión de primera instancia del organismo garante de transparencia estatal, éste deberá emitir una nueva.[2049]

Los fallos del recurso de inconformidad son vinculantes, definitivos e inatacables para los responsables y para los organismos garantes de transparencia de las entidades federativas, y solo podrán impugnarse por los titulares de los datos personales ante el Poder Judicial de la Federación mediante el juicio de amparo.[2050]

2044 Artículos 115 y 116 de la LGPDPPSO.

2045 Artículos 117 y 118 de la LGPDPPSO.

2046 Podrá ser sobreseído cuando: i) el recurrente se desista expresamente; ii) el recurrente fallezca; iii) el organismo garante modifique o revoque su respuesta de tal manera que el recurso de inconformidad quede sin materia o iv) admitido el recurso, se actualice alguna causal de improcedencia en los términos de la ley. Véase artículo 126 de la LGPDPPSO.

2047 Podrá ser desechado por improcedente cuando: i) sea extemporáneo; ii) el Instituto anteriormente haya resuelto en definitiva sobre la materia del mismo; iii) no se actualicen las causales de procedencia del recurso de inconformidad; iv) se esté tramitando ante el Poder Judicial algún recurso o medio de defensa interpuesto por el titular, o en su caso, por el tercero interesado, en contra del acto recurrido o v) el inconforme amplíe su solicitud en el recurso de inconformidad, únicamente respecto de los nuevos contenidos. Véase artículo 125 de la LGPDPPSO.

2048 Artículos 120 y 124 de la LGPDPPSO.

2049 La nueva resolución deberá dictarse dentro del plazo de 15 días, contados a partir del día siguiente al en que se hubiere notificado o se tenga conocimiento de la resolución dictada en la inconformidad. Véase artículo 127 de la LGPDPPSO.

2050 Artículo 129 de la LGPDPPSO.

La facultad de atracción de los recursos de revisión de los órganos garantes de transparencia de las entidades federativas consiste en que el INAI, cuando así lo apruebe la mayoría de sus comisionados de oficio o a petición fundada de dichos organismos garantes, podrá conocer de aquellos casos de datos personales que aún no hayan sido resueltos en el ámbito estatal, y que por su interés y trascendencia ameriten ser tratados por el órgano nacional de transparencia.[2051]

Para que el Instituto pueda atraer un asunto del ámbito local se deberá fundar y motivar el interés y trascendencia, lo que implica acreditar su relevancia, gravedad, novedad, complejidad y repercusión de manera sustancial en la solución de casos futuros para garantizar la tutela efectiva del derecho de protección de datos personales o fijar un criterio jurídico sobresaliente. Además de considerar específicamente para la materia de datos personales: i) la finalidad del tratamiento; ii) el número y tipo de titulares involucrados en dicho tratamiento realizado por el responsable; iii) la sensibilidad de los datos personales tratados; iv) las posibles consecuencias que se derivarían de un tratamiento indebido o indiscriminado y v) la relevancia del tratamiento en atención al impacto social o económico del mismo y del interés público.[2052]

La resolución del Instituto será definitiva e inatacable para el organismo garante de la entidad federativa y para el sujeto obligado de que se trate, mientras que los particulares podrán impugnarlas ante el Poder Judicial de la Federación.[2053]

La única excepción a las resoluciones definitivas en materia de protección de datos personales en posesión del sector público, es cuando existen elementos que puedan poner en peligro la seguridad nacional. En ese sentido, el Consejero Jurídico del Gobierno Federal podrá interponer un recurso de revisión ante la Suprema Corte de Justicia de la Nación (SCJN) cuando considere que las resoluciones emitidas por el Instituto pueden vulnerar la seguridad nacional.[2054]

El procedimiento de verificación a los sujetos obligados responsables del cumplimiento de la LGPDPPSO podrá iniciarse: i) de oficio cuando el Instituto o los organismos garantes de las entidades federativas cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes en materia de protección de datos personales que correspondan o ii) por denuncia del titular cuando considere que ha sido afectado por actos del responsable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones de la ley general y demás disposiciones, derecho que precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma.[2055]

La verificación no procederá ni se admitirá en los supuestos de procedencia del recurso de revisión o inconformidad previstos en la presente LGPDPPSO y tendrá una duración máxima de 50 días y concluirá con una resolución que emita el Instituto o los organismos garantes.[2056]

Las resoluciones del Instituto y de los órganos garantes estatales serán difundidas en versión pública, eliminando referencias al titular de los datos que lo identifiquen o lo hagan identificable y protegiendo la información reservada o confidencial.[2057]

2051 Artículo 130 de la LGPDPPSO.

2052 Artículos 130 y 131 de la LGPDPPSO y artículo 6 de los nuevos Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción, *Diario Oficial de la Federación*, 16 de febrero de 2017.

2053 Artículo 137 de la LGPDPPSO.

2054 Artículos 138,139 y 143 de la LGPDPPSO.

2055 Artículos 146 y 147 de la LGPDPPSO.

2056 Artículos 147, 149 y 150 de la LGPDPPSO.

2057 Artículos 33 de la LFTAIP y 57 de la LFPDPPP, y 114 de la LGPDPPSO.

Responsable del tratamiento

María Solange Maqueo Ramírez

1. Concepto

Tanto el artículo 3, fracción XIV, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), como el artículo 3, fracción XXVIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), coinciden en definir a los responsables del tratamiento como aquellas personas físicas o morales "que deciden sobre el tratamiento de los datos personales", aunque difieren en cuanto a la naturaleza, privada o pública, de quien funge como tal.

2. Elementos

De acuerdo con lo anterior, la definición del responsable del tratamiento se compone de tres elementos específicos: (1) el primero se refiere a la existencia de un ente (persona física o jurídica susceptible de ser sujeto de derechos y obligaciones en términos jurídicos, ya sea de derecho público o privado). Sobre este particular, cabe mencionar lo dispuesto por el artículo 8 del Reglamento de la LFPDPPP, el cual establece que "[l]as personas integrantes de un grupo que actúe sin personalidad jurídica y que trate datos personales para finalidades específicas o propias del grupo se considerarán también responsables o encargados, según sea el caso", donde la categoría de responsable (o encargado) recaerá en las personas que lo integran y no en el grupo como tal. (2) El segundo es relativo a la realización de actividades que configuran un tratamiento de datos personales en términos de la legislación aplicable y (3) el tercero consistente en que estas personas determinan o deciden efectivamente sobre el tratamiento.

3. Otras definiciones

El Reglamento General de Protección de Datos de la Unión Europea define al responsable del tratamiento como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el derecho de la Unión o de los Estados miembros".[2058]

Por su parte, los Estándares Iberoamericanos de Protección de Datos lo definen como aquella "persona física o jurídica de carácter privado, autoridad pública, servicios u organismo que, solo o en conjunto con otros, determina los fines, medios, alcance y demás cuestiones relacionadas con un tratamiento de datos personales".

Como puede observarse, la definición del Reglamento General de Datos Personales como la de los Estándares Iberoamericanos difieren de la que se adopta en el sistema jurídico mexicano, fundamentalmente en tres cuestiones:

1. No hay una referencia explícita a la corresponsabilidad en la definición legal de responsable, lo cual ciertamente no implica que ésta no sea factible en México si dos o más personas deciden sobre el tratamiento de los datos personales.

2058 Artículo 4 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. (Reglamento General de Protección de Datos).

2. Sobre los sujetos, en tanto que el Reglamento y los Estándares hacen alusión también a la posibilidad de que esa responsabilidad recaiga en servicios u otros organismos. Esta inclusión tiene sentido, jurídicamente hablando, si el término "responsable" se relaciona con el ámbito de aplicación de la normativa correspondiente, de tal forma que aún en aquellos supuestos en los que una persona física o moral tenga su residencia o establecimiento fuera del territorio correspondiente, pero presta servicios dentro del mismo, será considerado como responsable del tratamiento para efectos de dicha normativa.

Al respecto, el considerando 23 del Reglamento de la Unión Europea específica que con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de los interesados que residen en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento, si las actividades de tratamiento se refieren a la oferta de bienes o servicios de dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio *web* del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

Sobre el objeto en el que recaen las decisiones del responsable, mientras que en la legislación mexicana y en los Estándares, aunque con un fraseo distinto, se introduce en términos genéricos que las decisiones sean sobre el tratamiento de los datos personales, el Reglamento especifica que dichas determinaciones son sobre los fines y medios del tratamiento. En ese sentido, mientras que para la legislación mexicana cualquier persona que tome decisiones sobre la recolección, uso, divulgación, almacenamiento, transferencia o supresión de datos personales será considerada responsable del tratamiento, para la normativa de la Unión Europea, las determinaciones deben recaer sobre los fines y medios de dicho tratamiento, esto es, el por qué y el cómo del tratamiento.[2059] De tal forma que en este último caso se abre la posibilidad de que ciertas decisiones sobre el tratamiento de datos personales, no caracterizadas como esenciales en cuanto a los fines y medios del tratamiento por las legislaciones domésticas de los Estados miembros de la Unión, puedan ser adoptadas por el encargado del tratamiento sin que por ello pierda este carácter.

En términos generales, el responsable del tratamiento de datos personales está sujeto al cumplimiento de los principios del derecho a la protección de datos personales, los deberes de confidencialidad y la adopción de medidas de seguridad físicas, técnicas y administrativas, así como las demás obligaciones generales que establece tanto la LGPDPPSO como la LFPDPPP en la materia, por ejemplo, la incorporación de procedimientos que permitan ejercer de manera eficaz los derechos ARCO. Cabe decir que el primero de estos

2059 Grupo de Trabajo del Artículo 29 sobre Protección de Datos, Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento, adoptado el 16 de febrero de 2010, pp. 14 y 15

ordenamientos extiende dichas obligaciones a fin de incorporar la protección de datos desde el diseño y por defecto, la elaboración de sistemas de gestión y, en su caso, las evaluaciones de impacto a la protección de datos personales, por citar solo algunas. Todo lo cual es consistente con la llamada responsabilidad demostrada.[2060]

4. Diferencia entre responsable y encargado

De conformidad con el artículo 3, fracción IX, de la LFPDPPP el encargado es "[l]a persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable". De manera quizá más precisa, pero sin que ello implique una distinción sustantiva del término, el artículo 3, fracción XV, de la LGPDPPSO señala que el encargado es "[l]a persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable".[2061]

Las diferencias entre la figura del responsable y el encargado consisten en que mientras el primero decide sobre el tratamiento de los datos personales, el segundo se transforma en un mero ejecutor de las indicaciones que le formule el primero, siempre que sea ajeno a su organización y actúe a su nombre. En el supuesto de que el encargado tomara alguna decisión sobre el tratamiento de los datos personales, por cuenta propia, dejaría de ser considerado como encargado ocupando también el carácter de responsable. Estas diferencias quedan claramente explícitas en el artículo 58 de la LGPDPPSO, el cual señala que "[e]l encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable". Por ello es necesario que la relación entre el responsable del tratamiento y el encargado esté debidamente formalizada a través de algún instrumento jurídico, de forma que sea factible advertir la existencia, alcance y contenido de la relación jurídica.

Un ejemplo en el cual se materializa la relación entre responsable y encargado del tratamiento de datos personales se encuentra en la contratación de servicios, aplicaciones o infraestructura de cómputo en la nube. En estos casos, los artículos 63 y 64 de LGPDPPSO establecen obligaciones específicas en la relación jurídica a fin de garantizar que las políticas de protección de datos personales que adopte el proveedor (encargado) sean equivalentes a los principios y deberes establecidos por la normatividad del Estado mexicano en la materia.

En cuanto a las diferencias entre figuras también cabe mencionar que las comunicaciones entre los responsables y encargados no se entenderán en ningún caso como transferencias, sino que adquirirán el carácter de remisiones, término adoptado por la legislación mexicana para distinguir el régimen al cual se sujetan. Las comunicaciones entre responsables se entenderán, por el contrario, como transferencias nacionales o internacionales, según sea el caso.

Finalmente, cabe mencionar la posibilidad de que el encargado subcontrate algunos de los servicios que impliquen un tratamiento de datos personales por cuenta y nombre del responsable, para lo cual requiere la autorización expresa del responsable y la formalización

2060 El considerando 74 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), publicado en *Diario Oficial de la Unión Europea* el 4 de mayo de 2016, establece la responsabilidad del responsable entendida como la adopción de medidas oportunas, eficaces y, además, demostrables. En términos de este considerando, "dichas medidas deben tener en cuenta el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas".

2061 Sobre el concepto de "encargado del tratamiento" véase la voz correspondiente en este diccionario.

de esta subcontratación en un instrumento jurídico que permita acreditar la existencia, alcance y contenido de esta relación jurídica.[2062] En este caso, el subcontratado también tendrá el carácter de encargado del tratamiento de datos personales y, en caso de incumplimiento, asumirá el carácter de responsable.[2063]

Revisión del Sistema de Autorregulación Vinculante

Rosa María Franco Velázquez

El sistema de autorregulación vinculante en materia de protección de datos que se crea a través del cumplimiento de los requisitos y contenidos mínimos establecidos en los Parámetros de Autorregulación Vinculante[2064] tendrá que ser objeto de revisiones detalladas y periódicas.

Estas revisiones tienen que realizarse también cuando se produzcan cambios en la normativa que sea aplicable, en la tecnología o en los valores y procedimientos del responsable o encargado del tratamiento "que afecten aspectos significativos" del Sistema de Gestión de Datos Personales (SGDP).[2065]

El objeto de la revisión[2066] es, en particular, verificar que se cumple de manera continua con los contenidos exigibles a los esquemas de autorregulación vinculante, incluida la certificación. Es decir, la revisión se llevará a cabo por un tercero independiente con la finalidad de brindar "una mayor certeza en cuanto a que el esquema fue desarrollado e implementado de una manera adecuada, demostrando el compromiso adquirido en materia de protección de datos personales", tal y como se indica en los Considerandos de los Parámetros de Autorregulación Vinculante.

En concreto, las revisiones administrativas, mismas que deberán ser documentadas, se deberán basar en los siguientes aspectos o elementos:[2067]

I. la retroalimentación por parte de los usuarios del SGDP;
II. los riesgos identificados en el análisis de riesgos;
III. los resultados de auditorías;
IV. los resultados de las revisiones;
V. las actualizaciones o cambios en la tecnología utilizada por el responsable o encargado;
VI. los requerimientos por parte de autoridades;
VII. el manejo de quejas, y
VIII. las vulneraciones de seguridad.

2062 Artículos 61 y 62 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

2063 Cfr. Numeral 35 de los Estándares Iberoamericanos de Protección de Datos y artículo 112 del "acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público", publicados en el *Diario Oficial de la Federación* el 26 de enero de 2018.

2064 Parámetros de Autorregulación en Materia de Protección de Datos Personales, publicados en el *Diario Oficial de la Federación* del 29 de mayo de 2014.

2065 En el párrafo primero del numeral 32 de los Parámetros se indica que "También deberán preverse revisiones administrativas cuando se lleven a cabo cambios que afecten aspectos significativos del SGDP, tales como cambios en la normativa aplicable, en la tecnología o en los valores y procedimientos del responsable o encargado".

2066 El concepto de revisión, según la fracción XII del numeral 4 de los Parámetros, es definido como la "actividad estructurada, objetiva y documentada, llevada a cabo con la finalidad de constatar el cumplimiento continuo de los contenidos establecidos en los esquemas de autorregulación vinculante, incluida la certificación".

2067 Según lo indicado en el numeral 32 de los Parámetros.

Son los responsables y encargados quienes tienen también la obligación de "prever, implementar y mantener revisiones administrativas regulares y programadas, para asegurar un adecuado desarrollo continuo y la efectividad del SGDP".[2068]

La revisión, por tanto, se basa en el mantenimiento continuo de los requisitos exigibles a los esquemas de autorregulación vinculante, ya que su pérdida daría lugar a que no puedan ser mantenidos como tal.

Sin perjuicio de lo anterior, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en virtud de lo previsto en el numeral 48 de los Parámetros, podrá llevar a cabo revisiones periódicas de aquellos esquemas de autorregulación vinculante que hayan sido objeto de validación con el fin de "comprobar el nivel de eficacia y eficiencia del esquema, así como de su cumplimiento".

En concreto, y para garantizar que puedan realizarse estas revisiones periódicas, el INAI tiene atribuidas potestades que le permitirán efectuar requerimientos de información a los responsables o encargados del tratamiento que tengan un sistema de autorregulación vinculante validado, así como visitar las instalaciones de estos responsables o encargados del tratamiento o del administrador del esquema de autorregulación vinculante.

Además, el INAI, en virtud de la revisión que haya realizado, podrá emitir recomendaciones dirigidas, según corresponda, al responsable o al encargado del tratamiento o al administrador del esquema de autorregulación vinculante y el incumplimiento de las recomendaciones que emita el INAI podrá dar lugar a la baja del esquema de autorregulación vinculante del registro que mantiene, lo que supondría perder los beneficios correspondientes.[2069]

En relación con estas revisiones, cabe señalar que también les corresponde a los organismos de certificación "establecer procedimientos y planes para llevar a cabo revisiones periódicas de mantenimiento y vigilancia, incluyendo visitas de auditoría, en intervalos anuales para asegurar el cumplimiento continuo por parte de los responsables y encargados".[2070]

El incumplimiento de estas revisiones periódicas daría lugar a la pérdida de la condición de sistema de autorregulación vinculante.

Como parte del sistema de autorregulación vinculante, es necesario tomar en consideración que se deberá establecer un SGDP,[2071] que será objeto de revisión con el fin de lograr, de manera efectiva, la mejora continua del sistema.[2072] En concreto, se trata de una de las actividades a realizar como parte del ciclo PHVA (planificar, hacer, verificar y actuar) y que pertenece a la última de las fases indicadas.

Esta actividad da lugar a que, según corresponda, el responsable o encargado del tratamiento que tenga el sistema de autorregulación vinculante deba asignar, como parte de las funciones y responsabilidad exigibles, la relativa a "realizar revisiones administrativas y auditorías del SGDP".[2073]

2068 Numeral 32 de los Parámetros.

2069 En concreto, el numeral 48 de los Parámetros indica lo siguiente:
"Revisiones periódicas por parte del Instituto 48. El Instituto podrá realizar revisiones periódicas a los esquemas que haya validado, para lo cual podrá efectuar requerimientos de información y visitas a las instalaciones de los responsables o encargados adheridos al esquema de que se trate o de su administrador, a fin de comprobar el nivel de eficacia y eficiencia del esquema, así como de su cumplimiento. El Instituto podrá emitir recomendaciones derivadas de los resultados obtenidos de sus revisiones. El incumplimiento de estas recomendaciones podrá ser tomado en consideración por el Instituto para la baja del mecanismo de autorregulación vinculante en el registro, en términos del artículo 86 del Reglamento".

2070 Numeral 75 de los Parámetros.

2071 En virtud del numeral 14 de los Parámetros uno de los requisitos del contenido mínimo es el relativo a "VI. Desarrollar e implementar un SGDP".

2072 Numeral 37 de los Parámetros.

2073 La fracción III del numeral 21, relativo a la asignación de funciones y responsabilidades, indica que el responsable o encargado deberá asignar la relativa a "realizar revisiones administrativas y auditorías del SGDP y de la política para que reflejen las actualizaciones normativas, de práctica y tecnológicas".

Revocación del consentimiento

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El derecho a la revocación del consentimiento es una prerrogativa que la normatividad reconoce al titular de los datos para que pueda tener control sobre su información personal en posesión del responsable, habilitándole para que pueda retirar el consentimiento para el tratamiento en cualquier momento y sin que a éste se le atribuyan efectos retroactivos.

La revocación del consentimiento es un derecho que puede ejercer el titular como resultado de las características del consentimiento para el tratamiento, cualquiera que sea su modalidad (tácito, expreso o expreso y por escrito), dando lugar al cese del tratamiento de los datos personales.

Tanto en el sector privado como en el sector público, el derecho de revocación del consentimiento reconoce la posibilidad de que el titular de los datos revoque su consentimiento en cualquier momento y sin que a dicha acción se le atribuyan efectos retroactivos, respectivamente en el último párrafo del artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)[2074] y en el artículo 20 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales).

Aunque tradicionalmente el derecho a la revocación del consentimiento no es uno de los tradicionales derechos de acceso, rectificación, cancelación y oposición (ARCO),[2075] se suele sujetar al mismo procedimiento y condiciones para su ejercicio, y en el sector público los Lineamientos Generales sí lo incorporan en los tradicionales derechos de oposición y cancelación al señalar que la revocación se llevará a cabo por medio del ejercicio de los aludidos derechos.

Por su parte, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) reconocen este derecho y señalan, en su capítulo relativo a los principios, que "siempre que sea requerido el consentimiento para el tratamiento de los datos personales, el titular podrá revocarlo en cualquier momento, para lo cual el responsable establecerá mecanismos sencillos, ágiles, eficaces y gratuitos".[2076]

En el panorama internacional, el Reglamento General de Protección de Datos europeo (RGPD o GDPR por sus siglas en inglés) en el apartado 3 de su artículo 7 lo reconoce igualmente al precisar que el interesado tiene derecho a retirar su consentimiento en cualquier momento, y que dicha acción no afectará la licitud del tratamiento basada en el consentimiento previo a su retirada. [2077]

Retomando y profundizando un poco más en la explicación normativa doméstica anterior:

1. En el sector privado:
   a) El último párrafo del citado artículo 8 de la LFPDPPP obliga al responsable a prever el procedimiento para la revocación del consentimiento en el aviso de privacidad.

2074 Artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

2075 Derechos de acceso, rectificación, cancelación y oposición. Para mayor detalle se recomienda consultar la definición de "derechos ARCO" incluida en este *Diccionario de Protección de Datos Personales*.

2076 Artículo 12.1 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos.

2077 Artículo 7, apartado 3 del Reglamento General de Protección de Datos.

b) El artículo 21 del Reglamento de la LFPDPPP incorpora la regla de que el responsable deba establecer mecanismos sencillos y gratuitos, que permitan al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.

c) El lineamiento 29 de los Lineamientos del Aviso de Privacidad consigna la obligación del responsable de informar en el aviso de privacidad integral sobre el procedimiento y medios habilitados para el ejercicio del derecho de revocación del consentimiento, procurando que estos medios se implementen de forma tal que no se limite el ejercicio de este derecho por parte de los titulares, y que dicho procedimiento debe considerar lo ya especificado sobre la regla prevista en el artículo 21 del RLFPDPP.[2078] En concreto, señalan los lineamientos que se debe informar de:

i. Los requisitos, entre ellos, los mecanismos de acreditación de la identidad del titular y la personalidad de su representante y, en su caso, la información o documentación que se deberá acompañar a la solicitud.

ii. Los plazos dentro del procedimiento.

iii. Los medios para dar respuesta.

2. En el sector público:

a) Se entiende que es obligación del responsable informar mediante el aviso de privacidad sobre el procedimiento para la revocación del consentimiento de sus datos personales.

b) El artículo 20 de los Lineamientos Generales habilita al titular para revocar su consentimiento en cualquier momento, y señala que este derecho se ejercerá a través de los derechos de oposición y cancelación, por lo que, en consecuencia, su ejercicio se sujetará a los plazos y procedimientos establecidos para el ejercicio de derechos ARCO en general.

En definitiva:

a) El responsable se encuentra obligado a informar a los titulares de los datos sobre los medios y procedimientos para el ejercicio del derecho de revocación al consentimiento, incluso de forma independiente a la información relativa al ejercicio de los derechos ARCO.

b) La solicitud de revocación del consentimiento como cualquier otra prerrogativa que el titular ejerza ante el responsable deberá ser contestada expresamente por este último considerando su alcance y contenido.

c) Los términos de atención y respuesta sí son los mismos que los de los derechos ARCO. Así, en términos del RLFPDPPP los plazos aplicables a la respuesta de este derecho no podrán exceder los plazos generales establecidos para el ejercicio ARCO. Es decir, el plazo para comunicar la determinación adoptada respecto a la procedencia de la revocación no podrá exceder de 20 días hábiles contados a partir de la recepción de la solicitud, en caso de resultar procedente.[2079]

d) Si se concede la solicitud, ésta tiene un alcance general, es decir, dicha determinación deberá ser comunicada al encargado o encargados que traten los datos para que cesen el tratamiento de los mismos conforme a lo indicado por el responsable al titular.

2078 Estos medios según el lineamiento vigésimo noveno de los Lineamientos del Aviso de Privacidad, deberán ser de fácil acceso para los titulares y con la mayor cobertura posible, considerando su perfil y la forma en que mantienen contacto cotidiano o común con el responsable; gratuitos; que estén debidamente habilitados, y que hagan sencillo el acceso a la información.

2079 Artículo 32 de la LFPDPPP.

e) La negativa o falta de respuesta a la solicitud de derecho de revocación al consentimiento formulada por el titular podrá dar lugar a que el titular de los datos interponga ante la autoridad garante que corresponda (INAI u organismos garantes locales) una denuncia como resultado del tratamiento ilícito de sus datos.[2080]

Riesgo

Andrés Velázuez Olavarrieta

De acuerdo con la *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP), publicada en junio de 2015, el riesgo es la combinación de la probabilidad de un evento y su consecuencia desfavorable. La Agencia Española de Protección de Datos (AEPD)[2081] establece que el riesgo se deriva de la exposición a amenazas, por lo que, para la mejor comprensión, lo define como "la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas".

Riesgo de seguridad

Andrés Velázquez Olavarrieta

La *Guía para Implementar un Sistema de Gestión de Seguridad de Datos Personales* (GISGSDP), publicada en junio de 2015, define al riesgo de seguridad como "potencial de que cierta amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización".[2082] De ahí plantea que se debe identificar, valorar, comunicar y tratar el riesgo para encontrar, enlistar y describir los elementos del riesgo; establecer un proceso para asignar valores a la probabilidad y consecuencias del riesgo; compartir o intercambiar información entre la alta dirección, custodios y demás involucrados acerca del riesgo, y contar con procesos para modificar el nivel de riesgo.

En este último proceso, la *Guía* del IFAI contempla cinco rubros: aceptar el riesgo (decisión informada para coexistir con un nivel de riesgo), compartir el riesgo (proceso donde se involucra a terceros para mitigar la pérdida generada por un riesgo en particular, sin que el dueño del activo afectado reduzca su responsabilidad), evitar el riesgo (acción para retirarse de una situación de riesgo o decisión para no involucrarse en ella), reducir el riesgo (acciones tomadas para disminuir la probabilidad, las consecuencias negativas, o ambas, asociadas al riesgo), retención del riesgo (aceptación de la pérdida generada por un riesgo en particular. Esta acción implica monitoreo constante del riesgo retenido) y riesgo residual (el riesgo remanente después de tratar el riesgo).

2080 Artículo 22 de la LFPDPP y artículo 147 de la LGPDPPSO.

2081 AEPD. (2018). *Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD.* Disponible en: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf

2082 INAI. (2015, junio). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales.* Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

NOTAS

NOTAS

NOTAS

Seguridad de la información

Andrés Velázquez Olavarrieta

La seguridad de la información se define como el conjunto de reglas (políticas), mecanismos (controles) y acciones (procedimientos) que permiten asegurar la información de una organización sin importar la forma en que esta se represente (escrita, oral, gráfica, electrónica, entre otras).

Las tres propiedades que la seguridad de la información busca garantizar son: confidencialidad, integridad y disponibilidad. La confidencialidad es la propiedad que tiene la información de que únicamente personas debidamente autorizadas pueden acceder a ella. La integridad de la información consiste en que sea creada, modificada o eliminada solamente por personas debidamente autorizadas en función de sus roles y responsabilidades. La disponibilidad de la información consiste en que la información esté lista para ser tratada por personal autorizado en el momento y forma requerida.

La seguridad de la información es parte integral de los procesos de negocio de las organizaciones y para implementarla es necesario definir una estrategia y establecer planes de acción. Los elementos que conforman la estrategia y gestión de la seguridad de la información son:

a) contexto de la organización,
b) gobierno de seguridad de la información,
c) sistema de gestión de seguridad de la información y
d) cumplimiento

1. Contexto de la organización

El contexto de la organización se divide en externo e interno. El contexto externo comprende toda situación fuera de la organización que impacta en las decisiones estratégicas y tácticas en términos de la seguridad de la información. Algunos ejemplos de situaciones que comprenden el contexto externo son:

a) Situación económica. La situación económica del país o región en donde se encuentre la organización determina el interés de los atacantes, así como la facilidad de la organización para invertir en tecnologías de seguridad;

b) Situación geopolítica. El entorno político y la ubicación geográfica son riesgos de posibles ataques informáticos, de negación de servicio por parte de activistas o ataques a la infraestructura crítica por ciberejércitos o ciberterroristas;

c) Ambiente competitivo. La competencia entre las organizaciones ha provocado que organizaciones no éticas orquesten ataques cibernéticos hacia su competencia con fines comerciales.

d) Innovación en el mercado. La presión que tienen las organizaciones por ofrecer productos o servicios de novedad, que les represente una ventaja competitiva, provoca que la seguridad de la información no sea considerada desde un inicio.

Por otro lado, el contexto interno de una organización, desde el punto de vista de seguridad de la información, consiste en todas las situaciones propias de la organización que juegan un papel importante en la definición de acciones estratégicas y tácticas. Ejemplos de situaciones que conforman el contexto interno de una organización son:

a) la cultura organizacional. Está definida por el conjunto de principios y valores difundidos en toda la organización. Una organización con una cultura orientada a la seguridad de la información tendrá un menor número de incidentes de origen intencional o por error;

b) capacidad financiera. Una organización con una buena capacidad financiera y comprometida con la seguridad de la información podrá realizar inversiones en tecnología e implementación de procesos de gestión;

c) nivel de madurez en normatividad. Las organizaciones que cuentan con un marco normativo robusto podrán fácilmente crear, desplegar, forzar, seguir y actualizar políticas de seguridad de la información;

d) nivel tecnológico. Una organización que está altamente tecnificada podrá integrar y administrar correctamente tecnologías de punta de una manera eficiente y segura y

e) apetito al riesgo. Este término refiere al nivel de riesgo en seguridad de la información que una organización está dispuesta a aceptar como referencia para decidir sobre el tratamiento para cada escenario de riesgo.

2. Gobierno de seguridad de la información

Es un subconjunto del gobierno corporativo que provee estrategias, asegura que los objetivos de la organización sean alcanzados, administra apropiadamente los riesgos, usa los recursos responsablemente, y monitorea los programas de seguridad de la organización.

El gobierno de seguridad de la información en una organización que opera bajo los siguientes principios rectores:

a) obtener el compromiso de los altos directivos;

b) ser parte del gobierno corporativo;

c) alinear la seguridad de la información a la estrategia de negocio;

d) asignar autoridad, responsabilidades y recursos a las personas involucradas en la gestión de la seguridad de la información y

e) operar bajo mejores prácticas y un marco normativo.

Un gobierno de seguridad de la información está compuesto por una estructura con una definición clara de roles y responsabilidades. La estructura mínima recomendada para un gobierno de seguridad de la información y sus principales funciones son las siguientes:

a) alta dirección. La alta dirección o junta directiva (*board of directors*) debe conocer cuál es la información crítica de la organización y el nivel de riesgo al que está expuesta, además, debe garantizar el compromiso de apoyo al comité de seguridad y debe aprobar y difundir las políticas de seguridad de alto nivel;

b) comité de seguridad. El comité de seguridad debe estar compuesto por representantes de cada unidad de negocio con autoridad para la toma de decisiones, debe asegurar la alineación de los programas de seguridad con los objetivos del negocio y promover la cultura de la seguridad de la información, además de vigilar el cumplimiento de las políticas y

c) oficial de seguridad de la información (CISO por sus siglas en inglés). Es responsable de la implementación de la estrategia mediante la realización de programas de seguridad o planes de acción. Debe tener autoridad para la toma de decisiones y contar con los recursos necesarios.

3. Sistema de gestión de seguridad de la información (SGSI)

El SGSI es un proceso sistemático que permite establecer, implementar y mantener la seguridad de la información en una organización. El proceso que se sigue para poner en marcha un SGSI sigue el círculo de *Deming* el cual establece cuatro fases conocidas como PDCA (por sus siglas en inglés, *plan, do, check y act*):

a) Planeación

b) Implementación

c) Evaluación

d) Mejora

La fase de planeación consiste en definir el alcance mediante el establecimiento de los límites y la aplicabilidad. Se especifican claramente los objetivos del SGSI, es decir, se debe responder a la pregunta ¿Para qué se está haciendo el presente plan de gestión de la seguridad? Para llevarlo a cabo se debe contar con la autorización de la alta dirección mediante el compromiso, así como la asignación de recursos. Se define una estrategia de comunicación para exponer efectivamente los beneficios del plan de seguridad y se dejan en claro los roles y responsabilidades dentro del plan para todos y cada uno de los miembros de la organización. Finalmente, en esta fase se establecen los estándares o mejores prácticas para emplear en la implementación del plan de seguridad, así como en cada una de las actividades dentro de cada fase. La planeación de un SGSI puede diseñarse e implementarse utilizando estándares internacionales como el ISO/IEC 27001,[2083] NIST SP800-100[2084] o COBIT-5-IS.[2085]

La fase de implementación comprende tres tareas: realizar un análisis de riesgo, elaborar planes de acción e implementar medidas de seguridad. El análisis de riesgo es un procedimiento formal para identificar, evaluar y priorizar los riesgos dentro de una organización. Existen varios estándares internacionales para llevar a cabo un análisis de riesgo como ISO/IEC 27005,[2086] ISO/IEC 31000[2087] y NIST 800-30.[2088] Las etapas para realizar un análisis de riesgo son:

2083 ISO/IEC 27001. (2013). *Information technology-Security techniques-Information security management systems-Requirements*. ISO/IEC. Segunda edición.

2084 Bowen, P. et al. (2006, octubre). *Information Security Handbook: A Guide for Managers. Special Publication 800-100*. NIST.

2085 ISACA. (2013). *Cobit 5 for Information Security.*

2086 ISO/IEC 27005. (2011). *Information technology-Security techniques-Information security risk management*. ISO/IEC. Segunda edición.

2087 ISO/IEC 31000. (2018). *Risk Management*. ISO/IEC. Segunda edición.

2088 Stonebumer, G. et al. (2002, julio). *Risk Management Guide for Information Technology Systems. Special Publication 800-30*. NIST.

a) Identificación de activos. Consiste en identificar cuáles son los activos críticos de la organización que deberán protegerse.
b) Identificación de amenazas. Fase en la cual se determinan las fuentes de ataque y la forma en que pueden atacar, básicamente se pueden clasificar en amenazas internas y externas.
c) Identificación de vulnerabilidades. En esta etapa se identifican las debilidades en la infraestructura tecnológica, en los procesos o en la gente que puede ser explotada o aprovechada por las amenazas. En la evaluación de vulnerabilidades se debe de tomar en cuenta los controles existentes.
d) Determinación del riesgo. En la última fase se evalúa el riesgo con base en dos parámetros, la probabilidad de ocurrencia y el impacto producido. El análisis de riesgo genera una lista de riesgos evaluados y priorizados, esta lista sirve para elaborar un plan de acción de tratamiento para cada uno de los riesgos. En esta fase se seleccionan e implementan las medidas de seguridad correspondientes para aquellos riesgos que se van a mitigar. Algunos estándares internacionales para la selección e implementación de medidas de seguridad son el ISO/IEC 27002[2089] y el NIST 800-53.[2090]

La fase de evaluación del SGSI consiste en monitorear y medir el desempeño de las medidas de seguridad implementadas. Para realizar una evaluación objetiva, es necesario definir las métricas de desempeño y se analizan los resultados de las mediciones. La evaluación puede realizarse de manera automatizada o mediante auditorías.

El resultado de la evaluación de desempeño sirve para realizar la última fase del SGSI, la cual consiste en llevar a cabo los ajustes en la implementación de las medidas de seguridad con la finalidad de conformar un proceso de mejora continua.

4. Cumplimiento

La estrategia y gestión de la seguridad de la información de una organización están influenciadas por las disposiciones regulatorias a nivel nacional o internacional a las que estén sometidas las organizaciones. Existen obligaciones de cumplimiento por sector como las organizaciones del sector salud o entidades financieras, mientras que existen legislaciones a nivel global sin importar el sector como la legislación en el tema de protección de datos personales.

Seudonimización

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La seudonimización[2091] se refiere a un tratamiento de datos personales a partir del cual estos últimos no son susceptibles de ser atribuidos directamente a su titular sin el empleo de información adicional y desagregada.

2089 ISO/IEC 27002. (2013). *Information technology-Security techniques-Code of practice for information security controls*. ISO/IEC. Segunda edición.

2090 NIST: (2013, abril). *Security and Privacy Controls for Federal Information Systems and Organizations. Special Publication 800-53*. NIST.

2091 En relación con el contenido de este concepto, recomendamos consultar las definiciones de “anonimización”, “big data” y “disociación” que se encuentran en este *Diccionario de Protección de Datos Personales*.

El concepto de seudonimización no ha sido regulado en la normatividad nacional de protección de datos personales, pero es posible encontrar clarificaciones sobre su contenido y alcance en la regulación internacional.

El Reglamento General de Protección de Datos Personales europeo (RGPD O GDPR por sus siglas en inglés) aporta una definición legal de este concepto al puntualizar que es: "El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable".[2092]

El RGPD reconoce la utilidad de la seudonimización y precisa que tiene la capacidad de reducir riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos, sin excluir las medidas de seguridad técnicas u organizativas que pudieran adoptarse para garantizar la protección de los datos,[2093] teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento.[2094]

Así, podemos señalar que la seudonimización es un procedimiento que, como medida de seguridad, se aplica al dato personal para reducir los riesgos derivados de su tratamiento, mediante la sustitución de un atributo en un registro (por lo general, un atributo único) por otro, de forma tal que se puedan reidentificar los datos mediante el empleo de información adicional y separada[2095] que permita volver a asignar el atributo correcto a cada registro.

Al estudiar el concepto de dato personal, el Grupo de Trabajo del Artículo 29 (GT29 o WT29 por sus siglas en inglés)[2096] ha destacado que la seudonimización se emplea para ocultar identidades con el fin de poder recopilar más datos sobre una misma persona sin necesidad de conocer su identidad, siendo pertinente su uso en los ámbitos estadístico y en la investigación.[2097]

Así, se ha señalado que la "seudonimización" puede realizarse de forma que quede un rastro entre el seudónimo y la identidad con la que se corresponde, como por ejemplo listas de correspondencias o algoritmos criptográficos bidireccionales.[2098]

2092 Artículo 4, apartado 5, del Reglamento General de Protección de Datos Personales.

2093 Considerando 28 del Reglamento General de Protección de Datos Personales.

2094 Artículo 25
Protección de datos desde el diseño y por defecto
1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2095 En este sentido el Reglamento General de Protección de Datos señala:
(29) Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

2096 Este grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

2097 Grupo de Trabajo del Artículo 29, Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007. WP 136, p.23, consultado el 14 de noviembre de 2018. Disponible en:
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

2098 Grupo de Trabajo del Artículo 29, Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007. WP 136, p.23, consultado el 14 de noviembre de 2018.

La diferencia fundamental entre la seudonimización con otros conceptos afines, como la anonimización, es que tras el proceso de "seudonimización" los datos son rastreables, y por lo tanto pueden considerarse información sobre personas físicas indirectamente identificables y en consecuencia resultará de aplicación la normatividad (puesto que la utilización de un seudónimo supone la posibilidad de seguir un rastro hasta llegar a la identidad de la persona, aunque solo en condiciones previamente definidas),[2099] mientras que en el segundo caso, si se aplica una técnica robusta y real de anonimización, no es posible asociar el contenido de la información con una persona física identificada o identificable, y por lo tanto dicha información ya no podrá ser considerada dato personal.

Es decir, aunque la seudonimización es una medida de seguridad relevante para proteger los datos personales, no es la mejor forma de proteger adecuadamente a los interesados ante filtraciones de identidad o de atributos, pues aunque reduce la capacidad de vinculación de un conjunto de datos con la identidad del interesado, no es un método de anonimización.[2100]

Para que funcione la seudonimización es preciso tener en cuenta diversos factores como en qué etapa se utiliza, su grado de seguridad contra el rastreo inverso, el tamaño de la población en la que se oculta al individuo, la capacidad de vincular transacciones o documentos individuales con una misma persona, entre otros.[2101] Además, el GT29 recomienda:

a) que los seudónimos sean aleatorios e imprevisibles;
b) que el número de seudónimos posibles sea tan amplio que no exista la posibilidad de seleccionar aleatoriamente el mismo seudónimo dos veces y
c) en el supuesto de que sea necesario un alto nivel de seguridad, el grupo de posibles seudónimos debe ser por lo menos igual a la gama de valores de funciones criptográficas numéricas seguras.

En conclusión, la seudonimización es una medida de seguridad recomendada, especialmente si se realiza con seriedad y, técnicas y procedimientos robustos, a partir de la cual se pueden reducir los riesgos en el tratamiento de datos personales por medio de la desagregación de los datos personales de forma tal que estos no puedan identificar a la persona a menos de que el responsable se apoye de información adicional que se encuentre a su disposición.

2099 Grupo de Trabajo del Artículo 29, Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio de 2007. WP 136, p.23, consultado el 14 de noviembre de 2018.

2100 Grupo de Trabajo de Trabajo del Artículo 29, Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014. WP 216, p.7. Consultado el 14 de noviembre de 2018. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

2101 Grupo de Trabajo de Trabajo del Artículo 29, Dictamen 05/2014 sobre técnicas de anonimización, adoptado el 10 de abril de 2014. WP 216, p.19. Consultado el 14 de noviembre de 2018. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

Sistema de certificación en materia de protección de datos personales

Jacobo Esquenazi Franco

El sistema de certificación en materia de protección de datos personales[2102] tiene por objeto que las personas físicas o morales acreditadas como organismos de certificación determinen la conformidad o grado de cumplimiento de los esquemas, y de su implementación, así como prácticas y herramientas tecnológicas que adopten responsables y encargados con relación a la Ley,[2103] su Reglamento[2104], los Parámetros de autorregulación vinculante[2105], las Reglas de Operación[2106] y demás normativa aplicable.[2107]

Dicho sistema se integra de diversos actores y niveles: (i) la Secretaría de Economía, quien autoriza a las entidades de acreditación con fundamento en la Ley Federal sobre Metrología y Normalización, y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), que reconoce a las entidades de acreditación autorizadas por la Secretaría de Economía, a los organismos de certificación y a los responsables y encargados certificados, mediante su inscripción en el Registro de Esquemas de Autorregulación Vinculante (REA); (ii) las entidades de acreditación,[2108] encargadas de acreditar[2109] a organismos de certificación; (iii) los organismos de certificación,[2110] encargados de certificar[2111] a responsables y encargados que lo soliciten y (iv) los responsables y encargados que buscan la certificación por parte de los organismos de certificación.

Los responsables y encargados que obtengan las certificaciones podrán distinguirse de otros por su compromiso con el debido tratamiento de los datos personales y elevar el nivel de confianza frente a los titulares de datos personales y la autoridad. Según la certificación de que se trate, algunos otros beneficios pueden ser:

- Facilitar la defensa de los derechos de los titulares de datos personales;
- Desarrollar normas de protección de datos personales armonizadas con los procedimientos de los responsables y encargados;

2102 Preguntas frecuentes del Registro de Esquemas de Autorregulación Vinculante consultado en: http://rea.inai.org.mx/_catalogs/masterpage/Sec1_3.aspx

2103 La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010. (La Ley).

2104 El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *Diario Oficial de la Federación* el 21 de diciembre de 2011. (El Reglamento).

2105 Parámetros de Autorregulación en materia de Protección de Datos Personales, publicados en el *Diario Oficial de la Federación* el 29 de mayo de 2014. (Los Parámetros).

2106 El Acuerdo del Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, por el que se aprueba el Proyecto de Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante y se instruye su publicación oficial, publicado en el *Diario Oficial de la Federación* el 18 de febrero de 2015. (Las Reglas de Operación).

2107 Preguntas frecuentes del Registro de Esquemas de Autorregulación Vinculante consultado en: http://rea.inai.org.mx/_catalogs/masterpage/Sec1_3.aspx

2108 Persona moral autorizada por la Secretaría de Economía, de conformidad con la Ley Federal sobre Metrología y Normalización, para acreditar organismos de certificación en materia de protección de datos personales. Numeral 5, fracción IV, de los Parámetros.

2109 Acto por el cual una entidad de acreditación aprobada en términos de la Ley Federal sobre Metrología y Normalización, reconoce la competencia técnica y confiabilidad de organismos de certificación para la evaluación de la conformidad de la Ley, el Reglamento, los presentes Parámetros y demás normativa aplicable. Numeral 5, fracción I, de los Parámetros.

2110 Persona que tiene por objeto realizar funciones de certificación en materia de protección de datos personales. Numeral 5, fracción V, de los Parámetros.

2111 Procedimiento llevado a cabo por un organismo de certificación por el cual se asegura que un esquema y su implementación se ajustan a la Ley, el Reglamento, los presentes Parámetros y demás normativa en materia de protección de datos personales en posesión de particulares. Numeral 5, fracción II, de los Parámetros.

- Contar con un sistema de resolución extrajudicial de controversias que permite soluciones eficaces, equitativas, rápidas y a bajo costo;
- Facilitar las transferencias transfronterizas de datos personales;
- Poder ser considerados por el INAI para una disminución en el monto en caso de sanción.
- Contar con un sistema para documentar y acreditar ante el titular y la autoridad el cumplimiento de la normativa aplicable.

La Secretaría de Economía deberá notificar al INAI cierta información respecto a la persona moral que haya tramitado y obtenido la autorización para ser entidad de acreditación, así como cuando suspenda o revoque dicha autorización.[2112] La notificación al INAI deberá contener: i) nombre y domicilio de la entidad de acreditación autorizada; ii) oficinas que se encuentran amparadas por la autorización; iii) vínculo al sitio de Internet o cualquier otro medio a través del cual la entidad de acreditación publique la información requerida en términos de los Parámetros de autorregulación vinculante; iv) símbolo o distintivo en caso de que lo hubiera y v) la fecha efectiva de otorgamiento de la autorización.[2113]

El trámite para notificar y solicitar el reconocimiento e inscripción en el REA es gratuito.

Cualquier persona física o moral interesada en ser organismo de certificación deberá presentar su solicitud ante una entidad de acreditación autorizada para tal efecto por la Secretaría de Economía y reconocida como tal por el INAI, a través del REA, así como satisfacer los requisitos y procedimientos establecidos por dicha entidad de acreditación para otorgar acreditaciones, los cuales deberán ser puestos a disposición pública por la misma entidad de acreditación.

La persona u organización que trate datos personales (responsable o encargado) que esté interesado en obtener una certificación deberá iniciar el procedimiento ante un organismo de certificación acreditado por una entidad de acreditación reconocida por el INAI. El organismo de certificación establecerá el procedimiento que deberá seguir para obtener la certificación y se cerciorará que sus tratamientos, políticas, programas y procedimientos relacionados con la protección de datos personales sean acordes con lo previsto por la normativa mexicana en la materia.

Las certificaciones otorgadas en materia de protección de datos personales tendrán una vigencia de dos años. Los certificados[2114] podrán ser renovados al término de ese plazo. Los procedimientos y condiciones para la certificación y su renovación, modificación, suspensión y cancelación, así como los precios de las mismas, serán determinados por el organismo de certificación.[2115]

De conformidad con el artículo 39, fracciones I, II, III, IV y XII de la Ley, el INAI contará con las siguientes atribuciones específicas con respecto al sistema de certificación en materia de protección de datos personales:

I. Requerir a la Secretaría que inicie un procedimiento de suspensión o revocación de la autorización otorgada a las entidades de acreditación; […]a las entidades

2112 Sección III, "de las entidades de acreditación y de la acreditación a organismos de certificación". Numerales 61 a 73 de los Parámetros.

2113 Numeral 63 de los Parámetros.

2114 Documento expedido por un organismo de certificación acreditado, mediante el cual se hace constar la certificación en materia de protección de datos personales otorgada a un responsable o encargado en específico. En él se encuentran descritos los alcances de dicha certificación. Numeral 5, fracción III, de los Parámetros.

2115 Numeral 76 de los Parámetros.

de acreditación que inicien un procedimiento de suspensión o cancelación de acreditaciones otorgadas a un organismo de certificación y […] a los organismos de certificación que inicien un procedimiento de suspensión o cancelación de certificados, cuando disponga de elementos suficientes para justificar esa actuación en los términos de la Ley, el Reglamento y los Parámetros;

II. […]

III. […]

IV. Requerir información a las entidades de acreditación, organismos de certificación, responsables certificados, encargados certificados y autoridades, así como solicitar el auxilio de estas últimas, para la aplicación de los presentes Parámetros;

V. Participar, cuando así lo considere necesario, en los comités de evaluación para la acreditación de organismos de certificación; en los comités de certificación para la certificación de responsables y encargados en materia de protección de datos personales;[…]

VI. […]

VII. Emitir opiniones sobre los procedimientos de otorgamiento, suspensión y cancelación de acreditaciones llevados a cabo por las entidades de acreditación;

VIII. Hacer de conocimiento de la Secretaría, cuando conozca de hechos que pudieran derivar en una posible suspensión o revocación de una autorización a las entidades de acreditación respecto de la aplicación de la Ley sobre Metrología;

IX. Promover, […], la constitución de programas de estudio y capacitación con el objeto de formar técnicos calificados en materia de protección de datos personales;

X. Reconocer, mediante su inscripción en el Registro, a las entidades de acreditación autorizadas por la Secretaría de Economía; […]las acreditaciones de organismos de certificación que otorguen las entidades de acreditación autorizadas por la Secretaría de Economía, y […]a las certificaciones otorgadas por los organismos de certificación, en materia de protección de datos personales.

XI. […]

XII. […]

El INAI mantendrá un listado actualizado de las entidades de acreditación autorizadas, de los organismos de certificación, así como de los responsables o encargados certificados en materia de protección de datos personales, el cual se hará público a través del REA.[2116]

Sistema de gestión de seguridad de datos personales

Uciel Fragoso Rodríguez

El estándar internacional ISO/IEC 27000[2117] define a un sistema de gestión de seguridad de la información (SGSI) como el conjunto de políticas, procedimientos, guías, actividades y recursos asociados con un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información dentro de la organización con la finalidad de alcanzar los objetivos de negocio.

La adopción de un SGSI es una decisión estratégica que permite a las organizaciones preservar la confidencialidad, integridad y disponibilidad de la información. El sistema de gestión debe ser parte de los procesos de negocio y se basa en un procedimiento de gestión de riesgos.

2116 Numeral 60 de los Parámetros.

2117 ISO/IEC 27000, "Information security management systems – Overview and vocabulary". ISO/IEC. Third edition, 2014.

El estándar ISO/IEC 27001[2118] especifica los requerimientos para implementar un sistema de gestión de seguridad de la información dentro del contexto de una organización. Los requerimientos definidos en el estándar son genéricos y aplicables a todas las organizaciones, sin importar el tamaño, tipo o naturaleza. El estándar está organizado por cláusulas que permiten establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, las cláusulas referidas son:

1) Especificación del contexto de la organización. En este punto se determinan los aspectos externos e internos relevantes para el propósito del SGSI y que pudieran afectar los resultados. También se identifican los grupos de interés para definir los requerimientos de seguridad incluyendo aquellos de tipo legal y regulatorio. Otro aspecto importante en esta cláusula es el establecimiento del alcance del SGSI mediante la definición de sus límites y aplicabilidad.
2) Obtención del liderazgo y compromiso. Los altos directivos de la organización deben demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información. Para ello, deben establecer políticas y objetivos alineados al negocio, integrar el SGSI a los procesos del negocio, asignar recursos, comunicar la importancia del SGSI y promover la mejora continua. Otras responsabilidades de los altos directivos en términos de seguridad de la información es la asignación de roles, responsabilidades y niveles de autoridad, así como el seguimiento del desempeño del SGSI.
3) Establecimiento de planes de acción. En la fase de planeación se establecen los objetivos de seguridad a alcanzar y de identifican los factores críticos de éxito para garantizar la correcta implementación y operación del SGSI. En este punto se lleva a cabo una evaluación de riesgo en donde se identifican los riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información crítica de la organización. Se crean escenarios de riesgo, en donde se identifican las amenazas y se descubren las vulnerabilidades asociadas. Para cada escenario de riesgo se determina la probabilidad de ocurrencia y el impacto generado en caso de que dicho escenario de riesgo se materialice. La organización a través de su estructura de gobierno de seguridad de la información debe definir el tipo de tratamiento que se aplicará a cada escenario de riesgo, es decir, el riesgo podrá aceptar, mitigar o transferir. Para el caso de los escenarios de riesgo cuyo tratamiento es la mitigación, se deberán determinar las medidas de seguridad que permitirán reducir el riesgo por debajo del nivel aceptado por la organización. Finalmente, se deberá establecer las acciones para llevar a cabo su implementación detallando qué se hará, qué recursos serán requeridos, quién es el responsable de la implementación, cuándo se terminará y cómo serán evaluados los resultados.
4) Asignación de recursos para el soporte del SGSI. La organización debe identificar las habilidades del personal para una correcta implementación y operación del SGSI. Acciones aplicables en este rubro comprenden campañas de concientización, talleres, asesorías y cursos de capacitación. Es importante desplegar un buen sistema de comunicación interna y externa que permita coordinar eficientemente a las personas involucradas en la implementación y operación del SGSI. Otro recurso importante para la buena operación del SGSI es la correcta documentación del sistema que debe incluir la estandarización de formatos y un proceso de control documental que garantice el control de versiones y la seguridad de los documentos.

2118 ISO/IEC 27002, "Information technology – Security techniques – Code of practice for information security controls". ISO/IEC. Second edition, 2013

5) Mantenimiento adecuado de la operación. La organización debe planear, implementar y controlar procesos que garanticen la correcta operación de las medidas de seguridad del SGSI. Debido a la dinámica en el surgimiento de nuevas amenazas, vulnerabilidades y vectores de ataque, se debe realizar un análisis de riesgo a intervalos planeados.
6) Evaluación del desempeño. La organización debe monitorear y evaluar la efectividad y desempeño del SGSI. Para llevar a cabo esta tarea, la organización debe determinar:
   a. Qué se requiere monitorear y medir, incluyendo procesos y controles
   b. Métodos de monitoreo, medición, análisis y evaluación
   c. Cada cuando y quién debe realizar el monitoreo
   d. Procedimiento para realizar el análisis y la evaluación

   La organización debe conducir auditorías internas de manera periódica para proveer información sobre el nivel de conformidad del SGSI. Los altos directivos deben estar informados de los resultados de la evaluación de desempeño del SGSI para la toma de decisiones estratégicas que conduzcan a un proceso de mejora continua.
7) Ejecución de acciones de mejora continua. El resultado de la evaluación de desempeño y de las auditorías internas permite identificar no conformidades con respecto a los objetivos de seguridad establecidos en la fase de planeación. La organización debe decidir sobre las acciones a tomar y determinar si se trata de acciones menores que favorezcan la mejora continua o deben tomarse acciones correctivas que involucren grandes cambios en el SGSI.

En el caso del tratamiento de datos personales, el INAI[2119] desarrolló una guía para la implementación de un Sistema de Gestión de Seguridad de Datos Personales (GSGSDP)[2120] tomando como referencia diversos estándares internacionales de seguridad de la información. La guía propuesta se basa en un modelo por fases de mejora continua denominado "Planificar-Hacer-Verificar-Actuar" (PHVA) en donde se realizan las siguientes actividades en cada una de ellas:

a) Planificar. Se definen los objetivos, políticas, procesos y procedimientos que conforman el SGSDP con la finalidad de gestionar los riesgos relacionados con los datos personales y así cumplir con la legislación vigente sobre protección de datos personales y obtener los resultados definidos en la meta de la organización.
b) Hacer. En esta fase se implementan y operan las políticas, objetivos, procesos y procedimientos del sistema de gestión, de igual forma se despliegan los controles y mecanismos con sus indicadores de medición.
c) Verificar. Se evalúa y se revisa el cumplimiento del proceso de acuerdo con la legislación de protección de datos personales y se informa los resultados a la alta dirección para su evaluación.
d) Actuar. Se adoptan medidas correctivas y preventivas con el objetivo de lograr la mejora continua en función de los resultados obtenidos de la revisión de la alta dirección, auditorias y comparación con otras fuentes de información relevantes.

Cada fase del SGSDP está compuesta por diversos pasos que permiten la correcta implementación, operación y mantenimiento del sistema de gestión.

2119 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

2120 INAI. Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales. Junio 2015, p. 14-15. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Implementaci%C3%B3n_SGSDP(Junio2015).pdf

Fase de planeación

1) Establecer el alcance y los objetivos. Se define el alcance y se establecen los objetivos del sistema de gestión, tomando en consideración el contexto y los procesos de negocio de la organización se delimita el ámbito de aplicación del tratamiento relacionado con el flujo de los datos personales.
2) Elaborar una política de gestión de datos personales. Se emite e implementa una política de gestión y seguridad que conduzca al logro de los objetivos planteados en el paso anterior. La política debe ser aplicada a toda persona que trata datos personales y debe ser formalmente aprobada y apoyada por la alta dirección. La política debe establecer el compromiso de cumplir con las leyes vigentes en términos de protección de datos personales, por lo que debe ser comunicada a toda la organización e incluir reglas que cubran los principios establecidos en las leyes.
3) Establecer funciones y obligaciones de quienes traten datos personales. Se deben asignar privilegios y obligaciones a toda persona que trate datos personales en base al rol que desempeñan en el ciclo de vida de los datos personales.
4) Elaborar un inventario de datos personales. Los datos personales tratados por la organización deben ser identificados y clasificados según su nivel de sensibilidad, además se debe realizar una matriz de responsabilidad donde se relacione a la persona con el tipo de tratamiento para cada dato personal.
5) Realizar el análisis de riesgo de los datos personales. Permite establecer el nivel de riesgo al que están sometidos los datos personales en base a su riesgo inherente, el análisis de riesgo implica determinar el tipo de dato personal, identificar las amenazas y las vulnerabilidades asociadas y realizar la evaluación del riesgo considerando la probabilidad de ocurrencia y el impacto producido en caso de que el escenario de riesgo se materialice.
6) Identificación de las medidas de seguridad y análisis de brecha. En este paso se determinan las medidas de seguridad a implementar como resultado del análisis de riesgo desarrollado en el paso anterior. También se realiza el análisis de brecha que consiste en identificar las medidas de seguridad existente y las medidas faltantes.

Fase de implementación y operación del SGSDP

7) En este paso se ponen en operación las medidas de seguridad seleccionadas en el último paso de la fase anterior.

Fase de monitoreo y revisión del SGSDP

8) En este punto se evalúan los resultados de la implementación de las políticas, procesos y medidas de seguridad implementados, con la finalidad de verificar que se hayan alcanzado los objetivos establecidos.

Fase de mejora continua y capacitación

9) Paso consistente en implementar medidas correctivas y preventivas como resultado del monitoreo y revisión realizados en la fase anterior. La parte de capacitación se considera una acción sumamente importante dentro del proceso de mejora continua.

En el ámbito regulatorio, el artículo 34 de la LGPDPPSO[2121] establece lo siguiente en relación a un sistema de gestión de seguridad de datos personales:

> "Artículo 34. Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.
>
> Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia."

Sistema de justicia en línea

Faustino Gerardo Ezquerra Hidalgo

Plataforma tecnológica del Tribunal Federal de Justicia Administrativa que permite, entre otras cosas, la promoción, sustanciación y resolución del juicio en línea, así como la consulta de los expedientes electrónicos por las partes, autorizados, peritos y personal del propio tribunal desde cualquier computadora con acceso a internet, las 24 horas de los 365 días del año.

El anterior concepto se obtuvo en referencia a la utilización de la plataforma tecnológica del Tribunal citado, en relación con la modalidad del juicio en línea, el cual ha sido objeto de análisis en puntos precedentes, sin considerar que esta modalidad tiene objetivos y usos más amplios, como se advierte de la definición de la fracción XV de la Ley Federal de Procedimiento Contencioso Administrativo (LFPCA).[2122]

1. Delimitacion conceptual y conceptos correlacionados

Son diversos los artículos de la LFPCA que hacen referencia al sistema de justicia en línea en lo relativo a la importancia que tiene para la tramitación de un juicio en esta modalidad, por ejemplo, en el primer párrafo del artículo 58B[2123] de la LFPCA se sientan las bases para que el promovente de un juicio contencioso administrativo federal en línea y los demandados comparezcan ante el tribunal competente a deducir sus derechos por medio de esta plataforma tecnológica. Asimismo, en el artículo 58D se prevé que en el sistema de justicia en línea del tribunal se integrará el expediente electrónico, garantizándose su seguridad, inalterabilidad, autenticidad, integridad y durabilidad conforme a los lineamientos que expida el tribunal.

Por lo tanto, podemos decir que no podría existir la modalidad de juicio contencioso en línea, sin la existencia de un sistema de justicia en línea, la cual debe garantizar la seguridad, inalterabilidad, autenticidad, integridad y durabilidad de los expedientes electrónicos, ya que en casi en todos los casos se prescinde de un expediente físico.

2121 DOF. (2017, enero). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.* Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

2122 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 1-A. Para los efectos de esta Ley se entenderá por:
XV. Sistema de justicia en línea: sistema informático establecido por el Tribunal a efecto de registrar, controlar, procesar, almacenar, difundir, transmitir, gestionar, administrar y notificar el procedimiento contencioso administrativo que se sustancie ante el Tribunal.

2123 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 58-B. Cuando el demandante ejerza su derecho a presentar su demanda en línea a través del sistema de justicia en línea del Tribunal, las autoridades demandadas deberán comparecer y tramitar el juicio en la misma vía.

Por tal motivo, en el artículo 58A de la LFPCA se estipuló que el juicio contencioso administrativo federal se promovería, substanciaría y resolvería en línea, a través del Sistema de Justicia en Línea y se determinó que debería ser establecido y desarrollado por el Tribunal antes indicado, con apego a lo dispuesto en ese ordenamiento,[2124] lo cual se reiteró en el artículo segundo transitorio del decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Procedimiento Contencioso Administrativo y de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa, publicado en el *Diario Oficial de la Federación* el 12 de junio de 2009, al ordenarle al Tribunal Federal de Justicia Fiscal y Administrativa, ahora de Justicia administrativa, por parte del legislador federal, el desarrollo del sistema de justicia en línea a través del cual se sustanciaría el juicio en línea.[2125]

Antes y después de la publicación del decreto citado, los integrantes del entonces denominado Tribunal Federal de Justicia Fiscal y Administrativa, otras instancias de gobierno y prestadores de servicios realizaron múltiples acciones de orden jurídico, tecnológico y administrativo para el diseño, construcción e implementación del sistema de justicia en línea. Estas acciones se llevaron a cabo durante las gestiones y con el liderazgo de sus presidentes —el magistrado Francisco Cuevas Godínez (2008-2010) y el magistrado Juan Manuel Jiménez (2011-2013).

El propósito de estas acciones era otorgar a los ciudadanos una opción legal para promover y sustanciar juicios en línea. El decreto se publicó en el *Diario Oficial de la Federación* el 7 de agosto de 2011, no sin antes resolver varios problemas y superado una enorme resistencia dentro y fuera de la Institución.

La junta de gobierno y administración creó la comisión para la ejecución del proyecto de juicio en línea del Tribunal Federal de Justicia Fiscal y Administrativa mediante el acuerdo e/jga/13/2008. Posteriormente, cambió su denominación mediante el acuerdo e-jga-1-2011, para llamarse Comisión para la Implementación y Puesta en Operación del Sistema de Justicia en Línea. Al mismo tiempo se incorporaron varios magistrados, secretarios de acuerdos, archivistas, oficiales de partes y personal de las áreas de apoyo tecnológico y administrativo a los trabajos para la realización de dicho proyecto.

Algunas de esas acciones fueron:

A. La gestión y obtención de recursos federales y del Fondo Nacional para el Fortalecimiento y Modernización de la Impartición de Justicia (Fondo Jurica) de la Asociación Mexicana de Impartidores de Justicia (AMIJ) para el diseño, construcción e implementación del sistema de justicia en línea.

B. La realización de estudios de impacto regulatorio, impacto presupuestario, de mercado, costo-beneficio y encuestas sobre uso de tecnología a usuarios de los servicios que proporciona el Tribunal.

C. La realización de una licitación pública abierta y el proceso de invitación a por lo menos tres proveedores, para las fases de: "planeación y diseño", e "implementación y puesta en operación del sistema de justicia en línea", respectivamente, así como la contrata-

2124 Ley Federal de Procedimiento Contencioso Administrativo.
Artículo 58-A. El juicio contencioso administrativo federal se promoverá, substanciará y resolverá en línea, a través del sistema de justicia en línea que deberá establecer y desarrollar el Tribunal, en términos de lo dispuesto por el presente capitulo y las demás disposiciones específicas que resulten aplicables de esta Ley. En todo lo no previsto se aplicarán las demás disposiciones que resulten aplicables de este ordenamiento.

2125 Ley Federal de Procedimiento Contencioso Administrativo. Decreto publicado DOF el 12 de junio de 2009.
Segundo transitorio. Tribunal Federal de Justicia Fiscal y Administrativa, a la fecha de entrada en vigor del presente decreto iniciará el desarrollo e instrumentación del sistema de justicia en línea a través del cual se substanciará el juicio en línea.

ción de otros bienes y servicios complementarios conforme a la ley y la suscripción de múltiples convenios de acompañamiento por parte de la Asociación Mexicana de Impartidores de Justicia (AMIJ) y el Instituto Politécnico Nacional.

D. La adquisición, previa autorización de la Secretearía de Hacienda y Crédito Público y de la Secretaría de la Función Pública, de la plataforma tecnológica integrada por los servidores centrales y demás dispositivos de *hardware* y su respectiva instalación.

E. La contratación de un centro de cómputo externo (*data center*) de alta disponibilidad y seguridad para el alojamiento del equipo de cómputo y de comunicación, para la operación del Sistema de Justicia en Línea. Esto tiene por objeto mitigar los riesgos que existen por la probabilidad de siniestros, eventos o acción humana dolosa o imprudencial, que afecten total o parcialmente la plataforma informática del Tribunal o sus componentes.

F. La suscripción de un convenio con el servicio de administración tributaria con el objeto de la utilización de los servidores generados para la validación de certificados de firma electrónica avanzada, necesaria para la autorización de promociones, actuaciones y sentencias de los juicios en línea.

G. La elaboración de reglas de negocio, diagramas de flujo de procesos, bocetos de pantalla y plantillas, indicadores de gestión y reportes de operación que proporcionaría el sistema de justicia en línea.

H. Diseño y ejecución de un programa de administración del cambio en tres ejes: sensibilización al cambio, capacitación para usuarios internos y externos y difusión.

I. Reformas al Reglamento Interior del Tribunal y emisión de lineamientos para la operación del juicio en línea y el sistema de justicia en línea.

J. Inclusión del proyecto Juicio en Línea dentro del Plan Estratégico 2010-2020 del Tribunal. Objetivo 2. Poner en operación el juicio en línea de 2010 a 2013.

K. Implementación y puesta en operación del sistema de justicia en línea, desde el 7 de agosto de 2011 y hasta la fecha, en las salas especializadas en juicios en línea y propiedad intelectual, así como en la sala superior del ahora Tribunal Federal de Justicia Administrativa. Del 2 de mayo al 2 de septiembre de 2013 —en un proceso gradual— se desplegó dicho sistema en 12 salas de ocho regiones del país.

Todo lo anterior se consigna a detalle en la Memoria Cronológica del Sistema de Justicia en Línea[2126] del Tribunal.

En dicho documento también se da cuenta de que en la sesión del Pleno del Tribunal del 23 de abril de 2008, su entonces presidente, el magistrado Francisco Cuevas Godínez, sometió a su consideración el denominado Proyecto Juicio en Línea (E-Justicia) por virtud del cual se pretendía que la tramitación del juicio contencioso administrativo se llevara a cabo a través de internet, prescindiéndose del papel, al integrar las promociones y actuaciones jurisdiccionales en expedientes electrónicos, así como de que en dicha sesión se autorizó ese proyecto por unanimidad y de que se estableció la conveniencia de obtener la aprobación de la Asociación Mexicana de Impartidores de Justicia (AMIJ) y del Fondo Nacional para el Fortalecimiento y Modernización de la Impartición de Justicia, comúnmente llamado Fondo Jurica, para destinar recursos del propio fideicomiso, al diseño y consultoría del proyecto de juicio en línea.

Al respecto, resulta conveniente destacar que en el XVII Congreso Nacional de Magistrados, que se llevó a cabo en agosto de 2008, el magistrado Francisco Cuevas Godínez, en sesión plenaria hizo la presentación del proyecto de juicio en línea y destacó sus antecedentes, premisas, beneficios y factores de éxito. Por su parte, los magistrados participantes en las mesas de trabajo pertinentes a ese tema, arribaron sustancialmente a la conclusión de que: “es necesario, viable y debe instrumentarse a la brevedad el juicio en línea”.

2126 *Memoria Cronológica del Sistema de Justicia en Línea* fue elaborada en 2013, con derechos reservados para el Tribunal Federal de Justicia Fiscal y Administrativa, por el periodo comprendido del primero de enero de 2013 al 31 de diciembre de 2018.

En agosto del año siguiente, en el XVIII Congreso Nacional de Magistrados, se analizaron las reformas legales respectivas, así como los componentes funcionales del sistema de justicia en línea.

Como se vio en párrafos precedentes, el personal responsable del Tribunal Federal de Justicia Administrativa, para cumplir la obligación que se le encomendó a esa Institución en las disposiciones citadas, e implantar el sistema de justicia en línea para la substanciación y resolución del juicio en línea, realizó muy variadas actividades que dieron como resultado que sea una realidad y opción para los particulares y autoridades administrativas desde el 7 de agosto de 2011 y hasta la fecha. Sin embargo, los actuales responsables del gobierno de ese órgano jurisdiccional, como lo son su actual presidente, el magistrado Carlos Chaurand Arzate y los integrantes de su junta de gobierno y administración, conscientes[2127] de que la tecnología evoluciona de forma significativa en poco tiempo y de que, además de dar mantenimiento a las plataformas informáticas existentes hay que actualizarlas o en su caso renovarlas, han anunciado la consolidación de la segunda versión del sistema de justicia en línea.

En efecto, el magistrado Carlos Chaurand Arzate, desde el primer día de su gestión, el 2 de enero de 2017, al presentar los objetivos de la misma a los integrantes del Pleno de ese órgano jurisdiccional, trazó los ejes de acción que habrían de regir la actuación y desempeño de su presidencia, entre los que está, según indicó, retomar y consolidar el juicio en línea como herramienta fundamental para fortalecer la seguridad jurídica y promover la justicia expedita,[2128] y ello fue reiterado en su primer informe de gobierno.[2129]

Sistema de privacidad APEC

Jacobo Esquenazi Franco

1. Introducción

El Esquema de Privacidad de APEC (*APEC Privacy Framework*) fue creado en 2004 como parte de los trabajos del Grupo Rector para el Comercio Electrónico (*Electronic Commerce Steering Group o ECSG* por sus siglas en inglés) como el siguiente paso resultante de los trabajos del Plan de Acción para el Comercio Electrónico, aprobado en 1998 en el marco de la declaración de la reunión de Líderes de APEC realizada en Kuala Lumpur, Malasia.[2130]

El Esquema de Privacidad de APEC (EPA)[2131] surge del reconocimiento por parte de los líderes y ministros de APEC por la necesidad de contar con una serie de principios que per-

2127 Junta de Gobierno y Administración del Tribunal Federal de Justicia Administrativa en 2018.
Acuerdo SS/1/2018 de enero de 2018.
Magistrado Carlos Chaurand Arzate, presidente del Tribunal y de la Junta de Gobierno y Administración.
Magistrado de la Sala Superior, Juan Ángel Chávez Ramírez.
Magistrado de la Sala Superior, Guillermo Valls Esponda.
Magistrado de sala regional, Adalberto Gaspar Salgado Borrego.
Magistrada de sala regional, María Del Consuelo Arce Rodea.

2128 Boletín 01/2017 de 2 de enero de 2017 de la Dirección General de Comunicación Social del Tribunal Federal de Justicia Administrativa. Página *web* del Tribunal Federal de Justicia Administrativa: http://www.tfjfa.gob.mx/pdf/comunicacion_social/boletines/2017/Boletin_1.pdf/

2129 Primer informe de gobierno del presidente del Tribunal Federal de Justicia Administrativa. 11 de diciembre 2017. Página *web* del Tribunal Federal de Justicia Administrativa: http://www.tfjfa.gob.mx/pdf/comunicacion_social/discursos/2017/Informe_Anual_11-12-2017.pdf/

2130 Asia Pacific Economic Cooperation (APEC). (1998). *APEC Blueprint for Action on Electronic Commerce*. Disponible en: https://www.apec.org/Meeting-Papers/Leaders-Declarations/1998/1998_aelm/apec_blueprint_for.aspx.

2131 Asia Pacific Economic Cooperation (APEC). (2005). *APEC Privacy Framework*. Disponible en: http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf, 2005.

mitieran el libre flujo de datos personales como un elemento necesario para el desarrollo del comercio electrónico y la nueva economía, y que al mismo tiempo permitieran el desarrollo de protecciones adecuadas de la información personal en la región de Asia-Pacífico.

Estructura

El documento que contiene el EPA[2132] se estructuró con la intención de tener las definiciones o principios, junto con un comentario que sirviera, tanto para la descripción más detallada de los conceptos, como para explicar su aplicación.[2133]

2. Alcance

El EPA incluye una serie de definiciones que ayudan a determinar su alcance. Entre estas definiciones encontramos:[2134]

a) dato personal (*personal information*);

b) responsable de datos personales (*personal information controller*) e

c) información de acceso público (*publicly available information*).

El alcance también contiene una explicación sobre la aplicación del esquema. En ella se intenta reconocer que las diferencias entre las economías de la región en lo económico, social y legal hacen que se requiera de un grado de flexibilidad en la implementación de los principios contenidos en el esquema. En esencia, describe que el objetivo del esquema no es la homologación de las leyes de la región, sino que éstas contemplen el contenido de los principios, atendiendo a las diferencias entre las Economías, con el fin de que faciliten el comercio en la región.

Asimismo, el alcance hace referencia a la existencia de excepciones, incluidas las relacionadas con la soberanía nacional, seguridad nacional y pública. Sin embargo, establecen que estas excepciones deben ser limitadas y proporcionales a los objetivos que se persiguen con ellas, así como la necesidad de que sean tanto públicas como establecidas por ley.

3. Principios

El EPA contiene nueve principios que se describen a continuación:

a) Prevenir el daño (*preventing harm*): reconociendo el interés de los individuos por una expectativa legitima de privacidad, la protección de los datos personales debe diseñarse para prevenir su mal uso. Más aún, reconociendo que un daño puede resultar del mal uso de la información personal, las obligaciones específicas deben tomar en cuenta estos riesgos y las medidas para remediarlos deben ser proporcionales a la probabilidad y severidad del daño que resulte de la recolección y uso de los datos personales.

b) Aviso: los responsables de manejo de datos personales deben proveer avisos claros y accesibles sobre sus políticas y prácticas respecto al manejo de datos personales, incluyendo: a) el hecho de que se esté recolectando información personal; b) el propósito de la recolección; c) los tipos de personas u organizaciones a los que se puede compartir la información personal; d) la identidad y ubicación del responsable de los

2132 Asia Pacific Economic Cooperation (APEC). (2005). *APEC Privacy Framework*. Disponible en: http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

2133 A este esquema suele conocérsele en inglés como *facing page comentary* y es el mismo que se utiliza en los Lineamientos de Privacidad de la OCDE.

2134 Por motivos de espacio estas definiciones no se incluyen aquí, pero pueden ser consultadas en el documento original anteriormente citado.

datos personales, incluyendo como contactarlos en relación con sus prácticas y manejo de información personal; e) las opciones y medios que los responsables de los datos personales ofrecen a los individuos para que estos limiten la posibilidad de compartir y usar su información personal, así como de los medios para acceso y corrección de sus datos personales. El principio también dispone que deben seguirse todos los pasos prácticos para que el aviso pueda presentarse antes o en el momento de la recolección de los datos personales, o de lo contrario de la necesidad de que se presente tan pronto como sea práctico. Asimismo, se indica que no puede ser apropiado que los responsables de los datos personales provean de notificación cuando los datos son del dominio público.

c) Limitación de la recolección: este principio establece que la recolección de los datos personales debe limitarse a la que es relevante para sus propósitos y debe obtenerse de forma legal, justa y —cuando sea apropiado — con el aviso o consentimiento del individuo.

d) Usos de los datos personales: el principio de uso establece que la información personal recolectada debe utilizarse solamente para cumplir con el propósito de la recolección o algún propósito compatible. Sin embargo, establece tres excepciones, a) cuando se tiene el consentimiento de la persona a la que se refiere la información personal, b) cuando es necesaria para proveer de un bien o servicio solicitado por el individuo de quien se refieren los datos o c) por mandato de ley y otros instrumentos legales, decretos con efectos legales.

e) Elección (*choice*):[2135] el principio establece que "cuando sea apropiado",[2136]se debe proveer a los individuos de mecanismos para ejercer su elección en relación con la recolección, uso y comunicación (a otros) de sus datos personales. Estos mecanismos deben ser claros, prominentes, fáciles de comprender, de fácil acceso y costo. Asimismo, se establece que es posible que no sea apropiado que los responsables provean de estos mecanismos cuando los datos recolectados sean de dominio público.

f) Integridad de los datos personales: dicho principio plantea que la información personal debe ser precisa, completa y actualizada, en la medida de lo necesario para los propósitos para los que se requiera.

g) Medidas de seguridad: este principio establece que los responsables de los datos personales deben mantener medidas para salvaguardarlos ante riesgos como la perdida, el acceso, uso o modificación, comunicación o destrucción no autorizados y otros malos usos de la información personal. Estas medidas de seguridad deben ser proporcionales a la probabilidad y severidad potencial del daño, la reserva de la información y el contexto en el que esta se mantiene. Estas medidas deben ser revisadas y valoradas periódicamente.

2135 El concepto de elección, si bien es similar al del consentimiento que se utiliza en otros regímenes de privacidad alrededor del mundo, dado que los principios de APEC se crean en un entorno relacionado a las prácticas comerciales (para facilitar el comercio electrónico), se enfoca desde el punto de vista comercial o del consumidor, mientras que el concepto de consentimiento está basado en las fuentes de la protección de los datos personales como un derecho fundamental.

2136 El comentario en el documento establece que la inclusión de la frase "cuando sea apropiado" tiene la intención de establecer que existen situaciones cuando el consentimiento sea claramente implícito y que por lo tanto no fuera necesario proveer un mecanismo de elección, Asia Pacific Economic Cooperation (APEC). (2005). *APEC Privacy Framework*. Disponible en: http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf, 2005., p. 20

h) Acceso y corrección: el principio establece que los individuos pueden:
   1) obtener del responsable de los datos personales la confirmación sobre si mantiene la información personal sobre ellos;
   2) ser informados, habiendo acreditado su identidad, de la información personal que tiene el responsable:
      i. dentro de un plazo razonable;
      ii. con un cargo, si lo hubiere, que no sea excesivo;
      iii. de forma razonable y
      iv. de una forma que sea generalmente comprensible, y
   3) pugnar la precisión de la información relativa a ellos, y si es posible y apropiado, que sea rectificada, completada, enmendada o borrada.

   Asimismo, el principio establece algunas excepciones en el ejercicio de corregir la información personal, entre las que incluyen:
      i. cuando la dificultad de realizar las correcciones sea irracional o desproporcionada en relación con el riesgo a la protección de la privacidad en un caso específico;
      ii. cuando la información no pueda proporcionarse debido a un impedimento legal o de seguridad, o para proteger información comercial confidencial o
      iii. cuando la comunicación de la información, viole la privacidad de otras personas.

   El principio también estipula que si una solicitud bajo (a) o (b) una oposición bajo (c) sean denegadas, se debe proveer al individuo con las razones para ello y debe de ofrecerse un mecanismo para apelar a dicha negativa.

i) Responsabilidad demostrada (*accountability*): este principio establece que un responsable de los datos personales debe poder demostrar su cumplimiento de las medidas que habiliten el cumplimiento de los demás principios del esquema. Cuando el responsable transfiera información personal a otra persona u organización, ya sea local o internacionalmente, deberá obtener el consentimiento del individuo al que se refiere la información personal y tomar acciones para asegurar que quién la reciba la proteja de forma consistente con estos principios.

En 2015 se trabajó en una actualización del EPA que finalmente fue aprobada por los ministros de APEC en 2016. Esta actualización no modificó los principios aprobados, sino que se enfocó en robustecer el EPA al desarrollar, por medio de los comentarios, los principios de política que permitieran un balance entre la protección efectiva a la privacidad y el flujo necesario de datos para el desarrollo del comercio electrónico y la economía digital.[2137]

El esquema de privacidad de APEC contiene dos secciones adicionales. La primera es una guía de implementación para que las economías miembro de la APEC[2138] consideren aplicar estos principios en sus legislaciones o regímenes regulatorios. La segunda plantea la necesidad de desarrollar mecanismos dentro de APEC que permitan la implementación de los aspectos transfronterizos del esquema.

2137 APEC. (2016). *Updates to the APEC Privacy Framework, documento 2016/CSOM/012app17*. Disponible en: http://mddb.apec.org/Documents/2016/SOM/CSOM/16_csom_012app17.pdf

2138 A los participantes de APEC se les denomina "Economías" y no países o Estados miembros. Esto se debe a un acuerdo político en el que se decide que los trabajos se enfocan el tema económico por lo que hay una participación de "las tres chinas". Disponible en: https://www.apec.org/About-Us/About-APEC/Member-Economies

4. Implementación

La guía de implementación incluida en el esquema de privacidad de APEC contiene las siguientes secciones que se enfocan en consideraciones que las Economías de APEC deben dar para la aplicación de los principios en sus marcos regulatorios locales. Entre los temas que se incluyen permea por igual la idea del beneficio al desarrollo económico del uso y flujos internacionales de datos, como el beneficio a los ciudadanos de estas economías de la protección de sus datos personales.

La guía describe también que existe flexibilidad para que cada Economía establezca el modo en el que sus marcos regulatorios implementen estos principios. Las opciones van desde la implementación de los mismos en leyes, hasta el establecimiento de esquemas voluntarios de autoregulación. Sin embargo, se hace una mención a la necesidad de establecer prácticas de privacidad que protejan a los individuos de actitudes discriminatorias.

El esquema incluye también una descripción de los aspectos internacionales para la habilitación del esquema de privacidad de APEC. Se destaca en este caso tres áreas de colaboración: a) el intercambio de información y experiencias; b) la cooperación para el cumplimiento y facilitación de los flujos transfronterizos; c) el desarrollo cooperativo de reglas transfronterizas de protección de datos.

La sección de implementación internacional del esquema ha sido la base del desarrollo de otros mecanismos dentro de los trabajos de APEC, que se mencionan en las secciones siguientes.[2139]

A. Subgrupo de privacidad de APEC

Como resultado de la adopción del esquema de privacidad de APEC en 2005, se creó el subgrupo de protección de datos (*data privacy subgroup* o DPS por sus siglas en inglés), en el marco del ECSG.[2140] Dentro de los primeros trabajos del DPS se encuentra el establecimiento de los planes individuales de acción sobre privacidad (*information privacy individual action plans*)[2141] y el desarrollo de dos nuevos elementos descritos en el esquema de privacidad de APEC bajo la sección de implementación internacional.

En 2007 los miembros de APEC aprobaron una hoja de ruta para la implementación del esquema de privacidad. La hoja de ruta busca facilitar el desarrollo de mecanismos para generar flujos de datos transfronterizos responsables, con un enfoque en el desarrollo de reglas transfronterizas aplicables al sector privado.2142 La ruta planteada ha dado como resultado hasta ahora tres mecanismos prácticos que soportan el sistema de APEC, los cuales se describen en las secciones siguientes.

B. Acuerdo de Cumplimiento Transfronterizo de APEC

Como mencionamos, el esquema de privacidad de APEC planteaba el desarrollo de mecanismos de "cooperación para el cumplimiento y facilitación de los flujos transfronterizos". El DPS, con la participación de varias autoridades de protección de datos (APD),[2143]

2139 Por cuestiones de espacio se incluye una breve explicación de estos mecanismos.

2140 En el ESG y DPS existe una participación no solo de los gobiernos de las Economías de la región Asia-Pacífico, sino que de acuerdo con las reglas del mecanismo se cuenta con la participación de otros sectores incluyendo organizaciones de negocios, académicas y de expertos. Ver: https://www.apec.org/About-Us/How-APEC-Operates/Stakeholder-Participation

2141 Ver: APEC, 2006 Key APEC Documents, consultado en: https://www.apec.org/-/media/APEC/Publications/2006/12/Key-APEC-Documents-2006/06_apec_Keydocs.pdf pp. 16

2142 APEC, APEC Data Privacy Pathfinder (2007), consultado en: http://aimp.apec.org/Documents/2007/SOM/CSOM/07_csom_019.doc

2143 La CPEA cuenta actualmente con 27 DPA participantes. La lista completa puede consultarse en: https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

desarrolló el Acuerdo de Cumplimiento Transfronterizo de Datos de APEC (CPEA por sus siglas en inglés). Este acuerdo multilateral fue el primer mecanismo por medio del cual las APD de la región Asia-Pacífico pudieron proveerse mutuamente de asistencia para el cumplimiento de los marcos legales de privacidad y protección de datos.[2144]

El documento fundacional de la CPEA[2145] establece reglas que incluyen: a) limitantes legales a la cooperación; b) la designación y actividades de un administrador; c) reglas de incorporación o desincorporación en el acuerdo; d) deber de confidencialidad; e) intercambio de información y f) otros asuntos (que incluyen el intercambio de funcionarios y la manera de como dirimir disputas que tuvieran los DPA, entre otros temas).

C. Sistema de reglas transfronterizas de privacidad de APEC

En noviembre de 2011[2146] los líderes de APEC aprobaron el mandato para la implementación del sistema de reglas transfronterizas de APEC (conocido como CBPR por sus siglas en inglés).[2147] El CBPR se pensó como un mecanismo en el cual las políticas y prácticas de privacidad y protección de datos de las empresas de la región de APEC son revisadas y certificadas por un tercero, conocido como agente de cumplimiento (*accountability agent*). Este certificador (que a su vez es evaluado por los miembros de APEC, incluyendo ADP) hace la evaluación y certificación con base en reglas colectivamente aprobadas por los miembros de APEC y alineadas al EPA. Mediante la aplicación de estas reglas base comunes,[2148] el CBPR busca generar interoperabilidad entre los sistemas de protección de la privacidad y datos personales de las Economías de APEC, minimizando las diferencias que pudieran existir entre ellas.

Algunas de las Economías de APEC han determinado establecer límites al flujo transfronterizo de datos, exigiendo que las transferencias se realicen a países que permitan un nivel adecuado de protección. Sin embargo, han establecido como mecanismo de transferencia apropiado, que las empresas cuenten con una certificación CBPR.

D. Sistema de reconocimiento de encargados de APEC

El sistema de reconocimiento de encargados de APEC (*APEC privacy recognition for processors* o PRP por sus siglas en inglés), fue aprobado en 2015 y[2149] creado como una herramienta para que los responsables de protección de datos puedan cumplir sus obligaciones mediante la identificación de responsables de tratamiento de datos personales que cumplan con estándares de protección adecuados. El PRP al igual que el CBPR realiza la evaluación y certificación de los encargados de tratamiento de datos por medio de la evaluación realizada por agentes de cumplimiento. Esto se logra mediante el uso de un cuestionario que

2144 APEC. (2009). *APEC Cooperation Arrangement for Cross-Border Privacy Enforcement*. Disponible en: http://www.apec.org/~/media/Files/Groups/ECSG/CBPR/CBPR-CrossBorderPrivacyEnforcement.pdf

2145 La CPEA cuenta actualmente con 27 DPA participantes. La lista completa puede consultarse en: https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

2146 Declaración de Líderes de APEC, Hoolulu Hawaii, 12 de diciembre del 2011. Disponible en: https://www.apec.org/Meeting-Papers/Leaders-Declarations/2011/2011_aelm

2147 APEC. (s.f.) *APEC Cross Border Privacy Rules System: Policies, Rules and Guidelines*. Disponible en: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx

2148 El CBPR considera una serie de elementos mínimos comunes. Sin embargo no impide que las Economías impongan en sus marcos regulatorios requisitos adicionales de protección de datos que debieran ser revisados por los agentes de cumplimiento en sus respectivos territorios.

2149 APEC. (s.f.). *APEC Privacy Recognition for Processors System: Policies, Rules and Guidelines*. Disponible en: http://www.apec.org/~/media/Files/Groups/ECSG/2015/APEC%20PRP%20Rules%20and%20Guidelines.pdf

busca medir con los requisitos mínimos de cumplimiento[2150] y otorgar un reconocimiento a este cumplimiento que pueda asegurar a los responsables que están utilizando un encargado que cumple con un mínimo de obligaciones en materia de protección de datos.

E. Interoperabilidad con otros modelos de protección

En septiembre de 2012 se creó un grupo de trabajo entre la APEC y la Unión Europea (con la participación del WP29) para trabajar en la interoperabilidad entre el modelo de APEC y las Reglas de Cumplimiento Vinculante (BCR por sus siglas en inglés) de la Unión Europea (UE). Este diálogo produjo un primer documento de trabajo conocido como Referente Común para la Estructura del Sistema de la Unión Europea y el Sistema de APEC.[2151] El documento buscaba ser una guía informal para las empresas que buscan certificarse bajo CBPR y obtener sus BCR. El documento identifica los elementos comunes en ambos programas así como los requisitos adicionales existentes en cada uno de los ellos.

Los trabajos entre ambas organizaciones se suspendieron temporalmente en la segunda mitad de 2017, ya que los miembros del entonces WP29 (hoy transformado en Comité Europeo de Protección de Datos) se encontraban enfocados en la implementación del Reglamento Europeo de Protección de datos que entró en vigor en mayo del 2018. Sin embargo, se espera que el diálogo de interoperabilidad se reanude a principios de 2019.

Sistema Electrónico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (IFAI-Prodatos)

Ángel Trinidad Zaldívar y
Marina San Martín Rebolloso

IFAI Prodatos es el sistema electrónico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), mediante el cual, los interesados pueden presentar y dar seguimiento a la sustanciación de sus solicitudes de protección de derechos de las denuncias que formulen, así como de la sustanciación del procedimiento de imposición de sanciones, en el marco de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).[2152]

Se trata de una plataforma informática disponible en el sitio: https://www.datospersonales.org.mx/, que permite a los titulares de datos personales, a sus representantes legales y a los denunciantes formular requerimientos de protección de derechos y denuncias por presuntos incumplimientos a la citada LFDPPP, además de facilitar el trámite de los procedimientos relacionados.[2153]

2150 El cuestionario puede consultarse en: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/-/media/Files/Groups/ECSG/2015/APEC-PRP-Intake-Questionnaire-Final.docx

2151 APEC. (s.f.). *Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents.* Disponible en: www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf

2152 Artículo primero del acuerdo mediante el cual se aprueba la modificación del diverso acuerdo por el que se establece el sistema electrónico para la presentación de solicitudes de protección de derechos y de denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado el 28 de noviembre de 2013. (Acuerdo por el que se modifica el acuerdo del sistema electrónico para la LFPDPPP, 2018). *Diario Oficial de la Federación*, 23 de abril de 2018.

2153 Artículo 3, fracción IX de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (Lineamientos de Procedimientos 2015), *Diario Oficial de la Federación*, 9 de diciembre de 2015.

1. Antecedentes

No cabe la menor duda que la tecnología es hoy parte fundamental del ejercicio de nuestras libertades y derechos y particularmente en lo que se refiere a la transparencia y la protección de los datos personales. Esto lo entendió muy bien el legislador que, desde 2002 previó, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), que la documentación a que se podía tener acceso incluía tanto lo electrónico como lo informático[2154] y pergeñaba la necesidad de crear un sistema que permitiera realizar solicitudes y recibir las respuestas correspondientes, de ahí surge el Sistema Electrónico de Solicitudes de Información (Sisi).

Cinco años después, la reforma constitucional de 2007 ratificó la importancia de contar con un sistema electrónico que coadyuvara a garantizar el ejercicio del derecho de acceso. En el dictamen del proyecto de reformas respectivo se estableció que "la gran aportación mexicana al derecho de acceso a la información es la construcción de un sistema electrónico de solicitudes de información…no se trata solamente de un correo electrónico, sino de un sistema integral que facilita la comunicación entre el ciudadano y las autoridades, que contabiliza los plazos perentorios establecidos en la ley, que permite la entrega de información de manera expedita y sencilla y que abarata los procedimientos".[2155] Así es como el Sisi evolucionó y se convirtió en Infomex, un sistema electrónico con cobertura nacional, no solo de las instituciones del gobierno federal.

La exitosa experiencia de ese sistema electrónico, que ha seguido evolucionando hasta la plataforma actual, llevó a la conclusión de que habría que hacer algo similar para el tema de los datos personales y así es como nace IFAI Prodatos.

El INAI es la autoridad encargada de promover y proteger el ejercicio del derecho a la protección de los datos personales en posesión de los particulares y de vigilar el cumplimiento de las obligaciones por parte de los sujetos regulados por la ley específica de la materia; para ello tiene la facultad para conocer y resolver los procedimientos de protección de derechos y de verificación señalados en la LFPDPPP, así como para imponer las sanciones que corresponda.[2156]

De conformidad con el ordenamiento de protección de datos personales del sector privado y su Reglamento, las solicitudes podrán interponerse por el titular o su representante; ya sea mediante escrito libre, en los formatos que para tal efecto determine el Instituto o a través del sistema que este establezca.[2157] De acuerdo con lo anterior, corresponde al Instituto desarrollar dicha herramienta tecnológica para facilitar el desahogo de los procedimientos derivados de esta normativa.

2154 Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico. Véase Artículo 3, fracción III, de la de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), *Diario Oficial de la Federación*, 11 de junio de 2002.

2155 El artículo tercero transitorio de dicha reforma dispuso que: "La Federación, los Estados y el Distrito Federal, deberán contar con sistemas electrónicos para que cualquier persona pueda hacer uso remoto de los mecanismos de acceso a la información y de los procedimientos de revisión a los que se refiere este Decreto…" Véase la Reforma al artículo 6 constitucional que establece el acceso a la información pública como un derecho fundamental de los mexicanos, México, IFAI, 2007, p. 32 y 34.

2156 Artículos 38 y 39, fracción VI, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), *Diario Oficial de la Federación*, 5 de julio de 2010.

2157 Artículos 46 de la LFPDPPP, *Diario Oficial de la Federación*, 5 de julio de 2010; y 113 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Reglamento de la LFPDPPP), *Diario Oficial de la Federación*, 21 de diciembre de 2011.

En ese sentido, en noviembre de 2013, el entonces IFAI expidió el acuerdo por el que se establece el sistema electrónico para la presentación de solicitudes de protección de derechos y de denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, por medio del cual se estableció una plataforma informática a cargo del Instituto con el fin de que los titulares de los datos personales o sus representantes legales, y denunciantes, tuvieran la posibilidad de presentar, a través de medios electrónicos, solicitudes de protección de derechos y denuncias por presuntos incumplimientos a la LFPDPPP; así como para la sustanciación de los procedimientos que de ellas resulten.[2158]

Este sistema electrónico, creado en 2013, fue llamado IFAI Prodatos a partir de la reforma al Acuerdo referido, publicada el 23 de abril de 2018.[2159] Las modificaciones al sistema electrónico en cuestión se orientaron a precisar algunas disposiciones y en ajustar su denominación a IFAI Prodatos, de tal suerte que en los artículos transitorios, se ordenó a la Secretaría Ejecutiva a que, por conducto de la Dirección General de Tecnologías de la Información, realizara los ajustes necesarios al sistema, con el objeto de ponerlo a disposición de los presuntos infractores para que puedan contar con un registro para el desahogo y seguimiento de los procedimientos.

2. Funcionamiento

El sistema electrónico asigna un número de folio único para el seguimiento de las solicitudes de protección de derechos y una cadena de autenticidad para las denuncias por presuntos incumplimientos a la LFPDPPP, en ambos casos, se genera un acuse de recibo electrónico que acredita la fecha y hora de recepción.[2160]

La forma de identificación de los promoventes en el sistema electrónico es la firma electrónica avanzada (FIEL),[2161] la cual vincula y responsabiliza al titular o a su representante legal, de la misma forma y con los mismos efectos que la firma autógrafa en la sustanciación de los procedimientos.[2162] El Instituto podrá tener por reconocida la identidad del titular o la personalidad del representante cuando la misma ya hubiere sido acreditada ante el responsable al ejercer su derecho ARCO.[2163]

Para las solicitudes de protección de derechos y denuncias presentadas a través del Sistema de Protección de Datos Personales (IFAI Prodatos) se entenderá que éste será el medio aceptado para recibir notificaciones, salvo que se señale un medio distinto, de acuerdo con los mecanismos previstos en la LFPDPPP y en su Reglamento a este respecto.[2164]

2158 Artículo segundo, fracción V, del acuerdo por el que se establece el sistema electrónico para la presentación de solicitudes de protección de derechos y de denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. (Acuerdo por el que se establece el sistema electrónico para la LFPDPPP 2013. *Diario Oficial de la Federación*, 28 de noviembre de 2013.

2159 Artículo primero del acuerdo por el que se modifica el acuerdo del sistema electrónico para la LFPDPPP 2018.

2160 Artículo tercero del acuerdo por el que se establece el sistema electrónico para la LFPDPPP 2013.

2161 La firma electrónica avanzada (FIEL) es el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa. Véase artículo segundo, fracción IV, del acuerdo por el que se establece el sistema electrónico para la LFPDPPP 2013.

2162 Artículo 114 del Reglamento de la LFPDPPP y artículos sexto, séptimo y octavo del acuerdo por el que se establece el sistema electrónico para la LFPDPPP.

2163 Artículo 113 del Reglamento de la LFPDPPP.

2164 Artículo 114 del Reglamento de la LFPDPPP, artículo noveno del acuerdo por el que se establece el sistema electrónico

Las actuaciones que se presenten por este medio electrónico tendrán pleno efecto legal siempre que cumplan con los requisitos establecidos por la ley de la materia y su Reglamento, y deberán tomar en cuenta los días y horas considerados como hábiles.[2165]

Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (SNT)

Jorge Islas López

1. Introducción

Antes de la reforma constitucional y de la expedición de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) existía un problema de voluntad y de resistencia política: las entidades federativas evitaron, en diversas ocasiones, cumplir a cabalidad con los principios y derechos que reconocía la Constitución Política de Estados Unidos Mexicanos (CPEUM) a favor de los gobernados, sobre todo en materia de transparencia. La regulación federal fue aprovechada indebidamente por diversas legislaturas estatales, porque simplemente no estaban obligadas a legislar con el mismo espíritu de apertura y transparencia. En este sistema heterogéneo, inconsistente y asimétrico en detrimento de los derechos humanos para el acceso a la información, cada estado legisló lo que quiso y como quiso, bajo una forma de federalismo mal entendido.

En estas circunstancias, se crearon diversas leyes a modo, leyes que simularon integrar un sistema estatal para la transparencia y se creó un sistema de enormes asimetrías en la legislación, interpretación e implementación de las leyes. Esta fue la manera de limitar derechos, como el principio de máxima publicidad. A partir de la reforma constitucional del artículo 6 en materia de transparencia, se sentaron las bases para generar una nueva relación entre los diferentes órdenes de gobierno, de tal forma que por medio de un federalismo mejor coordinado y colaborativo en el acceso a la información y la transparencia, se diseñaran y ejecutaran políticas públicas en dichas materias. Las asimetrías normativas no deben preocuparnos cuando existe una ley que domina el proceso político, en este caso, cuando los congresos locales libres y plurales cumplen con su función de legislar de acuerdo con las bases y principios establecidos en la CPEUM. En principio, el Sistema Nacional de Transparencia, Acceso a la Información y Datos Personales (SNT) establecido con la promulgación de Ley General, se debe entender como la base común e institucional jurídica necesaria que revirtió las acciones legislativas o administrativas del ámbito local, los cuales no permitían consolidar el sistema de transparencia y acceso a la información de manera homogénea. En este sentido, el Sistema Nacional surge como una instancia nacional capaz de implementar "una política integral y completa en materia de transparencia y acceso a la información de alcance nacional, mediante la coordinación eficaz de la Federación, los estados y el Distrito Federal". [2166]

La LGTAIP, en la cual se establece el Sistema Nacional, permitió revertir las inconsistencias del modelo federalizado por medio de una regulación general en donde hay competencias concurrentes entre todos los órdenes y niveles de gobierno, los cuales deben observar y respetar las nuevas disposiciones en materia de derechos humanos de manera homo-

para la LFPDPPP 2013 y artículo 9 de los Lineamientos de Procedimientos 2015.

2165 Artículos cuarto y quinto del acuerdo por el que se establece el sistema electrónico para la LFPDPPP 2013 y artículo 18 de los Lineamientos de Procedimientos 2015.

2166 "Exposición de Motivos". *Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública*. México, 2014, p. 8.

génea, en particular el del derecho a la información pública.[2167] En este orden de ideas, el Sistema Nacional es uno de los principales avances en materia de derecho a la información pública y transparencia debido a la novedad que supuso dentro de la LGTAIP. El STN es la válvula institucional que permite tener un mismo sistema de reglas simétricas para proteger un derecho humano fundamental en igualdad de condiciones y circunstancias. Las disposiciones normativas previas, en materia de acceso a la información y protección de datos, no contemplaban un entramado institucional que ordenará y posibilitará la regulación y vigilancia uniforme y simétrica de los derechos ya mencionados. La idea de integrar y armonizar los derechos de transparencia, acceso a la información y protección de datos personales en un sistema es con el fin de crear un arreglo institucional consistente y equivalente para todos los sujetos obligados para que así su cumplimiento sea igualmente universalmente observado, aplicado e implementado en toda la República Mexicana.

2. Definición

El Sistema Nacional es una instancia nacional conformada por todo el conjunto de organismos que están obligados por ley con el ejercicio de la transparencia y del derecho de acceso a la información, lo que también incluye los procedimientos, instrumentos y políticas que se desarrollan armónicamente en función de este fin. En este rubro, el Sistema Nacional está formado por mecanismos y herramientas de los tres órdenes de gobierno que articulan políticas de transparencia. A este respecto, la CPEUM es muy clara en su artículo 6, apartado A, al señalar que el Sistema Nacional no solo transparenta la información, sino que también fortalece la rendición de cuentas del Estado mexicano. Lo anterior, se reitera en la exposición de motivos de la Ley General en la cual se prevé que el Sistema Nacional diseñe, ejecute y evalué un Programa Nacional de Transparencia y Acceso a la Información Pública, lo cual constituye un instrumento rector para la integración y las metas que deberá cumplir el sistema.[2168]

3. Características y beneficios

Por medio de la coordinación institucional entre las distintas instancias de los tres órdenes de gobierno, el SNT puede cumplir sus objetivos previstos en el artículo 29 de la Ley General para: generar información de calidad[2169] por medio de un esquema de gestión de la información, con requisitos y criterios homogéneos, haciendo la información accesible y comprensible y así contribuir a su evaluación por parte de la ciudadanía, promover el ejercicio del derecho de acceso a la información, construyendo una cultura de transparencia entre servidores públicos y ciudadanos, y ayudar en la rendición de cuentas, por medio de la fiscalización, vigilancia y control de las entidades gubernamentales.

El diseño institucional del Sistema se compone de un "conjunto orgánico y articulado de instancias, instrumentos, políticas, procedimientos, principios, normas, acciones y servicios"[2170] que establece corresponsabilidades y competencias coordinadas entre los dife-

2167 Este nuevo modelo obliga a todas las autoridades a observar una base legal común que reconoce las disposiciones y obligaciones en materia de derecho a la información, sin embargo, este piso normativo de reglas mínimas no impide que, en el ámbito de sus propias facultades y competencias, las entidades federativas, así como el gobierno de la Ciudad de México, puedan legislar sus propias normas tomando en cuenta su realidad social.

2168 INAI. (2014). Del Sistema Nacional de Transparencia: como instrumento para una política nacional en la materia. Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. México, p. 8.

2169 La información de calidad se debe de entender como "veraz, confiable, oportuna, congruente, integral, actualizada, accesible, comprensible y verificable" a través de criterios estandarizados. INAI. (2014). *Exposición de Motivos. Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública.* México, p. 9.

2170 INAI. (2014). *Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública. México,* p. 9.

rentes niveles gubernamentales para lograr la asistencia, colaboración, fomento, difusión, estructuración y aplicación en materia de transparencia y acceso a la información que la Ley General propone. En sentido estricto, el Sistema Nacional se integra orgánicamente por el INAI, los organismos garantes de las entidades federativas, la Auditoría Superior de la Federación, el Archivo General de la Nación y el Instituto Nacional de Estadística y Geografía. (Ley General de Transparencia y Acceso a la Información, artículo 30).

La integración del Sistema Nacional responde a dos objetivos:

a) la vinculación de la Federación con los estados y la Ciudad de México por medio de autoridades de transparencia y

b) el fortalecimiento del sistema de rendición de cuentas a través de organismos garantes de transparencia y de organismos con facultades administrativas respecto a los archivos públicos y la fiscalización de los recursos gubernamentales, así como la sistematización de los datos estadísticos.[2171] Asimismo, hay una afortunada convergencia y concurrencia de atracciones entre los diferentes órdenes de gobierno que hacen factible su cumplimiento.

4. Interpretación literal de la Ley

A. Funciones y reglamentación del Sistema Nacional

Sobre las diversas funciones del Sistema Nacional, el legislador estableció 15 funciones que tiene encomendadas el organismo. Al respecto, en la *Ley General de Transparencia y Acceso a la Información Pública, comentada*,[2172] Jaqueline Peschard realizó una clasificación de las mismas y las agrupó en tres categorías:

1) las funciones normativas;

2) las de desarrollo de políticas de transparencia y

3) las de promoción del ejercicio del derecho de acceso a la información.

Se retomará dicha clasificación por su claridad conceptual y organización categórica. Sin embargo, no coincido con la autora respecto a la clasificación de la fracción IV del artículo 31 de la LGTAIP, debido a que encuadra con las características de las funciones normativas (primera categoría a analizar), en contraposición con la categoría de desarrollo de políticas de transparencia, que Peschard identificó.

a) Funciones reglamentarias y normativas

En la primera categoría, referente a las funciones reglamentarias, podemos clasificar las fracciones I, IV, V, VI y XI del artículo 31 de la citada Ley. Por ello, las funciones reglamentarias y normativas engloban todas aquellas tareas del SNT relativas a la elaboración de disposiciones normativas y prácticas institucionalizadas. De esta forma, el Sistema Nacional debe elaborar lineamientos, objetivos, instrumentos, estrategias, modelos integrales y evaluables y códigos de buenas prácticas (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción I). La obligación del SNT de coadyuvar la elaboración y difusión de los distintos criterios de conservación y sistematización de los archivos de los sujetos obligados permite a la población localizar, de forma eficiente, la

2171 El objetivo doble se desprende del artículo 6, apartado A, fracción VIII de la Constitución el cual le otorga facultades al organismo garante nacional (el INAI) para coordinar los esfuerzos de los otros entes estatales para lograr el cometido de fortalecer el sistema nacional de rendición de cuentas.

2172 Peschard, J. (2017) "Comentario al artículo 31. El Sistema Nacional tiene como funciones", en Jorge Islas (coord.). *Ley General de Transparencia y Acceso a La Información Pública*, Comentada. INAI, pp. 133-135.

información pública, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción V). La ampliación del universo a regular de sujetos obligados en la Ley General es una de las innovaciones más importantes de esta ley, debido a que incluyó a todos los poderes públicos del Estado, partidos políticos, sindicatos y en general, a toda persona física y moral que reciba y ejerza recursos públicos o bien, ejerza actos de autoridad en la diferentes instancias y niveles de gobierno.[2173]

Asimismo, es deber de este organismo establecer los lineamientos necesarios para implementar la plataforma nacional de transparencia. A través de estos criterios o reglas de operación específicas se puede dar certidumbre a los particulares y a los sujetos obligados, de tal forma que la accesibilidad a la información se vuelve esencial, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción VI). Lo anterior se complementa con la obligación del organismo de emitir acuerdos y resoluciones generales relativos a su funcionamiento, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción XI). Por medio de estas reglas específicas se da consistencia y fluidez al Sistema Nacional.[2174]

De esta forma, por medio de criterios comunes se pueden comparar razonablemente los rendimientos de los distintos sujetos obligados, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción IV). En el desarrollo de los criterios mencionados, participa, al menos, un representante del Consejo Nacional de Armonización Contable, de acuerdo con el artículo 6 de la Ley General de Contabilidad Gubernamental. Dicho representante tiene derecho a voz y puede presentar observaciones por escrito de esos criterios, mismos que no tienen carácter obligatorio, pero serán considerados. Es el Consejo Nacional el que se encarga de aprobar estos criterios y es también el que los hace vinculantes para todos los sujetos obligados. En este sentido, el Sistema Nacional solo tiene la función de publicar estos criterios para el desarrollo de los indicadores, pero no es el encargado de establecerlos ni de aprobarlos. Lo anterior se debe a que el Sistema Nacional es un mecanismo interinstitucional y transversal que está diseñado para integrar y cohesionar diversas instancias del poder público con causas comunes en las que se pueden sumar esfuerzos para hacer un bloque conjunto y no fragmentado para que logré luchar por la transparencia y acceso a la información pública, y contra la corrupción.

b) Funciones de políticas de transparencia

La segunda categoría, referente al desarrollo de políticas públicas, comprende las fracciones I, III, VII, VIII, X, XII. Dicha clasificación resalta la función del SNT como desarrollador de acciones, programas y guías de alcance nacional, para así lograr que todas las personas gocen de información pública transparente, un acceso efectivo a la misma y una verdadera protección de sus datos personales. Por la forma en que fue ensamblado el sistema, se concibió como una nueva instancia del Estado que tiene como finalidad mejorar la creación e implementación de políticas públicas para fortalecer los derechos de acceso a la información y también para luchar contra la corrupción.

De esta manera, una de las funciones del Sistema Nacional es la de promover e implementar acciones para garantizar condiciones de accesibilidad a los grupos vulnerables, para que

2173 En el artículo 3 de la Ley Modelo Interamericana sobre Acceso a la Información se establecen exactamente los mismos criterios con los mismos sujetos obligados. OEA. (2010). *Ley Modelo Interamericana sobre Acceso a la Información*. Disponible en: https://www.oas.org/dil/esp/CP-CAJP-2840-10_Corr1_esp.pdf

2174 Otra de las funciones del Sistema Nacional es la de establecer criterios para la publicación de los indicadores de cumplimiento de los sujetos obligados, para que estos rindan cuentas del cumplimiento de sus objetivos y resultados obtenidos.

estos tengan acceso a la información pública en igualdad de condiciones, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción II). Si el ciudadano no tiene un conocimiento mínimo de los alcances y beneficios que otorgan estos derechos, en especial cuando hablamos de grupos vulnerables, su toma de decisiones se verá limitada, de tal forma que sin decisiones de calidad, no se pueden tomar determinaciones que posibiliten mejores condiciones de vida en los ámbitos personal, familiar y social.

En la misma línea y en un sentido más amplio, la obligación primordial del SNT es construir políticas nacionales que promuevan la transparencia, acceso a la información y la protección de datos personales, que se dan a través del desarrollo de los programas comunes de alcance nacional que promocionan, investigan, diagnostican y difunden estas materias, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción III). La anterior función tiene su expresión en la obligación del SNT de aprobar, ejecutar y evaluar el Programa Nacional de Transparencia y Acceso a la Información Pública, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción XII). En este programa se establecen las propuestas de los cinco integrantes para así darle movilidad y coherencia a sus objetivos. Estos parámetros mínimos de promoción y difusión de contenidos de información y acciones institucionales permiten a los ciudadanos tener más conciencia sobre la relevancia de estos derechos en el corto plazo, así como la creación de una nueva cultura de derecho a la información a largo plazo.

Asimismo, dentro de esta clasificación se encuentra la función del SNT de establecer políticas para impulsar la digitalización de la información en posesión de los sujetos obligados, así como para utilizar las tecnologías de información e implementar ajustes razonables que garanticen su acceso, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción VII). Para ello, el Sistema Nacional diseña e implementa políticas en materia de generación, actualización, organización, clasificación, publicación y accesibilidad de la información pública, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción VIII). Por último, en esta clasificación se encuentra la función de establecer programas de profesionalización, actualización y capacitación de los servidores públicos e integrantes de los sujetos obligados en estas materias, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción X). Esta función es necesaria pues respeta la interacción que tienen las áreas especializadas de los sujetos obligados con los órganos garantes para fortalecer la transparencia del servicio público hacia los particulares y los recursos de revisión.

c) Promoción del ejercicio del derecho al acceso a la información

En la tercera categoría, que es promover el ejercicio del derecho al acceso a la información, se encuentran las fracciones IX, XIII y XIV. En sentido estricto, este rubro expresa, en la fracción XIII del artículo 31, la tarea del Sistema Nacional de promover el ejercicio del derecho de acceso a la información en toda la República mexicana. Vinculado a esta función se encuentra la de promover la coordinación de todas las instancias que integran el SNT, lo cual ayuda a dar forma a las políticas y programas orientados a impulsar el conocimiento de la utilidad y los beneficios del acceso a la información en toda la República mexicana, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción XIII). En el mismo sentido, estas obligaciones pueden realizarse con el apoyo de la participación ciudadana, por ello el Sistema Nacional debe emitir acuerdos y resoluciones generales para lograr dicho objetivo, (Ley General de Transparencia y Acceso a la Información Pública, artículo 31, fracción IX). Al propiciar la participación ciudadana se

cumple con un propósito fundamental para generar mayor conciencia y responsabilidad de los ciudadanos respecto a los temas de orden público, ya que son actos que contribuyen a fortalecer a la democracia como una aspiración colectiva y como expresión de la voluntad general que concurre a la toma de decisiones con información, elemento esencial y el que se delibera y toma decisiones en el orden público.

B. Responsabilidades del Sistema Nacional

Uno de los deberes primordiales del Sistema Nacional es el de mantener en buen funcionamiento la plataforma nacional de transparencia. Por ende, en concordancia con el artículo 52 de la Ley General, es deber del Sistema establecer las medidas necesarias para garantizar la estabilidad y seguridad de la plataforma y así asegurar que sus servicios informáticos estén en funcionamiento de manera permanente. En este sentido, los individuos no deben encontrar obstáculo alguno al consultar la información deseada ya que de lo contrario se provoca incertidumbre en la población acerca de la transparencia de los organismos públicos y la distribución de recursos. El legislador acertó al obligar al SNT a homologar sus procesos y la simplicidad del uso de los sistemas, de tal forma que la plataforma nacional de transparencia sea más accesible a los usuarios.

Es obligación de los organismos garantes desarrollar políticas de transparencia proactiva, de acuerdo con el artículo 56 de la Ley General. Es por ello que estas políticas deben de ajustarse a los lineamientos del Sistema Nacional. Estas políticas de transparencia deben de estar basadas en las demandas de los ciudadanos, ya que toda política de difusión y socialización de la transparencia y acceso a la información debe realizarse con base en las condiciones sociales, económicas y culturales de cada región. Lo que para una región es importante es posible que para otras no tenga el mismo apremio ni impacto. De tal manera, la Ley General ofrece flexibilidad para que cada órgano garante impulse agendas de difusión y promoción con base en sus propios contextos y necesidades. A la luz de los intereses de la sociedad, el Sistema Nacional identifica, a través de ciertas metodologías, las políticas necesarias para incentivar a los sujetos obligados a publicar información adicional a la que establece la Ley en un afán de ofrecer un gobierno abierto, así como la idea de promover la reutilización de la información que generan los sujetos obligados. Esta política de transparencia proactiva es evaluada por los criterios que establece el mismo organismo, (Ley General de Transparencia y Acceso a la Información Pública, artículo 58).

La importancia que tiene la transparencia y el derecho de acceso a la información para el ejercicio de otros derechos sustantivos, como lo es la participación ciudadana,[2175] radica en que solo por medio del correcto ejercicio de estos derechos se puede formar una ciudadanía más informada y consciente de los asuntos públicos. De esta manera, los ciudadanos pueden conocer las actividades que los gobernantes realizan con los recursos públicos, así como los resultados que ofrecen en el cumplimiento de sus responsabilidades.

La regulación y articulación del Sistema Nacional como mecanismo gubernamental garante de la transparencia, protección de datos personales y acceso a la información pública es retomada en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (Ley General de Protección). El derecho a la protección de los datos personales, que es en el cual se aboca el citado instrumento normativo, tiene su fundamentación constitucional en el artículo 6 que asegura la protección de los datos personales de los

2175 La acción en la que los ciudadanos ejercemos nuestro derecho de autodeterminación política para votar o ser votados, para asociarnos libremente en la formación pacífica de los asuntos públicos, para ejercer el derecho de petición, para presentar iniciativas de leyes ciudadanas o bien para aprobar o rechazar una consulta pública que sea puesta a nuestra consideración.

individuos. La Ley General de Protección refuerza lo concertado en la LGTAIP, al estipular que la competencia en materia de datos personales es concurrente tanto al orden federal como al estatal. En sentido estricto, cuando hace referencia al Sistema Nacional, lo estipula como el órgano gubernamental que tiene como función hacer transversal la protección de datos personales, así como la armonización, regulación y estimación de todas las acciones que deban aplicarse en la materia, (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, artículo 10).

Además de las facultades y competencias que la Ley General le asigna al Sistema Nacional, también tiene la encomienda de diseñar, ejecutar y evaluar de forma pertinente un Programa Nacional de Protección de Datos Personales. Este programa, de acuerdo con el artículo 14 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, debe promover el ejercicio de los derechos de transparencia y protección de datos. Asimismo, debe encargarse de proponer y crear manuales de buenas prácticas en la materia en cuestión, entre otras funciones encaminadas a la tutela y promoción del derecho a la protección de datos personales.

5. Jurisprudencia y convencionalidad

En lo que respecta a los criterios emitidos por el Poder Judicial de la Federación, no existe en la actualidad criterio alguno respecto al Sistema Nacional. No obstante, hay criterios respecto al papel de la información confidencial y su relación con el derecho de acceso a la información pública. En este sentido, el artículo 116 de la LGTAIP establece explícitamente lo que significa información confidencial[2176] en contraposición al concepto de información pública. En conformidad con lo anterior, la tesis aislada I.4o.A.693 A[2177] establece que se considera información reservada aquella que tiene el carácter de secreto industrial por lo que no se considera que se viola el derecho a la información tutelado en el artículo 6 de la CPEUM, debido a que este derecho no es irrestricto. En el mismo sentido, la tesis aislada XXX.1o.3K[2178] reitera dicho criterio al establecer que para acceder a la información contenida en los expedientes judiciales que se consideran "confidenciales" solo es posible por medio de una resolución judicial. Por otro lado, repite que el ejercicio del derecho a la información no es irrestricto, y se refiere a los casos de excepción establecidos en las leyes. De lo anterior se entiende que el Poder Judicial ha expresado la importancia del secreto o información confidencial en la legislación mexicana, así como su papel en la protección de datos personales de terceros.

Si bien es cierto que no hay democracia sin información pública, tampoco lo hay cuando es violentada la secrecía y reserva que protege la ley en casos específicos. El concepto de secreto da un giro cuando se recurre a la jurisprudencia interamericana. En este rubro, en el Caso "Gomes Lund y otros (Guerrillha do Araguai) vs. Brasil"[2179] la Corte Interamericana de

2176 "La que contiene datos personales concernientes a una persona identificada o identificable". Asimismo, considera que los secretos bancarios, fiduciarios, industriales, comerciales, fiscales, bursátiles y postales, cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando esto no involucra el ejercicio de recursos públicos. Por último, también establece la Ley General que se considera información pública "aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello (...)" Segob. (2015). *Ley General de Transparencia y Acceso a la Información Pública*, artículo 116. México. Disponible en: http://www.dof.gob.mx/avisos/2493/SG_090516/SG_090516.html

2177 Tesis: I.4o.A.693 A, *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo XXXI, enero de 2010.

2178 Tesis: XXX.1o.3K, *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo XXXII, agosto de 2010.

2179 Corte IDH. (2010). Caso "Gomes Lund y otros (Guerrillha do Araguai) vs. Brasil". Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 24 de noviembre de 2010. Serie C. No. 219, párrafo 229.

Derechos Humanos (Corte IDH) ha insistido en que el derecho de acceder a la información pública no es un derecho absoluto por lo que puede estar sujeto a restricciones, mismas que deben estar previamente fijadas en la ley (en sentido formal y materia) para así asegurar que no quede al arbitrio de la autoridad la decisión. Asimismo, estas restricciones deben asegurar el respeto a los derechos o a la reputación de los demás. Si bien, este criterio es igual a lo establecido en la jurisprudencia nacional, se debe resaltar que en el mismo caso se establece que la carga de la prueba referente a la imposibilidad de revelar la información le corresponde al Estado, por lo cual debe de motivar y fundamentar la denegatoria de información. Ante la duda o vació legal de esta justificación siempre prima el derecho de acceso a la información. Asimismo, lo dicho por la Corte IDH respecto de que en casos de violaciones a derechos humanos las autoridades no pueden recurrir a mecanismos como el secreto de Estado o confidencialidad de la información.[2180]

6. Conclusión

De esta manera, el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales se presenta como el órgano nacional que pugna por hacer transversal la aplicación de la transparencia como eje rector de la actuación institucional y gubernamental en México. Busca la articulación de actores institucionales (de todos los niveles) y externos para la protección, promoción, difusión y salvaguardia de los derechos al acceso a la información y protección de datos. Promueve la construcción de un Estado garante de estos derechos que inhiba la corrupción y que tenga mecanismos institucionalizados para asegurar que los ciudadanos consulten información de interés público. En este sentido, abona al proceso de democratización en México, al sustentar y garantizar que los individuos tengan una herramienta para fiscalizar y para exigir la rendición de cuentas en cuanto a la gestión pública. Al promover herramientas efectivas y de fácil disposición que permitan el acceso a la información relevante del aparato estatal mexicano, se transparenta la actuación gubernamental y con ello, su responsabilidad frente a la ley y la sociedad. Lo anterior son mecanismos indispensables para controlar el poder arbitrario y para fomentar una nueva cultura en favor de la legalidad, la civilidad y la democracia.

Sistema de privacidad y protección de datos personales en Estados Unidos de América (modelo estadounidense)

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El entorno regulatorio de protección de datos personales y privacidad en Estados Unidos de América (EUA) es de carácter sectorial y no general (a diferencia de lo que sucede en Europa o en México). Esto quiere decir que en EUA no existe una ley homogénea y de carácter general que reglamente los derechos de privacidad y/o protección de datos personales a nivel federal, pues en dicho territorio lo que encontramos son leyes de carácter sectorial que reglamentan la privacidad en específicos sectores de actividad, sin olvidar que las buenas prácticas para industrias y sectores son también un referente importante en estas actividades.

2180 Corte IDH. (2010). Caso "Gomes Lund y otros (Guerrillha do Araguai) vs. Brasil". Excepciones preliminares, fondo, reparaciones y costas. Sentencia del 24 de noviembre de 2010. Serie C. No. 219, párrafo 230.

Otra diferencia importante es que en EUA el derecho de protección de datos personales no es considerado como un derecho fundamental[2181] —como sucede en Europa y países como Argentina, Colombia, Chile, México, Perú y Uruguay, entre otros—, sino que es un derecho de los consumidores, cuya tutela la ostentan organizaciones administrativas como la Comisión Federal de Comercio (*Federal Trade Commission)*, el Departamento de Transporte, o distintas autoridades locales, y no existe una autoridad de control única y homogénea.[2182]

EUA es un abanico de leyes y regulaciones sectoriales de carácter federal y local, donde, por ejemplo, los titulares no cuentan con un catálogo de derechos definido (como los tradicionales derechos ARCO), aplicables para cualquier tratamiento en general. Adicionalmente, varias agencias gubernamentales y grupos industriales han expedido diversos lineamientos, directrices y recomendaciones de carácter no obligatorio, pero que se consideran buenas prácticas en la materia. Lo anterior significa que las áreas de actividad en las que se aplica la privacidad se regulan de manera diferenciada, en ocasiones traslapándose o dejando lagunas para ciertos tratamientos de datos personales.

De esta forma, entre las leyes más relevantes a nivel federal podemos citar, sin ánimo de exhaustividad, las siguientes:

a) Ley de la Comisión Federal de Comercio (*Federal Trade Commission Act)*[2183]
b) Ley Federal de Modernización de los Servicios Financieros *(Gramm-Leach-Bliley Act)*
c) Ley de Transferibilidad y Responsabilidad del Seguro de Salud *(Health Insurance Portability and Accountability Act)*
d) Ley de Informes de Crédito Justos (*Fair Credit Reporting Act*)
e) Ley Federal de Transacciones Crediticias Justas y Exactas *(Fair and Accurate Credit Transactions Act*)
f) Ley de Privacidad de las Comunicaciones Electrónicas (*Electronic Communications and Privacy Act*)
g) Ley de Fraude y Abuso Informático (*Computer Fraud and Abuse Act*)
h) Ley para la Protección a la Privacidad de los Conductores *(Driver's Privacy Protection Act)*
i) Ley para la Protección de la Privacidad de los Niños en Línea *(Children's Online Privacy Protection Act)*
j) Ley para la Protección de la Privacidad en Video *(Video Privacy Protection Act)*

En el nivel local, por un lado, cabe señalar que:

1. Todos los estados cuentan con leyes específicas de notificación de vulneraciones de seguridad muy detalladas. Esto indica que la protección en EUA se enfoca más en la seguridad (además de la protección al consumidor y no al ciudadano) que en la privacidad en su conjunto. Si bien es cierto que no puede haber privacidad sin seguridad, también lo es que hay muchas más consideraciones a tener en cuenta dentro de una legislación en privacidad que solo el cumplimiento al imprescindible deber de seguridad.

2181 Para comprender el alcance de este derecho sugerimos consultar la definición de "protección de datos personales", en este *Diccionario de Protección de Datos Personales*.

2182 Recomendamos consultar la definición de "autoridad de control", en este *Diccionario de Protección de Datos Personales*.

2183 En el tema de privacidad esta Ley es relevante debido a que crea a la Comisión Federal de Comercio (*Federal Trade Commission)* (FTC) y la habilita para regular a las compañías e individuos que realizan sus negocios en el territorio de EE.UU., con la excepción de ciertas empresas financieras, de telecomunicaciones y de transporte. En general, la FTCA protege al consumidor, prohibiendo las prácticas y acciones empresariales engañosas e injustas.

2. En concreto, el estado de California sobresale por su regulación garantista y comprehensiva, en contraposición a la protección sectorial y segregada que hemos venido explicando. Actualmente, en California se encuentran vigentes las siguientes leyes:
   a) Ley de California para la Protección de la Privacidad en Línea *(California Online Privacy Protection Act)*
   b) Ley de California de Notificaciones por Brechas de Seguridad *(California Security Breach Notification Law)*
   c) La reciente Ley sobre Privacidad de Consumidores (Assembly Bill No. 375)m que tiene por objeto establecer controles y medidas para el tratamiento de los datos personales en el estado de California, para evitar el uso indebido de datos personales y salvaguardar los derechos de los consumidores de conformidad con lo previsto por la constitución de California[2184] y que entrará en vigor el 1 de enero de 2020.[2185]

Como apunte final, dadas las ineludibles implicaciones globales de la protección de datos personales, derivadas específicamente de las comunicaciones entre terceros Estados, y en particular con aquellos que forman parte de la Unión Europea (UE) por haber sido uno de los temas que más polémica ha generado, consideramos necesario analizar brevemente este tema.

Para las comunicaciones internacionales de datos se dispone de diversas herramientas, tales como cláusulas contractuales, normas corporativas vinculantes y, especialmente en este caso, el instrumento internacional denominado escudo de privacidad.

El Escudo de Privacidad sustituye al régimen instaurado por la decisión 2000/520/CE (régimen Safe Harbor o Puerto Seguro)[2186] y que fue abrogado como resultado de la sentencia C-362/14[2187] pronunciada por el Tribunal de Justicia de la Unión Europea.[2188]

2184 *Vid*, California legislative information. (2018, junio 29). *Assembly Bill No. 375*. Disponible en: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Fecha de consulta: 29 de octubre de 2018.

2185 En relación con el citado instrumento normativo es importante tomar en cuenta que se trata de una norma que establece condiciones y obligaciones rigurosas para el tratamiento de datos personales (incluso comparables a las previstas en el Reglamento General de Protección de Datos Europeo) como las siguientes:
se considera dato personal a la información que identifica, refiere, describe, es susceptible de ser asociada con, o que razonablemente podría estar relacionado, directa o indirectamente, con un consumidor (titular) o un hogar particular.
Se considera como finalidad del negocio al uso de datos personales que la empresa (responsable) con fines operativos de un proveedor de servicios, u otros fines notificados, siempre que el uso de estos datos sea razonablemente necesario y proporcionales para lograr el propósito operativo para el que los datos personales fueron recopilados o procesados por parte de la empresa.
Otorga a los titulares diversos derechos sobre su información personal: acceso, cancelación, portabilidad y oposición.
Autoriza a los responsables para que puedan ofrecer incentivos financieros para la recopilación de datos personales de los consumidores.
Prohíbe a las empresas vender los datos personales de un consumidor menor de 16 años, a menos que su representante legal lo autorice expresamente.
Prevé que las empresas que recopilen datos personales en el estado de California además de cumplir con la citada Ley deberán cumplir con las leyes federales, estatales o locales aplicables.

2186 La Decisión 2000/520/CE o Acuerdo Safe Harbor en materia de privacidad hace referencia a un proceso de cooperación en virtud del cual las organizaciones de EUA cumplen con la Directiva 94/46/CE relativa a la protección de datos personales. En síntesis, las disposiciones de Safe Harbor facultaban a las empresas estadounidenses a recabar datos responsabilidad de responsables establecidos en Europa y transferirlos a sus servidores sin tener que someterlos a las directrices de privacidad de la UE, mucho más estrictas que las de EUA, pues las reglas dentro de la UE impiden la comunicación de datos personales a terceros Estados que no garanticen un nivel de protección adecuado en términos de la directiva en materia de protección de datos personales.

2187 Resolución C-362/14 del Tribunal de Justicia de la Unión Europea. Disponible en: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dd65b559c5377d478bb481978c382e356b.e34KaxiLc3qMb40Rch0SaxuRbxb0?text=&docid=169195&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=573847

2188 La sentencia C-362/14 pronunciada por el TJUE tiene como antecedente la denuncia interpuesta por el ciudadano austriaco Maximilan Schrems ante el comisionado de protección de datos de Irlanda en contra de Facebook. Schrems, que era usuario de la red social desde 2008, con motivo de las revelaciones realizadas en 2013 por Edward Snowden sobre la red de vigilancia mundial organizada por la National Security Agency (NSA) en colaboración con la CIA, presentó una denuncia ante la autoridad de datos personales de su país por considerar que la normatividad estadounidense y las

De acuerdo con la Comisión Europea, el escudo de privacidad permite que los datos personales se transfieran de una empresa de la UE a otra de los EUA, únicamente si dicha empresa procesa (es decir, usa, almacena y/o transfiere posteriormente) los datos personales con arreglo a una serie de normas de protección y salvaguardias bien definidas.[2189]

A diferencia de su predecesor, el escudo de privacidad ofrece una serie de derechos y obliga a las empresas a proteger los datos personales acorde con los principios de privacidad.[2190]

Situación de emergencia

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La situación de emergencia es relevante en la normatividad de datos personales porque dicha circunstancia tiene consecuencias jurídicas concretas respecto del tratamiento de los datos personales de los titulares.

En particular, la normatividad especifica escenarios en los que una situación de emergencia será una excepción al consentimiento requerido para el tratamiento, sirviendo como base de legitimación del mismo, y en consecuencia.

En este sentido, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en la fracción V del artículo 10 establece que el tratamiento de los datos personales del titular podrá llevarse a cabo sin el consentimiento de este último cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.[2191]

Asimismo, en el ámbito público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) replica la regla prevista en la LFPDPPP al establecer, en la fracción VI de su artículo 22, que el consentimiento del tratamiento de los datos personales no será requerido cuando se actualice una situación de emergencia.[2192]

La situación de emergencia también se menciona en el artículo 79 de la LGPDPPSO que excepciona a los sujetos de derecho público de realizar la evaluación de impacto en la protección de datos en situaciones de emergencia o urgencia.[2193]

Así, desde la perspectiva de la protección de datos personales, la situación de emergencia se presenta como un fundamento para el tratamiento de los datos personales para hacer frente a contingencias que podrían afectar el bienestar y seguridad de las personas a una gran escala (epidemias, desastres naturales, terrorismo y pandemias) o en un nivel individual (violencia familiar), pues en caso de que dicho tratamiento se sujete a mecanismos como el consentimiento y no se cuente con este último, las consecuencias de no facilitar la

prácticas actuales de sus autoridades administrativas no garantizaban una protección suficiente a los datos de carácter personal transferidos a EUA frente a las actividades de vigilancia realizadas por las autoridades estadounidenses.

2189 Comisión Europea. (2016). *Guía acerca del Escudo de Privacidad UE-EE. UU*. Unión Europea. Disponible en: https://www.aepd.es/media/guias/guia-acerca-del-escudo-de-privacidad.pdf. Fecha de consulta: 15 de noviembre de 2018.

2190 Comisión Europea. (2016). *Guía acerca del Escudo de Privacidad UE-EE. UU*. Unión Europea.

2191 Artículo 10, fracción V de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

2192 Artículo 22, fracción VI de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

2193 Artículo 79. Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la evaluación de impacto en la protección de datos personales.

información personal necesaria en situaciones de emergencia pueden ser funestas, ya que en un contexto de esta naturaleza el acceso oportuno a la información es fundamental para atender las contingencias y proteger los derechos de los titulares y/o de terceras personas.

Finalmente, debe destacarse que, en este sentido, si bien la normatividad aplicable provee reglas para el tratamiento de los datos, ésta no necesariamente debe ser concebida como una barrera para el tratamiento y comunicación de aquella información personal "apropiada" para hacer frente a situaciones de emergencia y proteger los derechos fundamentales de los titulares de datos personales.

Así, definir desde la perspectiva jurídica qué significa el término "emergencia" implica referirse en primer lugar, a la definición genérica del término. Al respecto, el *Diccionario de la Real Academia de la Lengua Española* indica que la palabra emergencia alude a una "situación de peligro que requiere una acción inmediata".[2194]

Desde la perspectiva normativa, en nuestro país, la Ley General de Protección Civil establece que se entiende por emergencia a la "situación anormal que puede causar un daño a la sociedad y propiciar un riesgo excesivo para la seguridad e integridad de la población en general, generada o asociada con la inminencia, alta probabilidad o presencia de un agente perturbador.[2195]

En el ámbito doctrinal, Antonio María Hernández precisa que la emergencia alude a "situaciones excepcionales, previsibles o no que afectan el orden constitucional, los hechos que las producen pueden ser originados en diversas causas políticas, económicas, sociales o de la naturaleza, para enfrentar estos hechos, el derecho crea diversas instituciones de emergencia, que varían según las legislaciones, estas situaciones producen un acrecentamiento de facultades en los poderes estatales y particularmente en el Ejecutivo y correlativamente, un descaecimiento o restricciones en los derechos y garantías individuales; debe existir un verdadero estado de necesidad".[2196]

Para profundizar lo anterior, resulta interesante el caso "Lawless contra Irlanda" en el que estableció que una "emergencia pública que amenaza la vida de la nación" debe entenderse una situación verdaderamente excepcional que pone o puede poner en peligro el normal funcionamiento de las instituciones públicas, establecido de acuerdo con el deseo legalmente expresado de los ciudadanos, tanto en lo que concierne a la situación interna del país como a las relaciones con Estados extranjeros.[2197] En el citado caso, además se estableció que el término se refiere a situación excepcional de crisis o emergencia que afecta al conjunto de la población y constituye una amenaza a la vida organizada de la comunidad sobre la que se fundamenta el Estado.[2198]

En cuanto a los elementos de la "emergencia", desde la perspectiva jurídica, Antonio Hernández María precisa que los distintos elementos que la caracterizan son: a) se trata de situaciones excepcionales, previsibles o no que afectan el orden constitucional; b) los hechos que las producen pueden ser originados en diversas causas políticas, económicas, sociales o de la naturaleza; c) para enfrentar estos hechos, el derecho crea diversas instituciones de emergencia, que varían según las legislaciones; d) estas situaciones hacen

2194 RAE. (2018) "emergencia" en *Diccionario de la Real Academia de la Lengua Española.* Disponible en: http://dle.rae.es/?id=EiX5X40

2195 Artículo 2, fracción XVIII de la Ley General de Protección Civil.

2196 Hernández, A. (2016). *Las emergencias y el orden constitucional.* México. UNAM-Instituto de Investigaciones Jurídicas, p. 7.

2197 Tribunal Europeo de Derechos Humanos, caso "Lawless vs. Irlanda", de 01/07/1961.

2198 Ídem.

crecer las facultades de los poderes estatales, y particularmente en el Ejecutivo y correlativamente, un descaecimiento o restricciones en los derechos y garantías individuales; e) debe existir un verdadero estado de necesidad. [2199]

De esta manera, en la doctrina se ha manifestado, según expone Campillo Sainz, que existe un "estado de necesidad" cuando la integridad, la soberanía, las instituciones fundamentales, la dignidad de un país o el bien común se encuentran seriamente afectados o gravemente amenazados.[2200] Ante esta situación el referido autor precisa que, todos los intereses particulares —aun aquellos que en una época normal son objeto de especial tutela— deben subordinarse al interés general y la autoridad deberá de disponer de la libertad de acción y los medios necesarios para hacer frente al peligro.[2201]

Así, la Organización Mundial Salud, al referirse al término "emergencia" señala que éstas en su conjunto "pueden tener profundas repercusiones políticas, económicas, sociales y de salud pública, y sus consecuencias a largo plazo pueden a veces persistir durante años. Las emergencias pueden ser el resultado de desastres naturales, conflictos, brotes de enfermedades, contaminación de alimentos o derrames químicos o radionucleares, entre otros peligros".[2202]

De forma concreta, en el ámbito normativo, es la Constitución Política de los Estados Unidos Mexicanos la que, en su artículo 29, establece las restricciones a los derechos humanos.[2203] Dichas restricciones, además, deberán aplicarse respetando también el contenido de las disposiciones del derecho internacional de los derechos humanos.[2204]

2199 Hernández, A. (2016). *Las emergencias y el orden constitucional.* México. UNAM-Instituto de Investigaciones Jurídicas, p. 7.

2200 Ídem.

2201 Campillo, J. (2016) "El juicio de amparo y la legislación de emergencia (1944)" en *Doctrina constitucional mexicana.* Colección INEHRM. México. UNAM-Instituto de Investigaciones Jurídicas, p. 176.

2202 OPS/OMS. (2013). *Marco de respuesta a emergencias.* Washington. Disponible en: http://apps.who.int/iris/bitstream/handle/10665/89604/9789275317853_spa.pdf;jsessionid=A4C340FCCDA5BB07CA150C2DEA751900?sequence=1. Fecha de consulta: 26 de septiembre 2018.

2203 Artículo 29. En los casos de invasión, perturbación grave de la paz pública, o de cualquier otro que ponga a la sociedad en grave peligro o conflicto, solamente el Presidente de los Estados Unidos Mexicanos, con la aprobación del Congreso de la Unión o de la comisión permanente cuando aquel no estuviere reunido, podrá restringir o suspender en todo el país o en lugar determinado el ejercicio de los derechos y las garantías que fuesen obstáculo para hacer frente, rápida y fácilmente a la situación; pero deberá hacerlo por un tiempo limitado por medio de prevenciones generales y sin que la restricción o suspensión se contraiga a determinada persona. Si la restricción o suspensión tuviese lugar hallándose el Congreso reunido, éste concederá las autorizaciones que estime necesarias para que el Ejecutivo haga frente a la situación; pero si se verificase en tiempo de receso, se convocará de inmediato al Congreso para que las acuerde.
En los decretos que se expidan, no podrá restringirse ni suspenderse el ejercicio de los derechos a la no discriminación, al reconocimiento de la personalidad jurídica, a la vida, a la integridad personal, a la protección a la familia, al nombre, a la nacionalidad; los derechos de la niñez; los derechos políticos; las libertades de pensamiento, conciencia y de profesar creencia religiosa alguna; el principio de legalidad y retroactividad; la prohibición de la pena de muerte; la prohibición de la esclavitud y la servidumbre; la prohibición de la desaparición forzada y la tortura; ni las garantías judiciales indispensables para la protección de tales derechos.
La restricción o suspensión del ejercicio de los derechos y garantías debe estar fundada y motivada en los términos establecidos por esta Constitución y ser proporcional al peligro a que se hace frente, observando en todo momento los principios de legalidad, racionalidad, proclamación, publicidad y no discriminación.
Cuando se ponga fin a la restricción o suspensión del ejercicio de los derechos y garantías, bien sea por cumplirse el plazo o porque así lo decrete el Congreso, todas las medidas legales y administrativas adoptadas durante su vigencia quedarán sin efecto de forma inmediata. El Ejecutivo no podrá hacer observaciones al decreto mediante el cual el Congreso revoque la restricción o suspensión. Los decretos expedidos por el Ejecutivo durante la restricción o suspensión, serán revisados de oficio e inmediatamente por la Suprema Corte de Justicia de la Nación, la que deberá pronunciarse con la mayor prontitud sobre su constitucionalidad y validez.

2204 Al respecto, la Convención Americana de Derechos Humanos indica lo siguiente:
CAPITULO IV
SUSPENSION DE GARANTIAS, INTERPRETACION Y APLICACION
Artículo 27. Suspensión de Garantías
1. En caso de guerra, de peligro público o de otra emergencia que amenace la independencia o seguridad del Estado

Sobreseimiento del procedimiento

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El sobreseimiento es el acto jurídico de carácter procesal, fundado y motivado, emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) o los organismos garantes de las entidades federativas en el ámbito de sus respectivas competencias, mediante el cual se pone fin a un procedimiento administrativo en materia de protección de datos personales sin resolver de forma definitiva la resolución del procedimiento por razones que atiendan el fondo del asunto sometido a su consideración.

El sobreseimiento es una figura de derecho procesal que se encuentra regulada en la normatividad de protección de datos personales vigente en México de forma específica en las reglas aplicables a los procedimientos en dicha materia. De manera general, el sobreseimiento suele hacer referencia a la resolución judicial por la cual se declara que existe un obstáculo jurídico o de hecho que impide la decisión del fondo de la controversia.[2205] En el tema de datos personales opera de la misma forma, solo que aquí la resolución recae en uno procedimientos específicos regulados en la Ley.

Es decir, el sobreseimiento impide a la autoridad garante (federal o local, según corresponda) entrar al estudio del fondo de la cuestión planteada porque cumple con una condición de improcedencia[2206] y por lo tanto se decreta la conclusión del procedimiento instaurado.

En la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) la figura del sobreseimiento se acoge en relación con la sustanciación del procedimiento de protección de derechos (PPD)[2207] al establecerse la posibilidad de que se decrete el sobreseimiento respecto de la solicitud de protección de datos[2208] presentada por el titular (SPD).[2209]

Por otro lado, en la esquela del derecho público, la figura del sobreseimiento se reconoce respecto de los procedimientos de impugnación en materia de protección de datos personales: el recurso de revisión (RR) y el recurso de inconformidad (en adelante RI), ambos regulados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y los Lineamientos Generales de Protección de Datos Personales para el Sector Público (Lineamientos Generales).

---

parte, éste podrá adoptar disposiciones que, en la medida y por el tiempo estrictamente limitados a las exigencias de la situación, suspendan las obligaciones contraídas en virtud de esta Convención, siempre que tales disposiciones no sean incompatibles con las demás obligaciones que les impone el derecho internacional y no entrañen discriminación alguna fundada en motivos de raza, color, sexo, idioma, religión u origen social.

2. La disposición precedente no autoriza la suspensión de los derechos determinados en los siguientes artículos: 3 (derecho al reconocimiento de la personalidad Jurídica); 4 (derecho a la vida); 5 (derecho a la integridad personal); 6 (prohibición de la esclavitud y servidumbre); 9 (principio de legalidad y de retroactividad); 12 (libertad de conciencia y de religión); 17 (protección a la familia); 18 (derecho al nombre); 19 (derechos del niño); 20 (derecho a la nacionalidad), y 23 (derechos políticos), ni de las garantías judiciales indispensables para la protección de tales derechos.
3. Todo Estado parte que haga uso del derecho de suspensión deberá informar inmediatamente a los demás Estados Partes en la presente Convención, por conducto del secretario general de la Organización de los Estados Americanos, de las disposiciones cuya aplicación haya suspendido, de los motivos que hayan suscitado la suspensión y de la fecha en que haya dado por terminada tal suspensión.

2205 *Vid*, tesis 223064. Tribunales colegiados de circuito. Octava época. *Semanario Judicial de la Federación.* Tomo VII, mayo de 1991, p. 302.

2206 *Vid*, tesis, 232302. Pleno. Séptima época. *Semanario Judicial de la Federación*. Volumen 187-192. Primera parte, p. 88.

2207 Se recomienda consultar la definición de "procedimiento de protección de derechos", en esta obra.

2208 Ver definición de "solicitud de protección de datos", en el presente *Diccionario de Protección de Datos Personales.*

2209 Con fundamento en el artículo 53 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

De esta manera, los aspectos referentes a la operación de la figura del sobreseimiento en la normatividad de datos personales se estudian a partir de las normatividades referidas, destacando los supuestos en los que se hace presente esta figura.

1. Sobreseimiento en la normatividad del sector privado

El sobreseimiento se presenta dentro del PPD regulado en la LFPDPPP, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) y los Lineamientos de los Procedimientos, pero no en otros procedimientos como el de verificación y el de imposición de sanciones.

En relación con lo anterior, la fracción I del artículo 51 hace referencia a la facultad del INAI para decretar el sobreseimiento respecto de la SPD formulada por el titular:

> Artículo 51.- Las resoluciones del Instituto podrán:
>
> I. Sobreseer o desechar la solicitud de protección de datos por improcedente.

De forma concreta, los artículos 53 de la LFPDPPP y el 45 de los Lineamientos de los Procedimientos contemplan los siguientes supuestos bajo los cuales el INAI, a través de su Dirección General de Protección de Derechos y Sanción (DGPDS), podrá decretar el sobreseimiento de la SPD cuando:

a) el titular fallezca,
b) el titular se desista de manera expresa,[2210]
c) se admita la solicitud de protección de datos, pero sobrevenga una causal de improcedencia y[2211]
d) por cualquier motivo quede sin materia la misma.

No obstante, el sobreseimiento también puede resultar respecto del PPD en lo general. En este sentido, los Lineamientos de los Procedimientos[2212] contemplan los siguientes supuestos específicos en los que el INAI, por conducto de la DGPDS y como unidad administrativa competente, podrá decretar el sobreseimiento del PPD cuando:

a) el responsable haya acreditado haber dado respuesta a la SPD en tiempo y forma y la haya notificado al titular,

---

2210 En relación con esto se puede citar el siguiente precedente:
VII-J-SS-105
DESISTIMIENTO DE LA INSTANCIA EN EL JUICIO CONTENCIOSO ADMINISTRATIVO. PROCEDE DECRETAR EL SOBRESEIMIENTO DEL JUICIO. Cuando el promovente del juicio se desiste expresamente de la instancia desaparecen todas las consecuencias producidas por esa presentación, debido a que el desistimiento tiene como efecto que las cosas vuelvan jurídicamente al estado que guardaban hasta antes de la presentación de la demanda; ello es así pues dentro de la doctrina procesal, el desistimiento ha sido considerado como la renuncia al ejercicio de una acción, el abandono de una instancia o de la reclamación de un derecho, lo que implica que el desistimiento de la instancia solo da por terminado el proceso relativo. Además de que el desistimiento de la acción no es un deber sino un derecho, que el actor conserva para desistirse de la demanda o parte de ella, en el momento que lo considere conveniente, mientras no se dicte sentencia, y ese desistimiento extingue la acción, lo que conlleva a que desaparezca toda relación jurídico-procesal que debió haber en el juicio, por lo que procede sobreseer el juicio contencioso administrativo conforme lo dispuesto en la fracción I del artículo 9, de la Ley Federal de Procedimiento Contencioso Administrativo. (Tesis de jurisprudencia aprobada por acuerdo G/59/2013).
RTFJFA. (2013, diciembre). *Tesis de jurisprudencia aprobada por acuerdo G/59/2013*. Séptima época. Año III. No. 29, p. 93.

2211 Las causales de improcedencia se prevén en el artículo 52 de la LFPDPPP y el 44 de los Lineamientos de los Procedimientos:
a) el Instituto no sea competente;
b) el Instituto haya conocido anteriormente de la solicitud de protección de datos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente;
c) se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo;
d) se trate de una solicitud de protección de datos ofensiva o irracional, o
e) sea extemporánea.

2212 *Vid*, artículo 22 de los Lineamientos de los Procedimientos.

b) el responsable acredite haber dado respuesta a la solicitud de ejercicio de derechos en tiempo y forma, y la solicitud no haya sido presentada por el titular en los plazos previstos por la normatividad aplicable y

c) en caso de que el titular manifieste su conformidad con la respuesta emitida por el responsable durante el PPD o cuando la misma se haya emitido fuera del plazo establecido por el artículo 32 de la LFPDPPP[2213] y el responsable la haya notificado al titular y al INAI.

En consecuencia, en el sector privado, la figura del sobreseimiento tiene el alcance de concluir de forma definitiva el PPD, ya sea porque la resolución del INAI decrete el sobreseimiento de la SPD o se decrete el sobreseimiento del propio PPD bajo los supuestos previstos en el artículo 22 de los Lineamientos de los Procedimientos. Es decir, el sobreseimiento opera cuando la DGPDS del INAI concluye el PPD y lo deja sin efectos.[2214]

2. Sobreseimiento en el sector público

La LGPDPPSO prevé que la figura del sobreseimiento pueda presentarse dentro de los denominados procedimientos de impugnación en materia de protección de datos personales, es decir, el RR y el RI. Como se explicará más adelante, como sucede en otras áreas de práctica, en el sector público el sobreseimiento tendrá el efecto de dar por concluido el procedimiento de impugnación instaurado por el titular ya sea ante el INAI y/o ante algún organismo garante, según resulte procedente.

A. Sobreseimiento del recurso de revisión

El RR[2215] regulado por el artículo 103 de los LGPDPPSO y 136 de los Lineamientos Generales es un procedimiento que se instaura a petición del titular para que la autoridad garante federal y/o local, según corresponda, realice una revisión de la respuesta del responsable al que haya ejercido sus derechos ARCO conforme a lo supuestos de procedencia señalados en el artículo 104 de la LGPDPPSO.[2216] La figura del sobreseimiento se presenta dentro de este procedimiento y tendrá como efecto que el mismo llegue a su conclusión.

2213 Artículo 32. El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Tratándose de solicitudes de acceso a datos personales, procederá la entrega previa acreditación de la identidad del solicitante o representante legal, según corresponda.
Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

2214 VII-P-2aS-1059
SOBRESEIMIENTO DE JUICIO. SE ACTUALIZA CUANDO LA AUTORIDAD DEJA SIN EFECTOS EL ACTO IMPUGNADO. El artículo 8, fracción I, de la Ley Federal de Procedimiento Contencioso Administrativo, establece que es improcedente el juicio ante el Tribunal Federal de Justicia Fiscal y Administrativa en los casos, por las causales y contra los actos que ahí se indican, entre otros, que no se afecten los intereses jurídicos del demandante. Por su parte, el artículo 9, fracción IV, de la Ley Federal de Procedimiento Contencioso Administrativo consigna que procede el sobreseimiento del juicio, si la autoridad demandada deja sin efectos el acto impugnado. Por tanto, si en juicio se demuestra que la autoridad dejó sin efectos la resolución impugnada, lo procedente en el juicio es decretar su sobreseimiento, ya que dicha resolución dejó de afectar los intereses jurídicos del demandante y se actualiza la hipótesis de la fracción IV del artículo 9 de la Ley Federal de Procedimiento Contencioso Administrativo.
RTFJA. (2016, octubre). Octava época. Año I. No. 3, p. 576

2215 Vea la definición de "recurso de revisión" para más información.

2216 Artículo 104. El recurso de revisión procederá en los siguientes supuestos:
I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;
II. Se declare la inexistencia de los datos personales;
III. Se declare la incompetencia por el responsable;
IV. Se entreguen datos personales incompletos;
V. Se entreguen datos personales que no correspondan con lo solicitado;
VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales;
VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia;
VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;
IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;
X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;
XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y
XII. En los demás casos que dispongan las leyes.

El artículo 111 de la LGPDPPSO reconoce la facultad del INAI y de los organismos garantes, en el ámbito de sus respectivas competencias, para emitir resoluciones que puedan decretar el sobreseimiento del RR:

> Artículo 111. Las resoluciones del Instituto o, en su caso, de los organismos garantes podrán:
>
> I. Sobreseer o desechar el recurso de revisión por improcedente.

Por otro lado, el artículo 113 de la LGPDPPSO establece con claridad los supuestos en los que la autoridad garante, ya sea federal o local, tendrá la facultad de sobreseer un RR. Los casos en los que la autoridad garante podrá decretar el sobreseimiento del RR son:

a) cuando el recurrente se desista expresamente,
b) cuando el recurrente fallezca,
c) admitido el recurso de revisión, se actualice alguna causal de improcedencia en términos de la LGPDPPSO,
d) cuando el responsable modifique o revoque su respuesta de tal manera que el RR quede sin materia o
e) quede sin materia el RR.

De esta forma, la emisión del acto en virtud del cual se decreta el sobreseimiento tendrá como efecto que el RR interpuesto llegue a su fin y su fin sin que se dirima de forma expresa el fondo de dicho procedimiento.

B. Sobreseimiento del recurso de inconformidad

EL RI es un medio de impugnación que permite que el titular pueda impugnar una resolución derivada de un RR, ya sea que ésta haya sido emitida por el INAI y/o por un organismo garante local.[2217] De forma análoga a como sucede en la tramitación del RR, la figura del sobreseimiento se actualiza como ejercicio de la facultad legal concedida por la LGPDPPSO al INAI como autoridad garante federal que conoce del RI.

De acuerdo con lo previsto por el artículo 124 de la LGPDPSO, el INAI tiene la facultad para sobreseer o desechar el RI, en cuyo caso el RI quedará sin materia para su continuación y será concluido de forma definitiva.[2218]

2217 Artículo 117. El titular, por sí mismo o a través de su representante, podrá impugnar la resolución del recurso de revisión emitido por el organismo garante ante el Instituto, mediante el recurso de inconformidad.
El recurso de inconformidad se podrá presentar ante el organismo garante que haya emitido la resolución o ante el Instituto, dentro de un plazo de quince días contados a partir del siguiente a la fecha de la notificación de la resolución impugnada.
Los organismos garantes deberán remitir el recurso de inconformidad al Instituto al día siguiente de haberlo recibido; así como las constancias que integren el procedimiento que haya dado origen a la resolución impugnada, el cual resolverá allegándose de los elementos que estime convenientes.

2218 Artículo 124. Las resoluciones del Instituto podrán:
I. Sobreseer o desechar el recurso de inconformidad;
II. Confirmar la resolución del organismo garante;
III. Revocar o modificar la resolución del organismo garante, o
IV. Ordenar la entrega de los datos personales, en caso de omisión del responsable.
Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los Organismos garantes deberán informar al Instituto sobre el cumplimiento de sus resoluciones.
Si el Instituto no resuelve dentro del plazo establecido en este capítulo, la resolución que se recurrió se entenderá confirmada.
Cuando el Instituto determine durante la sustanciación del recurso de inconformidad, que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente Ley y a las demás disposiciones aplicables en la materia, deberá hacerlo del conocimiento del órgano interno de control o de la instancia competente para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo.
Las medidas de apremio previstas en la presente Ley, resultarán aplicables para efectos del cumplimiento de las resoluciones que recaigan a los recursos de inconformidad. Estas medidas de apremio deberán establecerse en la propia resolución.

En cuanto a los supuestos respecto de los cuales procede el sobreseimiento del RI, el artículo 126 de la LGPDPSO contempla los siguientes supuestos:

a) cuando el recurrente se desista expresamente,
b) cuando el recurrente fallezca,
c) cuando el organismo garante modifique o revoque su respuesta de tal manera que el RI quede sin materia y
d) cuando, una vez admitido el RI, se actualice alguna causal de improcedencia en los términos de la LGPDPSO.

Así, en términos de los dispuesto por la LGPDPPSO, el sobreseimiento opera en los casos señalados en el artículo 126 de dicho ordenamiento y tendrá como consecuencia que el RI concluya de forma definitiva sin que haya existido un previo pronunciamiento de la autoridad garante federal respecto del fondo de la controversia que suscitó el RI.

Solicitud de protección de datos dentro del procedimiento de protección de derechos

Gabriel López López

Es la petición formulada por el titular que, habiendo considerado que la respuesta recaída a su solicitud de derechos de acceso, rectificación, cancelación y oposición (ARCO) no fue atendida o que lo fue indebidamente, acude ante el INAI a solicitar el inicio del procedimiento de protección de derechos (PPD).

Es un procedimiento administrativo seguido en forma de juicio, por virtud del cual el titular que habiendo ejercido previamente sus derechos ARCO ante el responsable y considerando que los mismos no fueron atendidos o que lo fueron indebidamente, acude ante el INAI, quien actuando como órgano materialmente jurisdiccional, previa audiencia y conciliación de las partes, cuando éstas expresen su voluntad de avenir, determina si el responsable atendió debida y oportunamente la solicitud de derechos ARCO.

1. Procedencia del PPD

Los artículos 45, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP),[2219] en sus párrafos primero, segundo y tercero y 115 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), previenen las hipótesis conforme a las cuales procede el PPD, siendo éstas las siguientes:

a) cuando el titular no haya recibido respuesta por parte del responsable;

2219 Artículo 45. El procedimiento se iniciará a instancia del titular de los datos o de su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de esta Ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.
En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable. En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.
La solicitud de protección de datos también procederá en los mismos términos cuando el responsable no entregue al titular los datos personales solicitados; o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

b) cuando el responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;

c) cuando el responsable se niegue a efectuar las rectificaciones a los datos personales;

d) cuando el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;

e) cuando el responsable se niegue a cancelar los datos personales;

f) cuando el responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición y

g) por otras causas que a juicio del Instituto sean procedentes conforme a la Ley o al Reglamento.

2. Medios de presentación de la solicitud

De la interpretación conjunta de los artículos 114 del RLFPDPPP y 12 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones (LPPDIVIS) se aprecia que la solicitud de protección de derechos podrá presentarse a través de las siguientes modalidades:

a) mediante escrito libre o a través de los formatos que proporcione el INAI, directamente ante las oficinas de dicho Instituto;

b) mediante escrito libre o a través de los formatos que proporcione el INAI, a través de correo certificado con acuse de recibo;[2220]

c) mediante escrito libre o a través de los formatos que proporcione el INAI, por servicio de mensajería dirigido a las oficinas de dicho Instituto, y

d) por medios electrónicos, a través del sistema electrónico del Instituto (IFAI-Prodatos),[2221] para lo cual es necesario que el solicitante cuente con la firma electrónica avanzada (FIEL).[2222]

3. Requisitos de la solicitud

Por lo que corresponde a la solicitud de protección de derechos, los elementos que debe contener son los siguientes:

a) el nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si existe;

b) el nombre del responsable ante el cual se presentó la solicitud de ejercicio de los derechos ARCO;

2220 De conformidad con el artículo 42, de la Ley del Servicio Postal Mexicano, el servicio de acuse de recibo de envíos o de correspondencia registrados, consiste en recabar en un documento especial la firma de recepción del destinatario o de su representante legal y en entregar ese documento al remitente, como constancia.

2221 El artículo 3, fracción IX, de los LPDDIVIS, define al sistema electrónico del instituto (IFAI Prodatos), como la plataforma informática proporcionada por el Instituto para que los titulares de datos personales o sus representantes legales, y denunciantes a través de medios electrónicos, presenten solicitudes de protección de derechos y denuncias por presuntos incumplimientos a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y a la normatividad que de ésta derive, así como para la sustanciación de los procedimientos que de ellas resulten. Disponible en: https://www.datospersonales.org.mx/

2222 El artículo 3, fracción VIII, de los LPDDIVIS, define a la firma electrónica avanzada (FIEL), como el conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos, la cual produce los mismos efectos jurídicos que la firma autógrafa.

c) el domicilio para oír y recibir notificaciones;

d) la fecha en que se le dio a conocer la respuesta del responsable, salvo que el procedimiento se inicie ante la ausencia de respuesta del responsable;

e) los actos que motivan su solicitud de protección de datos y

f) los demás elementos que se considere procedente hacer del conocimiento del INAI.

4. Documentos que deben adjuntarse a la solicitud

Conforme lo establecido en los artículos 46, párrafos tercero y cuarto, de la LFPDPPP, 116 del RLFPDPPP y 15 de los LPDDIVIS, al formularse su solicitud, el titular deberá acompañarla de la siguiente documentación:

a) copia de la solicitud del ejercicio de derechos que corresponda, así como copia de los documentos anexos para cada una de las partes, de ser el caso;

b) el documento que acredite que actúa por su propio derecho o en representación del titular;

c) el documento en que conste la respuesta del responsable, de ser el caso;

d) en el supuesto en que impugne la falta de respuesta del responsable, deberá acompañar una copia en la que obre el acuse o constancia de recepción de la solicitud del ejercicio de derechos por parte del responsable;

e) las pruebas documentales que ofrece para demostrar sus afirmaciones;

f) el documento en el que señale las demás pruebas que ofrezca, tales como documentales públicas o privadas, la inspección judicial, el cuestionario sobre el que verse la prueba pericial o testimonial, precisando los hechos sobre los que deban versar, así como los nombres y domicilios de los peritos o testigos, las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología, y

g) cualquier otro documento que se considere procedente someter a consideración del INAI.

En aquellos casos en que el titular no pueda acreditar que acudió con el responsable, ya sea porque éste se hubiere negado a recibir la solicitud de ejercicio de derechos ARCO o a emitir el acuse de recibo, lo hará del conocimiento del INAI mediante escrito, y éste le dará vista al responsable para que manifieste lo que a su derecho convenga, a fin de garantizar al titular el ejercicio de sus derechos ARCO.

5. Plazo para presentar la solicitud

Conforme a lo previsto por los artículos 45, primer párrafo de la LFPDPPP y 17, fracción I, de los LPPDIVIS, el plazo para presentar la solicitud es de 15 días hábiles siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.

En aquellos casos en que el responsable emita una respuesta, el cómputo relativo comenzará a contar a partir del día siguiente de su notificación y, si omite hacerlo, iniciará una vez que concluya el diverso plazo de 20 días que tiene para dar respuesta y pueda considerarse que no se pronunció en algún sentido y, por tanto, a partir de ese momento, el titular podrá instar al INAI la protección de sus datos personales.

Para el cómputo del plazo de referencia no se consideran días hábiles los sábados, domingos, el 1 de enero, 5 de febrero, 21 de marzo, 1 de mayo, 5 de mayo, 1 y 16 de septiembre, 20 de noviembre, 1 de diciembre de cada seis años —cuando corresponda a la transmisión del Poder Ejecutivo Federal— y el 25 de diciembre, así como los días en que tengan vacaciones generales en el INAI o aquellos en que se suspendan las labores.

En los casos en que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá presentarse a partir de que haya vencido el plazo de 20 días para emitir respuesta a la solicitud del titular. Para estos efectos, bastará que acompañe, a su solicitud de protección de derechos, el documento en el que conste la fecha de presentación de la solicitud de derechos ARCO.

De conformidad con lo previsto por el artículo 18 de los LPPDIVIS, el horario de presentación de las solicitudes ante el INAI comprende de las 9:00 a las 18:00 horas de lunes a viernes. Asimismo, tratándose de las solicitudes que se presenten a través del sistema IFAI Prodatos, después de las 18:00 horas, o en días inhábiles, éstas se tendrán por recibidas el día y hora hábil siguiente.

Recibida la solicitud, el INAI deberá proveer sobre su admisión en un plazo no mayor a 10 días, notificará tal circunstancia en un plazo no mayor a 10 días al promovente y correrá traslado al responsable de la misma conjuntamente con los documentos exhibidos, a fin de que éste manifieste lo que a su interés convenga y ofrezca las pruebas respectivas. Con este acuerdo se inicia el PPD.

Soporte electrónico

Andrés Velázquez Olavarrieta

El Artículo 4 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) establece que "la Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización". En el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) se entiende por soporte electrónico al medio de almacenamiento al que se pueda acceder solo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms.

Dada su importancia, se creó la NOM-151-SCFI-2015.[2223] Donde se contemplan algunos requisito que deben observarse para la conservación de mensajes de datos y digitalización de documentos. Esta norma prevé y regula, en otros aspectos, la conservación de mensajes de datos y la digitalización de documentos.

De acuerdo con la NOM-151-SCFI-2015 se define la digitalización como "el proceso que permite la migración de documentos impresos a mensaje de datos", esto quiere decir que se permitirá migrar del papel al documento electrónico para que éste surta plenos efectos legales y que se le trate como si fuese el original, quedando al libre arbitrio si elimina o no el papel.

2223 Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5436180&fecha=06/05/2016

Soporte físico

Andrés Velázquez Olavarrieta

El artículo 4 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) considera los soportes físicos o electrónicos para el tratamiento de datos personales. El soporte físico es definido en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) como "el medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales".

Este soporte ha sido muy importante, sin embargo, dada la digitalización, está siendo trasladado a los medios electrónicos por lo que se creó la NOM-151-SCFI-2015 con la cual se vigila "el proceso que permite la migración de documentos impresos a mensaje de datos", es decir, pasar de un soporte físico a uno electrónico para que éste surta plenos efectos legales y que se le trate como si fuese el original, quedando al libre arbitrio si elimina o no el papel.

Subcontratación

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El término "subcontratación" es empleado en la normatividad de datos personales para referirse a la comunicación de datos personales entre un encargado del tratamiento —que originariamente ya es un subcontratado según la terminología común del responsable del tratamiento— y un tercero contratado por dicho encargado (que podrá ser una persona física o moral), con la previa autorización y conocimiento del responsable del tratamiento para que ejecute en nombre y por cuenta de este último determinadas actividades que impliquen el tratamiento de datos personales.

En relación con el término subcontratación, debe precisarse que si bien el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) lo emplean en diversas ocasiones, dicho término no tiene una definición legal concreta como sucede en el caso de figuras como remisión (la comunicación entre responsable y encargado) y la transferencia (comunicación entre responsables) de datos personales. No obstante, derivado de la regulación normativa de este concepto en los sectores público y privado, podemos sustraer diversos elementos que permitirán realizar una explicación sobre el alcance de esta figura, así como de las obligaciones legales que el encargado del tratamiento o el tercero subcontratado deberán cumplir para no incurrir en los supuestos de responsabilidad legal establecidos en la normatividad aplicable.

1. Obligaciones del encargado del tratamiento en relación con las subcontrataciones

De acuerdo con lo previsto en la normatividad de datos personales (artículos 54 y 55 del RLFPDPP y artículos 61 y 62 de la LGPDPPSO), el encargado del tratamiento que realice la subcontratación de servicios de un tercero deberá cumplir con lo siguiente:

a) Obtener la autorización del responsable del tratamiento para la subcontratación. En este caso, si en las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el encargado, se prevé la posibilidad

de que el encargado pueda realizar subcontrataciones, la autorización de la subcontratación se entenderá como otorgada en dichos términos. Sin embargo, en el supuesto de que la subcontratación no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos, el encargado deberá obtener la autorización por parte del responsable.

b) Formalización de la subcontratación. Una vez obtenida la autorización del responsable, el encargado del tratamiento deberá formalizar la relación con el subcontratado[2224] a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido.[2225]

c) Carga de la prueba. El encargado del tratamiento tendrá la obligación de acreditar que la subcontratación se realizó con la autorización del responsable.

En el sector público, además de preverse los elementos citados en el artículo 59 de la LGPDPPSO, conforme a lo ordenado por el artículo 109 de los Lineamientos Generales de Protección de Datos personales para el Sector Público, el encargado deberá prever en el contrato o instrumento jurídico con el tercero subcontratado las siguientes obligaciones:

a) Permitir al INAI o al responsable realizar verificaciones en el lugar o establecimiento donde lleva a cabo el tratamiento de datos personales.

b) Colaborar con el INAI en las investigaciones previas que lleve a cabo en términos de lo dispuesto en la LGPDPPSO y en los Lineamientos Generales.

c) Generar, actualizar y conservar la documentación necesaria que le permita acreditar el cumplimiento de sus obligaciones.

En consecuencia, no debe olvidarse que el hecho de que exista una subcontratación de servicios sobre un tratamiento de datos personales, no implica ningún tipo de exoneración legal para el encargado del tratamiento respecto del cumplimiento de las obligaciones que tanto el RLFPDPPP como la LGPDPPSO prevén al respecto, según corresponda en cada caso.

Para un mayor detalle sobre la concreción de obligaciones correspondiente a la figura del encargado del tratamiento en lo general, recomendamos consultar las voces de “encargado” y “remisión” de datos personales presentes en esta obra.

2. Obligaciones de la persona física o moral subcontratada

De conformidad con lo previsto por los artículos 54 del RLFPDPPP y 61 de la LGPDPPSO, el tercero subcontratista tendrá las mismas obligaciones que se establecen para el encargado del tratamiento en la normatividad de datos personales.

En este mismo sentido, se pronuncian los Estándares de Protección de Datos Personales para los Estados Iberoamericanos en cuyo artículo 35.2 se indica que el subcontratado asumirá el carácter de encargado en los términos de cada legislación de los Estados miembros.

2224 Los Lineamientos Generales de Protección de Datos personales para el Sector Público contemplan la obligación de que el encargado prevea —en el instrumento jurídico con el subcontratado— los elementos previstos en el artículo 61 y 62 de la LGPDPSO:
Subcontratación de servicios que impliquen el tratamiento de datos personales.
Artículo 110. De acuerdo con lo previsto en los artículos 61 y 62 de la Ley General, en el contrato o cualquier instrumento que suscriba con el subcontratado se deberá prever, al menos, las cláusulas generales a que se refieren los artículos 59 de la Ley General y 109 de los Lineamientos Generales.

2225 En este sentido, el artículo 35.2 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos contempla lo siguiente:
35.3. El encargado formalizará la prestación de servicios del subcontratado a través de un contrato o cualquier otro instrumento jurídico que determine la legislación nacional del Estado Iberoamericano que resulte aplicable en la materia.

De manera general podemos señalar que tanto el RLFPDPPP[2226] como la LGPDPPSO[2227] coinciden al establecer las obligaciones aplicables al tercero subcontratista y que, como señalamos, serán idénticas a las del encargado original.

De la misma forma, podemos precisar que la normatividad de datos personales señala como obligaciones del encargado del tratamiento las siguientes:

a) Dependencia: únicamente puede tratar los datos conforme a las instrucciones que le facilite el responsable.
b) Finalidad: debe abstenerse de tratar los datos para finalidades distintas a las instruidas por el responsable.
c) Seguridad: debe cumplir con las medidas de seguridad previstas en la normatividad de datos personales.
d) Confidencialidad: debe tratar los datos con confidencialidad, la cual subsistirá aún después de que finalice el contrato de prestación de servicios que le vincula al responsable.
e) Cancelación: una vez finalizada la relación, o siempre que el responsable se lo pida, debe suprimir los datos personales que trate, salvo que una ley exija su conservación.
f) No transmisión: no podrá transferir ni remitir los datos a terceros, salvo en alguno que:
    i. el responsable le dé instrucciones para que lo haga,
    ii. el responsable le permita subcontratar o
    iii. los requiera la autoridad competente en términos de Ley.

No obstante, para mayor detalle sobre la concreción de las obligaciones legales del encargado del tratamiento, de nuevo recomendamos al lector a la consulta de la voz de "encargado del tratamiento".

3. Responsabilidad de la persona física o moral subcontratada

Finalmente, dado que el tercero subcontratista asumirá completamente las obligaciones inherentes a la figura del encargado del tratamiento, puede señalarse que, en el supuesto de que este último incumpla las instrucciones del responsable, según disponen el artículo 53 del RLFPDPPP y el artículo 60 de la LGPDPPSO, el tercero subcontratista será considerado como un responsable ilícito del tratamiento y por lo tanto, asumirá las obligaciones del responsable conforme a la normatividad aplicable a la protección de datos personales.

Esto quiere decir que el tercero subcontratado (a quien aplican las obligaciones originarias de un encargado) será considerado responsable, con las obligaciones propias de éste, cuando destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o efectúe una transferencia, incumpliendo las instrucciones del responsable.

2226 *Vid*, Artículo 50 del RLFPDPPP.

2227 Artículo 59 de la LGPDPPSO.

Subencargado

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El concepto "subencargado" hace referencia a la persona física o moral que —derivado de la comunicación de datos personales que le realiza un encargado del tratamiento—lleva a cabo actividades específicas de tratamiento de datos personales a nombre, y por cuenta, de un responsable del tratamiento con su previa autorización y conocimiento.

En relación con el subencargado, podemos señalar que éste se encuentra obligado a asumir las obligaciones propias que la normatividad de datos personales establece para el encargado del tratamiento de conformidad con lo previsto por los artículos 54 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPP) y 61 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

En este sentido, y de manera general, podemos señalar que tanto el RLFPDPPP[2228] como la LGPDPPSO[2229] coinciden al establecer las obligaciones aplicables al subencargado del tratamiento, mismas que se reseñan a continuación.

En términos de la legislación nacional, el subencargado debe cumplir con las siguientes obligaciones respecto del tratamiento de datos personales que realice a nombre y por cuenta del responsable:

a) Dependencia: únicamente puede tratar los datos conforme a las instrucciones que le facilite el responsable.
b) Finalidad: debe abstenerse de tratar los datos para finalidades distintas a las instruidas por el responsable.
c) Seguridad: debe cumplir con las medidas de seguridad previstas en la normatividad de datos personales.
d) Confidencialidad: debe tratar los datos con confidencialidad, la cual subsistirá aún después de la finalización del contrato de prestación de servicios que le vincula al responsable.
e) Cancelación: una vez finalizada la relación, o siempre que el responsable se lo pida, debe suprimir los datos personales que trate, salvo una ley exija su conservación.
f) No transmisión: no podrá transferir ni remitir los datos a terceros, salvo en alguno de los siguientes casos que:
    i. el responsable le dé instrucciones para que lo haga,
    ii. el responsable le permita subcontratar o
    iii. los requiera la autoridad competente en términos de Ley.

Finalmente, dado que el subencargado asume completamente las obligaciones inherentes a la figura del encargado del tratamiento, puede señalarse que, en el supuesto de que este último incumpla las instrucciones del responsable, según disponen el artículo 53 del RLFPDPPP y el artículo 60 de la LGPDPPSO, el subencargado, por antonomasia, será

2228 Artículo 50 del RLFPDPPP.

2229 Artículo 59 de la LGPDPPSO.

considerado como un responsable ilícito del tratamiento y en consecuencia, asumirá el carácter de responsable en términos de la normatividad aplicable.[2230]

Esto quiere decir que subencargado (a quien aplican las obligaciones originarias de un encargado) será considerado responsable y asumirá las obligaciones propias de éste cuando destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o efectúe una transferencia, incumpliendo las instrucciones del responsable.

Supresión de datos personales

María Solange Maqueo Ramírez

El artículo 3, fracción XXX, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) establece que la supresión consiste en "[l]a baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable". En términos análogos, el artículo 2, fracción XII del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) indica que la supresión es la "[a]ctividad consiste en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad, previamente establecidas por el responsable".

En atención al principio de calidad,[2231] la supresión de los datos debe realizarse (siempre que no exista una disposición en contrario como razones contables, fiscales, administrativas o históricas) una vez que éstos han dejado de ser necesarios para las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento, o bien, porque el titular de los datos personales ejerció su derecho de cancelación, previo bloqueo, en su caso, de los datos personales. En ese sentido, la supresión es la última etapa del tratamiento de datos personales durante su ciclo de vida. Así, la supresión de datos personales constituye un tratamiento por lo que debe efectuarse de conformidad con los principios y deberes jurídicos en la materia.

Cabe hacer notar que el término "supresión" en el sistema jurídico mexicano tiene una connotación distinta a la que se utiliza, por ejemplo, en el sistema jurídico europeo. Si bien en ambos casos la supresión supone la eliminación, destrucción o borrado de los datos personales, el reglamento general de protección de datos de la Unión Europea lo define como un derecho subjetivo en sí mismo, equivalente a lo que ellos denominan "derecho al olvido",[2232] cuya actualización se produce —salvo los supuestos de excepción previstos por el propio ordenamiento— cuando concurra cualquiera de las siguientes circunstancias: (a) los datos personales ya no sean necesarios para los fines para los cuales fueron recogidos o tratados; (b) el interesado retire su consentimiento en los supuestos previstos por el propio ordenamiento; (c) el interesado se oponga al tratamiento de los datos, siempre que no prevalezcan otros motivos legítimos para que éste continúe; (d) los datos hayan sido tratados ilícitamente; (e) se trate del cumplimiento de una obligación legal o (f) se hayan obtenido en relación con la oferta de servicios de la sociedad de la información.[2233]

2230 Sobre este particular, debe tenerse en cuenta también lo dispuesto en los Estándares de Protección de Datos: 35.4. Cuando el subcontratado incumpla sus obligaciones y responsabilidades respecto al tratamiento de datos personales que lleve a cabo conforme a lo instruido por el encargado, asumirá la calidad de responsable conforme a la legislación nacional del Estado iberoamericano que resulte aplicable en la materia.

2231 Cfr. Artículo 11 de la LFPDPPP, artículos 36 y 37 del RLFPDPPP, artículo 23 de la LGPDPPSO y artículo 19 de los Estándares de Protección de Datos para los Estados Iberoamericanos.

2232 El derecho de supresión sería equivalente en el sistema jurídico mexicano al derecho de cancelación.

2233 Artículo 17 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos

1. Plazos de conservación

Dado que la supresión de los datos personales supone la conclusión del tratamiento de datos personales, solo puede efectuarse una vez que han transcurrido los plazos de conservación correspondientes. De ahí que la supresión deba realizarse una vez que se han cumplido las finalidades que justificaron el tratamiento de los datos personales, más los plazos jurídicos, administrativos, contables, fiscales e históricos aplicables y, en su caso, el periodo de bloqueo correspondiente. En algunos supuestos, estos periodos de tiempo pueden coincidir.[2234]

Procedimiento

La supresión de datos personales debe seguir procedimientos adecuados que garanticen que los datos personales sean efectivamente borrados, eliminados o destruidos, de tal forma que no sea posible su recuperación o reutilización por el responsable o encargado del tratamiento ni por cualquier tercero. Para esos efectos, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha emitido la *Guía para el Borrado Seguro de Datos Personales* en la cual establece algunos parámetros y criterios de carácter meramente orientativo para que los responsables o encargados del tratamiento de datos personales conozcan "métodos y técnicas basadas en las mejores prácticas estándares, para la eliminación segura de los datos personales en los sistemas de tratamiento",[2235] de acuerdo con el tipo de soporte en el que se contienen los datos personales. Para esos efectos, la citada guía contiene tanto métodos físicos de borrado (entre los que se incluyen algunas características para la destrucción de los medios de almacenamiento físicos o electrónicos) como métodos lógicos (tales como la desmagnetización, la sobreescritura o el cifrado de medios).[2236]

Sobre el particular, los Lineamientos Generales de Protección de datos Personales para el Sector Público establecen que las políticas, métodos o técnicas que se adopten para la supresión de datos personales deberá considerar:

a) irreversibilidad: que el proceso utilizado no permita recuperar los datos personales,
b) seguridad y confidencialidad: que en la eliminación definitiva de los datos personales se consideren los deberes de confidencialidad y seguridad a que se refieren la Ley General y los presentes Lineamientos Generales, y
c) que sea favorable al medio ambiente: que el método utilizado produzca el mínimo de emisiones y desperdicios que afecten el medio ambiente.[2237]

Asimismo, el responsable del tratamiento de los datos personales está obligado a documentar la supresión de los datos personales, de acuerdo con el artículo 24 de la LGPDPPSO y 38 del RLFPDPPP. Ello supone la elaboración de un escrito en el que se establezca su realización y los métodos y técnicas utilizados para esos efectos.

En relación con lo anterior, el artículo 33 de la LGPDPPSO establece para los responsables del tratamiento de datos personales del sector público la obligación de elaborar un

datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), publicado en el *Diario Oficial de la Unión Europea L 119* el 4 de mayo de 2016.

2234 INAI. (2016, junio). *Guía para el borrado seguro de datos personales*. México, p. 6.

2235 INAI. (2016, junio). *Guía para el borrado seguro de datos personales*. México, pp. 3 y 4.

2236 INAI. (2016, junio). *Guía para el borrado seguro de datos personales*. México, pp. 14 y ss.

2237 INAI. (2018, enero 26). "Acuerdo mediante el cual se aprueban, los Lineamientos Generales de Protección de Datos Personales para el Sector Público", en *Diario Oficial de la Federación*.

“inventario de datos personales”. Sobre el particular, el artículo 59 de los Lineamientos Generales de Protección de Datos Personales para el sector Público establece que en dicho inventario se deberá documentar la información básica de cada tratamiento realizado, entre lo cual se incluye el ciclo de vida del dato. En consecuencia, siendo la supresión parte de ese ciclo de vida, ésta deberá constar en el inventario correspondiente.

Finalmente, cabe destacar que si la supresión se produce como consecuencia del ejercicio del derecho de cancelación por parte del titular de los datos personales o su representante, será necesario que el responsable del tratamiento de datos personales le notifique de esta situación, pues con ello se tendrá por realizada la cancelación correspondiente.

NOTAS

NOTAS

NOTAS

NOTAS

T

Tercero

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

Desde una acepción genérica, el término "tercero" hace referencia a una "persona que que no es ninguna de dos o más de quienes se trata o que intervienen en un negocio de cualquier género".[2238]

En el ámbito del derecho de protección de datos personales, la figura del tercero se reconoce y define de forma específica en la fracción XVI del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que indica que un tercero es:

> XVI. Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos. [2239]

Sin embargo, la LGPDPPSO no distingue esta figura y la normatividad aplicable al sector privado es poco precisa al definir sus contornos, y es necesario recurrir al derecho comparado para poder concretar un poco más los alcances de esta definición.

En España, el Reglamento de la Ley Orgánica de Protección de Datos Personales[2240] especifica, en su artículo 5, que el tercero es "la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento". Además, añade que podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

El Reglamento General de Protección de Datos de la Unión Europea (en adelante RGPD)[2241] define al "tercero" como:

2238 RAE. (2017). Tercero, en *Diccionario de la Lengua Española*. Disponible en: http://dle.rae.es/?id=ZX6JZWO

2239 Artículo 3, fracción XVI, de la LFPDPPP.

2240 Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

2241 *Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016.

10) tercero: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Por lo tanto, uniendo la definición de la LFPDPPP a lo expuesto por los textos en derecho comparado, podemos señalar que el tercero:

1. Puede ser una persona física o moral.
2. Puede ser un sujeto nacional o extranjero.
3. Es distinto del titular.
4. Es distinto del responsable.
5. Es distinto del encargado del tratamiento.
6. Es distinto a las personas que realizan el tratamiento bajo la autoridad del responsable o del encargado.

Se trata de los casos en que un tercero realiza el tratamiento por cuenta propia, es decir, para realizar un interés legítimo, singular y propio que él ostenta, pero sin determinar ni los fines ni los medios del tratamiento (esto lo hacen los responsables) y, como lo realizan persiguiendo un interés propio (el de su negocio o actividad para el que resulta necesario el tratamiento), tampoco se puede entender ese tratamiento como desarrollado por cuenta del responsable (es decir, por un encargado, que no tiene interés en ese tratamiento, siendo solo un mandato del responsable).

No siempre es sencillo diferenciar esta figura de los otros sujetos que intervienen en el tratamiento, pero reiteramos, la existencia de interés propio (del tercero) en el tratamiento es una de las diferencias primordiales, junto con no ser quien determina la finalidad y usos del tratamiento (eso lo hace el responsable). Por ejemplo, es como un operador de telecomunicaciones cuando es mero transmisor al prestar servicios de correo electrónico. Un tercero es una persona física a la que se le comunica información porque es necesaria para la defensa de su interés legítimo y/o su derecho en un procedimiento judicial (condóminos en un condominio, progenitores respecto de sus hijos, aunque no sean menores, etc.).

Titular de los datos personales

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El titular de los datos personales es la persona física a quien corresponden o conciernen los datos personales sujetos a tratamiento y por tanto es a quien se considera como sujeto de protección del derecho a la protección de datos personales.

Tanto la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) como la Ley General de Protección de Datos personales en Posesión de Sujetos Obligados (LGPDPPSO)[2242] definen en idénticos términos la figura del titular de los datos y señalan que se trata de la persona física a quien corresponden los datos personales.[2243]

2242 *Vid*, artículo 3, fracción XVII de la LFPDPPP y artículo 3, fracción XXXI de la LGPDPPSO.

2243 Así también lo hace la *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, publicada por el INAI. *Vid*, INAI. (2016, junio). *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, p. 4. Disponible en: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf Fecha de consulta: 17 de octubre de 2018.

El titular, como señala la *Guía para Titulares de Datos Personales* del INAI en su volumen 1 es el dueño de los datos personales, aunque éstos se encuentren en posesión de un tercero para su tratamiento.[2244]

En este orden de ideas, el individuo titular de los datos personales, la persona física[2245] a la que se asocian los mismos, es el sujeto de protección de la normatividad de datos personales, el titular del derecho humano a la protección de datos personales.[2246]

Del contenido de la exposición anterior, se pueden desprender diversos elementos que permiten explicar el alcance y contenido de la figura del titular de los datos personales:

1. Es una persona física o natural

Hace referencia a una persona o individuo que existe y, que en términos de la legislación civil —que se aplica de forma supletoria a la normatividad de datos personales según el artículo 5 de la LFPDPPP—,[2247] tiene capacidad jurídica. Es decir, que tiene la cualidad de ser sujeto de derechos y obligaciones.[2248] Por ello, debe anotarse que en esta materia este concepto es de trascendental importancia pues la normatividad de datos personales gira en torno a la garantía de la protección de la persona física respecto al lícito tratamiento de sus datos personales, quedando excluida la protección de las personas jurídicas.[2249] Así lo

2244 INAI. (s. f.). *Guía para Titulares de Datos Personales*, volumen 1, p. 10. Disponible en: *http://inicio.ifai.org.mx/Guias/Guia%20Titulares-01_PDF.pdf* Fecha de consulta: 17 de octubre de 2018,

2245 En este sentido, por ejemplo, normatividades como el Reglamento General de Protección de Datos de la Unión Europea no utiliza el concepto de titular, sino el de interesado. Podemos derivar su definición de la disposición donde se define datos personales:
"1) datos personales: toda información sobre una persona física identificada o identificable (el interesado); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

2246 En relación con este tema, se recomienda consultar la definición de "protección de datos personales" que se incluye en esta obra.

2247 La LFPDPPP tiene una norma supletoria a la normatividad de datos personales. *vid*, figura del titular de los datos personales: en este sentido, el artículo 22 del Código Civil Federal establece lo siguiente:
Artículo 22. La capacidad jurídica de las personas físicas se adquiere por el nacimiento y se pierde por la muerte; pero desde el momento en que un individuo es concebido, entra bajo la protección de la ley y se le tiene por nacido para los efectos declarados en el presente código.

2248 "CAPACIDAD DE DERECHO Y CAPACIDAD DE EJERCICIO (PERSONALIDAD EN JUICIO). Existe una distinción entre capacidad de derecho y capacidad de obrar o de ejercicio: la primera, es la cualidad de ser sujeto de derechos y obligaciones, y la tienen todos los seres humanos, y la segunda, es la posibilidad de efectuar manifestaciones de voluntad, jurídicamente eficaces. La capacidad de obrar constituye la regla general, y por excepción, hay casos de incapacidad determinados por la ley, como son: la menor edad; la interdicción; la mujer casada, en algunos estados, como el de Puebla, y la falta de personalidad, tanto del actor como del demandado; esto implica carencia de capacidad de obrar, en el sujeto, o carencia o defecto en la representación, o de prueba de ésta. Ahora bien, si quien compareció como cesionario de los legatarios en una sucesión, promoviendo la remoción de albacea definitivo, solo probó la cesión que le hicieron algunos de esos legatarios y no acreditó ser cesionario de los otros, este hecho implicaría carencia de acción, en lo que a esas partes se refirió, pero no falta de personalidad, ya que el cesionario, como titular de los derechos adquiridos, promovió por su propio derecho y no como apoderado de los legatarios, y por lo mismo, cualesquiera que hayan sido los fundamentos de la autoridad responsable para declarar improcedente esa falta de personalidad, no incurrió en violación de garantías".
Amparo civil en revisión 8625/43. Bravo viuda de Bonilla Magdalena, sucesión del 31 de agosto de 1944. Unanimidad de cuatro votos. El ministro Emilio Pardo Aspe no intervino en la votación de este asunto por las razones que constan en el acta del día. La publicación no menciona el nombre del ponente.
Vid, Tesis, 350119. Tercera Sala. Quinta época. *Semanario Judicial de la Federación*. Tomo LXXXI, pp. 4865.

2249 No obstante, en la esfera jurisdiccional se ha señalado lo siguiente:
"PRINCIPIO DE INTERPRETACIÓN MÁS FAVORABLE A LA PERSONA. ES APLICABLE RESPECTO DE LAS NORMAS RELATIVAS A LOS DERECHOS HUMANOS DE LOS QUE SEAN TITULARES LAS PERSONAS MORALES. El artículo 1 de la Constitución Política de los Estados Unidos Mexicanos, al disponer que en los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en dicha Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las garantías para su protección, no prevé distinción alguna, por lo que debe interpretarse en el sentido de que comprende tanto a las personas físicas, como a las morales, las que gozarán de aquellos derechos en la medida en que resulten conformes con su naturaleza y fines. En consecuencia, el principio de interpretación más favorable a la persona, que como imperativo establece el párrafo segundo del citado precepto, es aplicable respecto de las normas relativas a los derechos humanos de los que gocen las personas morales, por lo que deberán interpretarse favoreciendo

destacaba también el Grupo de Trabajo del Artículo 29 (GT29 o WP29 por sus siglas en inglés),[2250] al señalar que precisamente la protección proporcionada por la normatividad "se aplica a las personas físicas, es decir, a los seres humanos", especificando además que "el derecho a la protección de los datos personales es, en ese sentido, universal sin circunscribirse a los nacionales o residentes en determinado país".[2251]

2. Es el sujeto de protección de la normatividad

El derecho a la protección de datos personales es un derecho humano inherente a la persona,[2252] sustentado en la propia dignidad[2253] y libertad de la persona. La protección de datos personales, como derecho autónomo e independiente, gira en torno al individuo.

3. Los datos personales son de su titularidad y le conciernen

Los datos personales tienen tal carácter en la medida en que estos se refieren a la persona o se pueden asociar con ella.[2254] Es decir, "los datos son personales cuando son datos relativos a seres vivos identificados o identificables en principio".[2255] En relación con lo anterior, el GT29 declara que para considerar que los datos versan sobre una persona debe haber un elemento contenido, un elemento finalidad o[2256] un elemento resultado:[2257]

---

en todo tiempo la protección más amplia, a condición de que no se trate de aquellos derechos cuyo contenido material solo pueda ser disfrutado por las personas físicas, lo que habrá de determinarse en cada caso concreto. *Vid*, Tesis: P./J. 1/2015 (10a.). Pleno. Décima época. Jurisprudencia. *Gaceta del Semanario Judicial de la Federación*. Libro 16. Marzo de 2015. Tomo I, p. 117.

2250 Este grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo de la UE, de carácter consultivo e independiente para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.

2251 Grupo de Trabajo del Artículo 29 (WP 136). Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

2252 En relación con este tema, por ejemplo, el GTA29 al referirse a la información de personas fallecidas ha destacado que: "en principio, la información relativa a personas fallecidas no se debe considerar como datos personales sujetos a las normas de la Directiva, ya que los difuntos dejan de ser personas físicas para el derecho civil. Sin embargo, en determinados casos los datos de los difuntos aún pueden recibir indirectamente una cierta protección". *Vid*, Grupo de Trabajo del Artículo 29 (WP 136). Dictamen 4/2007 sobre el concepto de datos personales. Adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pd

2253 "DIGNIDAD HUMANA. CONSTITUYE UNA NORMA JURÍDICA QUE CONSAGRA UN DERECHO FUNDAMENTAL A FAVOR DE LAS PERSONAS Y NO UNA SIMPLE DECLARACIÓN ÉTICA. La dignidad humana no se identifica ni se confunde con un precepto meramente moral sino que se proyecta en nuestro ordenamiento como un bien jurídico circunstancial al ser humano, merecedor de la más amplia protección jurídica, reconocido actualmente en los artículos 1, último párrafo; 2, apartado A, fracción II; 3, fracción II, inciso c y 25 de la Constitución Política de los Estados Unidos Mexicanos. En efecto, el Pleno de esta Suprema Corte ha sostenido que la dignidad humana funge como un principio jurídico que permea en todo el ordenamiento, pero también como un derecho fundamental que debe ser respetado en todo caso, cuya importancia resalta al ser la base y condición para el disfrute de los demás derechos y el desarrollo integral de la personalidad. Así las cosas, la dignidad humana no es una simple declaración ética, sino que se trata de una norma jurídica que consagra un derecho fundamental a favor de la persona y por el cual se establece el mandato constitucional a todas las autoridades, e incluso particulares, de respetar y proteger la dignidad de todo individuo, entendida ésta -en su núcleo más esencial- como el interés inherente a toda persona, por el mero hecho de serlo, a ser tratada como tal y no como un objeto, a no ser humillada, degradada, envilecida o cosificada". *Vid*, Tesis: 1a. CCCLIV/2014 10a. Primera Sala. *Gaceta del Semanario Judicial de la Federación*. Libro 11. Octubre de 2014. Tomo I, p. 602.

2254 Se recomienda consultar la definición de "dato personal" contenida en este *Diccionario de Protección de Datos Personales*.

2255 Grupo de Trabajo del Artículo 29 (WP 136). Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio. Disponible en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

2256 Según señala el GT29, debe tenerse en cuenta que estos tres elementos (contenido, finalidad y resultado) habrán de ser considerados como condiciones alternativas y no acumulativas, pues cuando exista el elemento de contenido, no hay ninguna necesidad de que también aparezcan los otros elementos para considerar que la información se refiere a una persona física. Es decir, para determinar si los datos se refieren a una persona hay que contestar, analizando cada dato, en función de sus características.

2257 Grupo de Trabajo del Artículo 29 (WP 136). Dictamen 4/2007 sobre el concepto de datos personales, adoptado el 20 de junio.

a) Contenido: está presente en aquellos casos en que —de acuerdo con lo que una sociedad suele general y vulgarmente entender por la palabra "sobre"— se proporciona información sobre una persona concreta, independientemente de cualquier propósito que puedan abrigar el responsable del tratamiento de los datos o un tercero, o de la repercusión de esa información en el interesado. La información versa sobre una persona cuando se refiere a esa persona, lo que debe ser evaluado teniendo en cuenta todas las circunstancias que rodean el caso.

b) Finalidad: este elemento existe cuando los datos se utilizan o es probable que se utilicen, teniendo en cuenta todas las circunstancias que rodean el caso concreto, con la finalidad de evaluar, tratar de determinada manera o influir en la situación o el comportamiento de una persona.

c) Resultado: se presenta este elemento cuando a pesar de la ausencia de un elemento de contenido o de finalidad cabe considerar que los datos versan sobre una persona determinada porque, teniendo en cuenta todas las circunstancias que rodean el caso concreto, es probable que su uso repercuta en los derechos y los intereses de determinada persona.

Toma de decisiones sin intervención humana valorativa

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

El concepto "decisiones sin intervención humana valorativa" hace referencia a un tratamiento de datos personales que tiene lugar mediante el uso de distintas tecnologías de carácter automatizado sin que intervenga la valoración de una persona física.

Según el *Diccionario de la Lengua Española* (DLE), la palabra "automatizar" significa convertir ciertos movimientos en movimientos automáticos o indeliberados.[2258]

En cambio, el adjetivo "automático" hace referencia a un mecanismo o aparato que funciona en todo o en por parte por sí solo.[2259] Al hablar de un tratamiento de datos personales[2260] automatizado, se acepta que se trata de operaciones que son efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados, y entre las que destacan el registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión, entre otras.

De esta forma, en aquellos tratamientos de datos personales que son realizados mediante el uso de mecanismos automatizados, algoritmos y técnicas de inteligencia artificial que imitan el comportamiento del cerebro humano, al no existir la intervención de una persona física para la toma de decisiones específicas, existe un importante riesgo de que la determinación final adoptada a partir del uso de dichas técnicas pueda afectar negativamente a la persona o bien produzca riesgos en su persona.[2261] En consecuencia, existen

2258 RAE. (2017). Automatizar, en *Diccionario de la Lengua Española.* Disponible en: https://dle.rae.es/?id=4TVTwDp

2259 RAE. (2017). Automático, en *Diccionario de la Lengua Española.* Disponible en: https://dle.rae.es/?id=4TO3M08

2260 Se recomienda consultar la definición de "tratamiento" presente en este *Diccionario de Protección de Datos Personales*.

2261 En este sentido, la primera ley española en protección de datos personales, la antigua Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal se concibió como un ordenamiento innovador para hacer frente al uso de la informática y que tuvo por objeto limitar el uso de la informática y otras

previsiones específicas en la normatividad que tutelan el derecho de la persona a conocer el alcance de dichas determinaciones y los elementos personales que se emplearon para su elaboración.

De esta manera, en diversas normatividades de datos personales se ha reconocido el derecho de las personas a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, y que se base únicamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad.[2262]

En particular, dicho derecho incluye también la facultad del titular de impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos personales que ofrezca una definición de sus características o personalidad, es decir, una elaboración de su perfil.

En México, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), en su artículo 112, establece en su primer párrafo que cuando ocurra el tratamiento de datos personales sobre la base de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre. Es decir, con base en esta disposición, se busca que el titular pueda consentir o no, un tratamiento automatizado de datos personales que pudiera generar efectos en su esfera jurídica.

Dada la importancia de conocer el alcance y la lógica empleada para la adopción de determinaciones sustentadas en tratamientos de datos automatizados, el RLFPDPPP también habilita al titular de los datos a que pueda conocer la información sobre su persona que obra en poder del responsable así como a solicitar la rectificación de la misma cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto para que, a partir de los procedimientos adoptados por el responsable, pueda estar en posibilidad de solicitar que la decisión adoptada sea reconsiderada.[2263]

Asimismo, los Estándares de Protección de Datos para los Estados Iberoamericanos también reconocen la prerrogativa del titular a no ser objeto de tratamientos automatizados sin intervención humana cuando las determinaciones le produzcan efectos jurídicos o le afecten de manera significativa.[2264]

---

técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

2262 La Ley Orgánica de Protección de Datos Personales dispone:
Artículo 13. Impugnación de valoraciones.
1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

2263 Segundo párrafo del artículo 112 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

2264 29. Derecho a no ser objeto de decisiones individuales automatizadas
29.1. El titular tendrá derecho a no ser objeto de decisiones que le produzcan efectos jurídicos o le afecten de manera significativa que se basen únicamente en tratamientos automatizados destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

Finalmente, también destacan las previsiones del Reglamento General de Protección de Datos Personales europeo que protegen al titular de los datos para que no sea objeto de decisiones basadas únicamente en el tratamiento automatizado,[2265] incluida la elaboración de perfiles cuando éstas le produzcan efectos jurídicos o le afecten significativamente.[2266]

Transferencia

Isabel Davara Fernández de Marcos,
Alexis Cervantes Padilla y
Gregorio Barco Vega

La transferencia de datos personales se encuentra definida con precisión en la legislación nacional en materia de protección de datos personales.

En el sector privado, la transferencia se define en la fracción XIX del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), y en el sector público, dicho concepto se define en la fracción XXXII del artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO):

Definición de "transferencia"	
Artículo 3, fracción IIX, de la LFPDPPP	Artículo 3, fracción XXXII, de la LGPDPPSO
Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.	Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado.

En adición a lo anterior, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) precisa que la transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a una persona distinta del titular, del responsable o del encargado.

De las definiciones presentadas se pueden sustraer los siguientes elementos:

a) La transferencia es realizada por un responsable del tratamiento regulado por la normatividad de datos personales.

2265 El considerando 71) del Reglamento General de Protección de Datos señala:
(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

2266 Artículo 22 del Reglamento General de Protección de Datos.

b) La transferencia de datos personales implica la divulgación de datos personales a un tercero.

c) El tercero receptor de los datos personales puede ser una persona distinta del titular de los datos, del responsable que transfiere y/o del propio encargado del tratamiento.

1. Condiciones para las transferencias de datos personales

Las transferencias de datos personales se sujetan a una serie de reglas específicas para su concreción, entre ellas, la normatividad de los sectores público y privado coinciden al señalar requisitos de naturaleza similar, aunque en ambos casos existen particularidades.

De esta manera, en los siguientes apartados explicaremos las particularidades jurídicas que deben cubrirse para legitimar las transferencias de datos personales en los sectores público y privado.

a) Transferencias de datos personales en el sector privado

En el sector privado encontramos distintas disposiciones que regulan las transferencias:

I. Comunicación del aviso de privacidad: el artículo 36 de la LFPDPPP previene que cuando el responsable del tratamiento pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a estos últimos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento. Así, las transferencias quedan sujetas a que el tratamiento se realice conforme al aviso de privacidad y el tercero receptor deberá asumir las obligaciones previstas en la legislación.[2267]

II. Formalización: la transferencia de datos personales, en correspondencia con lo dispuesto por el artículo 73 del RLFPDPPP,[2268] deberá encontrarse debidamente formalizada entre las partes para demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales, estando ambas partes obligadas a demostrar el cumplimiento de las obligaciones previstas en la normatividad de datos personales.[2269]

III. Consentimiento: el artículo 68 del RLFPDPPP ayuda en la distinción de las diferencias de la transferencia respecto de otras figuras (como la remisión) y señala que la transferencia, por regla general, se encuentra sujeta al consentimiento del titular de los datos (salvo las excepciones previstas en la Ley) y debe estar informada en el aviso de privacidad, así como limitarse a la finalidad concreta que la justifique.[2270]

IV. Excepciones al consentimiento: el artículo 37 de la LFPDPPPP establece los supuestos en los que las transferencias pueden llevarse a cabo sin consentimiento del titular:

2267 En este sentido el RLFPDPPP indica:
Artículo 72. El receptor de los datos personales será un sujeto regulado por la Ley y el presente Reglamento en su carácter de responsable y deberá tratar los datos personales conforme a lo convenido en el aviso de privacidad que le comunique el responsable transferente.

2268 Formalización de las transferencias nacionales
Artículo 73. La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.

2269 Prueba del cumplimiento de las obligaciones en materia de transferencias
Artículo 69. Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realizó conforme a lo que establece la Ley y el presente Reglamento la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.

2270 Condiciones para la transferencia
Artículo 68. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en el artículo 37 de la Ley y deberá ser informada a este último mediante el aviso de privacidad y limitarse a la finalidad que la justifique.

1) cuando la transferencia esté prevista en una ley o tratado en los que México sea parte;
2) cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
3) cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
4) cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
5) cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
6) cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial y
7) cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

b) Transferencias de datos personales en el sector público

En el sector público, el artículo 65 de la LGPDPPSO[2271] previene, como regla general, que las transferencias, ya sean nacionales o internacionales, se encuentran sujetas al consentimiento del titular de los datos, salvo la actualización de las excepciones previstas en la misma norma.[2272]

En relación con las excepciones al consentimiento para la realización de las transferencias en términos de la LGPDPPSO el artículo 70 de dicho dispositivo normativo indica que no será obligado recabar el consentimiento del titular cuando se actualicen las siguientes hipótesis normativas:

I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o tratados internacionales suscritos y ratificados por México.
II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales.

2271 Artículo 65. Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de esta Ley.

2272 En este contexto, la LGPDPPSO indica lo siguiente:
Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:
I. cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;
II. cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
III. cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
IV. para el reconocimiento o defensa de derechos del titular ante autoridad competente;
V. cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
VI. cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VII. cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
VIII. cuando los datos personales figuren en fuentes de acceso público;
IX. cuando los datos personales se sometan a un procedimiento previo de disociación, o
X. cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia.

IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última.

V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados.

VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero.

VIII. Cuando se trate de los casos previstos en el artículo 22 de la LGPDPPSO.

IX. Cuando la transferencia sea necesaria por razones de seguridad nacional.

Así, la LGPDPPSO en su artículo 66 establece que las transferencias deberán formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.

La obligación de formalización de las transferencias no será aplicable cuando:

I. La transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos.

II. La transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.

De la misma forma, debe notarse que en el caso de las transferencias nacionales, el sujeto receptor de los datos personales queda sujeto al cumplimiento de las obligaciones de confidencialidad y respeto al principio de finalidad.[2273]

Finalmente, para que la transferencia de datos personales sea lícita, será necesario que el tercero receptor de los datos se obligue a proteger y dar tratamiento a los datos conforme a las condiciones de la LGPDPPSO[2274] así como a los términos convenidos en el aviso de privacidad.[2275]

2273 Artículo 67. Cuando la transferencia sea nacional, el receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.

2274 Artículo 68. El responsable solo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.

2275 Artículo 69. En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular.

2. Condiciones para las transferencias internacionales de datos personales

En relación con las transferencias internacionales de datos personales debe distinguirse la regulación aplicable al sector privado y al público. Respecto a las comunicaciones de datos, debe destacarse que en el sector privado se señalan reglas particulares en el RLFPDPPP y en el sector público se sujetan a las reglas determinadas para las transferencias nacionales.

A continuación se reseñarán los aspectos distintivos de las transferencias internacionales de acuerdo con la legislación del sector privado.

En primer lugar, el RLFPDPPP establece que independientemente de que las transferencias internacionales pudieran estar exceptuadas de la recolección del consentimiento del titular en razón de lo previsto por el artículo 37 de la LFPDPPP serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales.[2276]

En este contexto, el RLFPDPPP obliga a formalizar las transferencias internacionales de datos personales a través de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.[2277]

Finalmente, el RLFPDPPP señala como elemento de potestad, que el responsable del tratamiento que realiza la o las transferencias pueda solicitar la opinión de la autoridad garante federal (INAI) para determinar si cumplen con los requisitos establecidos en la LFPDPPP y su Reglamento.[2278]

Para la explicación de los aspectos a los que se sujetan las transferencias de datos personales en el sector público, se recomienda consultar el inciso b) de esta definición, pues como decíamos las transferencias internacionales se sujetan a las mismas reglas que las transferencias del orden nacional en la LGPDPPSO.

2276 Artículo 74. Sin perjuicio de lo dispuesto en el artículo 37 de la Ley, las transferencias internacionales de datos personales serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales.

2277 Formalización de las transferencias internacionales
Artículo 75. A tal efecto, el responsable que transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

2278 Opinión del Instituto respecto de las transferencias
Artículo 76. Los responsables, en caso de considerarlo necesario, podrán solicitar la opinión del Instituto para conocer si las transferencias internacionales que realicen cumplen con lo dispuesto por la Ley y el presente Reglamento.

Tratamiento

Isabel Davara Fernández de Marcos,[2279]
Alexis Cervantes Padilla y
Gregorio Barco Vega

El objetivo de la normatividad de protección de datos personales es garantizar al titular de los mismos el tratamiento lícito y legítimo de sus datos personales. El concepto de tratamiento, por tanto, resulta uno de los más trascendentales en la normatividad de datos personales, pues, para empezar, solo partiendo de este concepto podremos delimitar si una actividad específica se encuentra bajo la aplicación de la legislación.

En el ámbito nacional e internacional existen diversas y prolíficas definiciones de "tratamiento", cada una con particularidades pero que en esencia hacen referencia a las actividades que involucran la ejecución de determinados procedimientos o acciones tendientes a la utilización de datos personales por parte del responsable, el encargado del tratamiento o un tercero. A lo largo del presente análisis explicaremos cada una de las definiciones que se encuentran en los textos más relevantes.

En México, el concepto de tratamiento fue incorporado en el plano normativo por primera vez en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) que lo define en la fracción XVIII de la siguiente manera:

> Artículo 3. Para los efectos de esta Ley, se entenderá por:
>
> XVIII. Tratamiento: la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

En la LFPDPPP, por tanto, existen cuatro acciones relacionadas con la utilización de los datos personales: obtención, uso, divulgación y almacenamiento. A continuación explicamos cada una de ellas:

a) Obtención. Se asimila con la recolección de los datos personales. Los datos pueden obtenerse directamente del titular cuando el responsable o su encargado los recolectan de aquel, ya sea de forma personal (cuando hay presencia física de ambas partes) o impersonal (por ejemplo, a través de algún medio de comunicación electrónica). También pueden obtenerse indirectamente del titular, cuando el responsable los recibe de la transferencia de un tercero o de alguna fuente de acceso público.
b) Uso. De acuerdo con la descripción normativa, abarca varias acciones como: acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.
c) Divulgación. Se entiende como la comunicación de datos personales a un tercero. Esta puede llevarse a cabo como una transferencia o una remisión.[2280]
d) Almacenamiento. Se entiende como la acción de reunir, guardar o registrar los datos personales.

La definición también refiere a que las acciones que se consideran tratamientos de datos personales se pueden realizar por cualquier medio, es decir, a través de un soporte físico o electrónico o mediante la aplicación de tecnologías automatizadas o de técnicas manuales.[2281]

2279 Agradecemos el inestimable apoyo de Juan Carlos Salamanca Vázquez, José Ernesto Rodríguez Duque y Alejandra Rojas Apaez para la elaboración de este trabajo.

2280 Para más información, véase la definición de "divulgación" en este diccionario.

2281 En este sentido, en España la Ley Orgánica de Protección de Datos Personales señala: Artículo 3. *Definiciones.*

Como adelantábamos, al definir el tratamiento se está delimitando el ámbito objetivo de aplicación de la normatividad, y así, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) señala:

> Ámbito objetivo de aplicación
>
> Artículo 3. El presente Reglamento será de aplicación al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.
>
> No se aplicarán las disposiciones del presente Reglamento cuando para acceder a los datos personales se requieran plazos o actividades desproporcionadas.
>
> En términos del artículo 3, fracción V de la Ley, los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.

Como vemos, las disposiciones se aplican a tratamientos de datos personales ya sea que estos obren en soportes electrónicos[2282] o en soportes físicos.[2283] Es decir, no resulta determinante el tipo de soporte para establecer la aplicación de la normatividad sino la actualización de los supuestos jurídicos que el artículo 3, fracción XVIII, de la LFPDPPP describe como un tratamiento de datos personales.

En el derecho público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) en la fracción XXXIII de su artículo 3 define al tratamiento de la siguiente manera:

> XXXIII. Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

De esto se desprende que la LGPDPPSO utiliza un acercamiento ligeramente diferente a la definición acuñada por la LFPDPPP. La LGPDPPSO establece que "tratamiento" será la operación (o conjunto de operaciones) efectuadas mediante procedimientos manuales o automatizados aplicados a datos personales. Esta operación (o conjunto de operaciones) se relacionan, a su vez, con una serie de acciones. Dividiremos la definición en tres elementos que explicamos a continuación:

a) Operación o conjunto de operaciones aplicados a datos personales. El término "operación" encuentra en el *Diccionario de la Lengua Española* una definición[2284] relacionada con "datos" que la restringe a las operaciones analíticas de tipo matemático. No obstante, lo más relevante es que esta ejecución se aplica a "datos personales".

A los efectos de la presente Ley Orgánica se entenderá por: [...] c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2282 Artículo 2, fracción X del RLFPDPPP.

2283 Artículo 2, fracción XI del RLFPDPPP.

2284 De acuerdo con el *Diccionario de la Lengua Española* la palabra "operación" tiene las siguientes acepciones:
1.f. Acción y efecto de operar.
2.f. Ejecución de algo.
3.f. Com. Negociación o contrato sobre valores o mercaderías. Operación de bolsa, de descuento.
4.f. Mat. Conjunto de reglas que permiten, partiendo de una o varias cantidades expresiones, llamadas datos, obtener otras cantidades o expresiones llamadas resultados.

b) Efectuados mediante procedimientos manuales o automatizados. Los procedimientos pueden ser manuales si son realizados directamente por personas, o automatizados si se llevan a cabo por sistemas como los computacionales.

c) Operaciones o conjunto de operaciones relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales.

En primer lugar, cabe resaltar que dentro de las operaciones enumeradas se incluyen las mencionadas en la LFPDPPP, obtención, uso, almacenamiento y transferencia. En segundo lugar, están las demás operaciones que podrían encuadrarse dentro de las primeras cuatro, por lo que puede concluirse que en la LFPDPPP también están reguladas todas estas operaciones (el registro, posesión y conservación dentro de almacenamiento; organización, elaboración, utilización, acceso, manejo, aprovechamiento y disposición dentro de uso; comunicación, difusión y divulgación, dentro de transferencia).

El ámbito de aplicación objetivo de la LGPDPPSO se ve determinado por su definición de tratamiento y su artículo cuatro precisa:

> Artículo 4. La presente Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

En el ámbito regional, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos) de forma similar, indican:

> 2. Definiciones
>
> 2.1. Para los efectos de los presentes Estándares se entenderá por:
>
> i. Tratamiento: cualquier operación o conjunto de operaciones efectuadas mediante procedimientos físicos o automatizados realizadas sobre datos personales, relacionadas, de manera enunciativa más no limitativa, con la obtención, acceso, registro, organización, estructuración, adaptación, indexación, modificación, extracción, consulta, almacenamiento, conservación, elaboración, transferencia, difusión, posesión, aprovechamiento y en general cualquier uso o disposición de datos personales.
>
> (Numeral 2.1 Estándares Iberoamericanos).

Sin embargo, encontramos una diferencia importante: el listado de operaciones enumeradas es enunciativa, por lo que, en general, "cualquier uso o disposición de datos personales" deberá considerarse un tratamiento. Como una diferencia menor, señalamos que los Estándares denominan "procedimientos físicos" a lo que nuestra normatividad denomina "procedimientos manuales".

En el panorama internacional, el Reglamento General de Protección de Datos europeo (RGPD o GDPR por sus siglas en inglés) define tratamiento en su artículo 4 como:

> 2) Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Al igual que los Estándares Iberoamericanos, el GDPR enlista el tipo de operaciones de forma enunciativa, lo que permite que cualquier operación realizada sobre protección de datos personales pueda entrar en la definición.

En este sentido, la definición de tratamiento mencionada en el apartado 2) del RGPD es fundamental ya que a partir de esta última se pueden precisar algunas ideas sobre el alcance aplicativo de dicha norma en el que no interesan los medios tecnológicos utilizados para el tratamiento de los datos, ya sean manuales o automatizados, sino el hecho de que se actualice la definición de tratamiento. Así lo previene el artículo 2 del RGPD que fija su ámbito de aplicación con independencia de la naturaleza de los medios empleados para dar tratamiento a los datos.

Respecto de lo anterior, vale la pena destacar que el considerando 15 del RGPD ha señalado que dicho criterio responde a la necesidad de evitar que haya un grave riesgo de elusión y que la protección de las personas físicas debe ser tecnológicamente neutra y no depender de las técnicas utilizadas.[2285]

Finalmente, para resumir la explicación, a continuación se presenta una tabla comparativa del término "tratamiento" en las distintas normatividades analizadas que engloban las diferentes actividades que pueden constituir el tratamiento de los datos:

LFPDPPP	LGPDPPSO	Estándares Iberoamericanos	RGPD
Lista limitativa	Lista limitativa	Lista enunciativa	Lista enunciativa
- obtención - uso - divulgación - almacenamiento	- obtención - uso - registro - organización - conservación - elaboración - utilización - comunicación - difusión - almacenamiento - posesión - acceso - manejo - aprovechamiento - divulgación - transferencia - disposición de datos personales	- obtención - acceso - registro - organización - estructuración - adaptación - indexación - modificación - extracción - consulta - almacenamiento - conservación - elaboración - transferencia - difusión - posesión - aprovechamiento - y en general cualquier uso o disposición de datos personales	- recogida - registro - organización - estructuración - conservación - adaptación o modificación - extracción - consulta - utilización - comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión - limitación - supresión - destrucción

2285 15) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

Tratamiento intensivo de datos personales

María Solange Maqueo Ramírez

El tratamiento intensivo de datos personales supone la concurrencia de dos elementos: (1) que haya un tratamiento de datos personales, esto es, "cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales relacionados con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales"[2286] y (2) que éste sea de tal magnitud o importancia que se considere un riesgo potencial en el tratamiento de datos personales que pudiera representar una grave afectación del derecho a la protección de datos personales, por lo que sus efectos atienden a la generación de medidas preventivas adicionales o reforzadas para quienes tratan datos personales caracterizados como intensivos o relevantes.

Cabe advertir que el término "tratamiento intensivo o relevante" que introduce la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) es tratado de manera diferenciada en otros instrumentos normativos internacionales o de derecho comparado, a pesar de que sus efectos sean análogos. Al respecto, el Reglamento General de Protección de Datos Personales de la Unión Europea, en su artículo 36, hace referencia a un tipo de tratamiento que "entrañe un alto riesgo para los derechos y libertades de las personas".[2287] En términos similares, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos (Estándares Iberoamericanos), aprobados por la Red Iberoamericana de Protección de Datos (RIPD) en el marco del XV Encuentro Iberoamericano de Protección de Datos, en junio de 2017, en su numeral 41.1, se refiere al "tratamiento de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares".

1. Supuestos

El artículo 75 de la LGPDPPSO establece que "se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando: I. Existan riesgos inherentes a los datos personales a tratar; II. Se traten datos personales sensibles, y III. Se efectúen o pretendan efectuar transferencias de datos personales". Además, la propia Ley, en sus artículos 14, fracción XIX y 76, le confiere atribuciones al Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales para emitir criterios adicionales que establezcan aquellos supuestos que importarán un tratamiento de esta naturaleza.

Al respecto, el artículo 8 del acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto en la protección de datos personales desarrolla el contenido del artículo 75 de la citada ley en los siguientes términos:

> Artículo 8. [...], el responsable estará en presencia de un tratamiento intensivo o relevante de datos personales cuando concurra alguna [sic] las siguientes condiciones:
>
> I. Existan riesgos inherentes a los datos personales a tratar, entendidos como el valor potencial cuantitativo o cualitativo que pudieran tener éstos para una tercera persona no autorizada para su posesión o uso en función de la sensibilidad de los datos personales; las categorías de

2286 Artículo 2, fracción XXXIII, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

2287 Reglamento General de Protección de Datos Personales de la Unión Europea, artículo 36.

titulares; el volumen total de los datos personales tratados; la cantidad de datos personales que se tratan por cada titular; la intensidad o frecuencia del tratamiento, o bien, la realización de cruces de datos personales con múltiples sistemas o plataformas informáticas;

II. Se traten datos personales sensibles [...], entendidos como aquellos que se refieran a la esfera más íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

III. Se efectúen o pretendan efectuar transferencias de datos personales [...], entendidas como cualquier comunicación de datos personales, dentro o fuera del territorio mexicano, realizada a persona distinta del titular, responsable o encargado, considerando con especial énfasis, de manera enunciativa mas no limitativa, las finalidades que motivan éstas y su periodicidad prevista; las categorías de titulares; la categoría y sensibilidad de los datos personales transferidos; el carácter nacional y/o internacional de los destinatarios o terceros receptores y la tecnología utilizada para la realización de éstas.

El artículo 9 del citado acuerdo establece otros criterios adicionales que configuran tratamientos intensivos de manera particular:

Artículo 9. [...] el responsable está en presencia de un tratamiento de intensivo o relevante de datos personales, de manera particular, cuanto pretenda:

I. Cambiar la o las finalidades que justificaron el origen de determinado tratamiento de datos personales, de tal manera que pudiera presentarse una incompatibilidad entre las finalidades de origen con las nuevas finalidades, al ser estas últimas más intrusivas para los titulares.

II. Evaluar, monitorear, predecir, describir, clasificar o categorizar la conducta o aspectos análogos de los titulares, a través de la elaboración de perfiles determinados para cualquier finalidad, destinados a producir efectos jurídicas que los vinculen o afecten de manera significativa, especialmente, cuando a partir de dicho tratamiento se establezcan o pudieran establecerse diferencias de trato o un trato discriminatorio económico, social, político, racial, sexual o de cualquier otro tipo que pudiera afectar la dignidad o integridad personal de los titulares.

III. Tratar datos personales de grupos vulnerables atendiendo, de manera enunciativa más no limitativa, a su edad; genero; origen étnico o racial; estado de salud; preferencia sexual; nivel de instrucción y condición socioeconómica.

IV. Crear bases de datos concernientes a un número elevado de titulares, aun cuando dichas bases no estén sujetas a criterios determinados en cuanto a su creación o estructura, de tal manera que se produzca la acumulación no intencional de una gran cantidad de datos personales respecto de los mismos.

V. Incluir o agregar nuevas categorías de datos personales a las bases de datos ya existentes y en posesión del responsable, de tal forma que, en caso de presentarse una vulneración de seguridad por la cantidad de información contenida en ellas, pudiera derivarse una afectación a la esfera personal de los titulares, sus derechos o libertades.

VI. Realizar un tratamiento frecuente y continúo de grandes volúmenes de datos personales, o bien, llevar a cabo cruces de información con múltiples sistemas o plataformas informáticas.

VII. Utilizar tecnologías con sistemas de vigilancia; aeronaves o aparatos no tripulados; minería de datos; biometría; Internet de las cosas; geolocalización; técnicas analíticas; radiofrecuencia o cualquier otra que pueda desarrollarse en el futuro y que implique un tratamiento de datos personales a gran escala.

VIII. Permitir el acceso de terceros a una gran cantidad de datos personales que anteriormente no tenían acceso, ya sea, entregándolos, recibiéndolos y/o poniéndolos a su disposición en cualquier forma.

IX. Realizar transferencias internacionales de datos personales a países que no cuenten en su derecho interno con garantías suficientes y equivalentes para asegurar la debida protección de los datos personales, conforme al sistema jurídico mexicano en la materia.

X. Revertir la disociación de datos personales para la consecución de finalidades determinadas, especialmente si éstas son de carácter intrusivo o invasivo al titular.

XI. Tratar datos personales sensibles con la finalidad de efectuar un tratamiento sistemático y masivo de los mismos.

XII. Realizar una evaluación sistemática y exhaustiva de aspectos propios de las personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para éstas o que les afecten significativamente de modo similar.

XIII. Realizar un tratamiento a gran escala de datos personales sensibles o datos personales relativos a condenas e infracciones penales.

XIV. La observación sistemática a gran escala de una zona de acceso público.

2. Efectos

De conformidad con los artículos 74 y 85 de la LGPDPPSO, el tratamiento intensivo o relevante de datos personales entraña dos consecuencias principales para el responsable del tratamiento de datos personales, (1) la realización y presentación ante el órgano garante competente de evaluaciones de impacto en la protección de datos personales, cuando pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen este tipo de tratamiento y (2) la designación, de manera potestativa, de un oficial de protección de datos personales, especializado en la materia, que sea parte de su unidad de transparencia.

Finalmente cabe decir que dado el carácter no exhaustivo de los supuestos previstos para categorizar un tratamiento de datos personales como intensivo o relevante, los responsables pueden realizar consultas a los órganos garantes competentes, en términos del artículo 12 del citado Acuerdo del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, a fin de recibir una opinión técnica que confirme o niegue su obligación de elaborar y presentar una evaluación de impacto en la protección de datos personales. De tal forma que ante cualquier duda respecto de si se está o se podría estar ante un tratamiento intensivo o relevante de datos personales resulta conveniente acudir ante los órganos garantes competentes, con el objeto de evitar caer en un incumplimiento de la ley.

NOTAS

NOTAS

NOTAS

NOTAS

Unidad de transparencia

María Marván Laborde

Las unidades de transparencia son las unidades administrativas que tienen como objetivo principal hacer las gestiones necesarias al interior de cada sujeto obligado para lograr que funcionen adecuadamente la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). En el caso de la Federación, también se encargan de la implementación de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP). En cada una de las entidades, la ley local correspondiente establece las funciones de las unidades de transparencia. Debido a la exhaustividad de la LGTAIP, la Ley Federal y las de las entidades suelen repetir lo que establece la primera, la Ley General.

Las principales funciones de las unidades de transparencia están en el artículo 45 de la LGTAIP. Entre ellas se encuentra la responsabilidad del cumplimiento cabal de las obligaciones de transparencia (fracción I), para ello deberán recabar y difundir la información a la que se refieren los siguientes capítulos del título quinto de la Ley: capítulo II "De las obligaciones de Transparencia Comunes", que consta de 48 fracciones; capítulo III "De las Obligaciones de Transparencia Específicas de los Sujetos Obligados", capítulo IV "De las Obligaciones Específicas de las Personas Físicas o Morales que Reciben y Ejercen Recursos Públicos o Ejercen Actos de Autoridad" y capítulo V "De las Obligaciones Específicas en Materia Energética", (artículos del 70 al 88).

Podemos considerar que las unidades de transparencia son la puerta de entrada de todas las solicitudes de acceso a la información y por tanto, a través de ellas, los sujetos obligados entablan contacto inmediato con el solicitante para hacer llegar las solicitudes a las diversas áreas que pudieran dar respuesta a su solicitud. Es menester que el titular de la unidad de transparencia tenga un conocimiento claro de la institución en la que trabaja para poder dirigir las solicitudes de acceso a la información a todas las áreas pertinentes. La unidad deberá hacer todos los trámites internos para conseguir la información y será quien envíe a los solicitantes las notificaciones necesarias del proceso (admisión, prevención, ampliación de plazos, cuando estas hayan sido aprobadas por el comité de transparencia y, finalmente, las respuestas). (Fracciones II, IV y V).

Para poder cumplir con sus funciones de tramitar las solicitudes de acceso a la información y mantener actualizadas las obligaciones de transparencia, es indispensable que la

unidad de transparencia cuente con el apoyo institucional de todas y cada una de las unidades administrativas del sujeto obligado, es por ello que se establece, en la fracción VII, la facultad de proponer el personal habilitado que pueda dar trámite a las solicitudes. Este es personal, propio de cada área, conoce el funcionamiento y por tanto tiene habilidades claras para localizar y organizar la información.

El principio de máxima publicidad no solo es importante al clasificar la información, podemos encontrar obligaciones que se desprenden de éste a lo largo de la LGTAIP, una de ellas consiste en la obligación de las unidades de transparencia de auxiliar a los particulares en la elaboración de solicitudes de acceso a la información y orientarlos sobre los sujetos competentes que, en todo caso, podrían satisfacer sus inquietudes. (Fracción III).

Las unidades de transparencia son responsables de la gestión de solicitudes, y por tanto, deben llevar un registro de las mismas en el que dé cuenta de las solicitudes recibidas, respondidas, las notificaciones a los particulares, los costos de reproducción y el envío de la información en su caso. (Fracción VIII).

Cuando una unidad de transparencia no responda satisfactoriamente una solicitud —ya sea porque argumente no ser competente, por la inexistencia de la información o pretenda que la información sea clasificada como reservada o confidencial en términos de las leyes aplicables— es obligación de las unidades de transparencia someter la respuesta a la consideración del comité de transparencia. Usualmente el titular de la unidad de transparencia ocupa un lugar en dicho comité, sin embargo, esto no es una definición legal, a veces puede tener un lugar con voz pero sin voto y esa es una decisión interna de cada sujeto obligado.

Al igual que todas las autoridades coadyuvantes de la transparencia, el acceso a la información y la protección de datos personales, las leyes establecen que las unidades de transparencia deben trabajar en la promoción e implementación de sendas políticas públicas al interior de la institución en la que trabajan. (Fracción X).

Por su parte, la LFTAIP, en su artículo 11, establece que todos los sujetos obligados deben contar con un comité de transparencia y una unidad de transparencia. Debido a que el nivel jerárquico del titular de la unidad de transparencia es considerado crucial para la buena implementación de la ley, es mandatorio que éste sea nombrado de manera directa por el titular del sujeto obligado, así mismo, se le obliga al titular a tomar las previsiones necesarias para proporcionar capacitación de manera continua y especializada al personal que forme parte de los comités de transparencia y unidades de transparencia, es decir a los servidores públicos encargados directamente de hacer operativas las disposiciones legales en esta materia.

El personal de la unidad de transparencia tiene la responsabilidad de hacer del conocimiento de la instancia competente y el superior jerárquico la probable responsabilidad por el incumplimiento de las obligaciones que estas leyes imponen a cada servidor público dentro de su institución.

Para garantizar el acceso a la información a la población indígena, invidentes o cualquier otro grupo demográfico que pudiese encontrarse en una situación de desventaja, las unidades de transparencia deberán promover acuerdos o convenios con aquellas instituciones que pudieran coadyuvar a garantizarles el acceso a la información. También es mandato de ley que físicamente las unidades de transparencia se encuentren en lugares visibles y accesibles al público en general.

Llama la atención que ni la LGTAIP ni la LFTAIP establecen como función de las unidades de transparencia dar trámite a las solicitudes de los particulares para el ejercicio de los derechos ARCO en materia de protección de datos personales, tampoco lo hace la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), la única mención que encontramos en esta ley a las unidades de transparencia se encuentra en el cuarto párrafo del artículo 50, que dice lo siguiente:

> La información deberá ser entregada sin costo, cuando implique la entrega de no más de 20 hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.

Sin embargo, de la lectura sistemática de las tres leyes queda claro que los órganos garantes de la transparencia y la protección de datos personales son autoridad en esta materia. Los sujetos obligados establecidos en la LGTAIPG son responsables de garantizar el eficiente ejercicio de los derechos ARCO de los particulares. Esto queda demostrado porque la Plataforma Nacional de Transparencia y Protección de Datos Personales se encuentra habilitada para recibir solicitudes de derechos ARCO. Vale la pena mencionar que se hace la advertencia de que en el Estado de México, Nayarit y Veracruz aún no contemplan la posibilidad de ejercer estos derechos a pesar de que la LGPDPPSO lo mandata indubitablemente.

Para subsanar esta omisión, el INAI emitió el acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el sector público, este acuerdo fue publicado el 19 de diciembre de 2017 y en sus artículos 84 al 107 establece con claridad todas las funciones y pasos que se deben seguir en las instituciones del sector público para que las personas puedan ejercer los derechos ARCO, destaca el papel central de las unidades de transparencia como la unidad administrativa que sirve de enlace entre el particular que quiere ejercer cualquiera de los derechos de acceso, rectificación, cancelación u oposición con el resto de la institución y por supuesto en caso de que el particular entable una queja frente al INAI la unidad de transparencia será responsable del proceso.

NOTAS

Vida privada

Eduardo Ferrer Mac-Gregor Poisot

El derecho a la vida privada es un derecho de la personalidad[2288] que protege a las personas de no ser interferidos en aquellas actividades que se reservan al ámbito personal y que se excluyen del escrutinio de la actividad pública. Este concepto se ha relacionado con lo que no constituye vida pública, el ámbito reservado frente a la acción y el conocimiento de los demás, lo que se desea compartir únicamente con aquellos que uno elige, las actividades de las personas en la esfera particular, relacionadas con el hogar y la familia, o aquello que las personas no desempeñan con el carácter de servidores públicos.[2289]

De acuerdo con Villanueva, se entiende por vida privada "la prerrogativa de los gobernados, que consiste en no ser interferidos o molestados por persona o entidad alguna en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público".[2290] El derecho a la vida privada, según el referido autor, se materializa en el momento de proteger del conocimiento ajeno el hogar, la oficina o el ámbito laboral, los expedientes médicos, legales y personales, las conversaciones o reuniones privadas, la correspondencia por cualquier medio, la intimidad sexual, la convivencia familiar o afectiva y todas las actividades y conductas que se realizan en lugares no abiertos al público.[2291]

La Primera Sala de la SCJN ha destacado que el concepto "vida privada" comprende a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, esto es, la vida privada es lo genéricamente reservado y la intimidad —como parte de aquélla— lo radicalmente vedado, lo más personal

2288 Los llamados derechos de la personalidad, que también se denominan derechos sobre la propia persona, individuales o personalísimos, constituyen un tipo singular de facultades reconocidas a las personas físicas para el aprovechamiento legal de diversos bienes derivados de su propia naturaleza somática, de sus cualidades espirituales y, en general, de las proyecciones integrantes de su categoría humana. *Vid*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. (2000). *Enciclopedia Jurídica Mexicana*. Tomo III D-E. Editorial Porrúa. México, pp. 408-410.

2289 Tesis: 1a. CCXIV/2009. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXX. Diciembre de 2009, p. 277.

2290 Villanueva, E. (2014). "Derecho a la vida privada", en Ferrer Mac-Gregor, Eduardo, Martínez Ramírez, Fabiola, *et al.,* (coord.), *Diccionario de derecho procesal constitucional y convencional*, 2a. ed. México. Instituto de investigaciones Jurídicas Universidad Nacional Autónoma de México, p. 385.

2291 Villanueva, E. (2014). "Derecho a la vida privada", en Ferrer Mac-Gregor, Eduardo, Martínez Ramírez, Fabiola, *et al.,* (coord.), *Diccionario de derecho procesal constitucional y convencional*, 2a. ed. México. Instituto de investigaciones Jurídicas Universidad Nacional Autónoma de México, p. 385.

y de ahí que, si bien son derechos distintos, al formar parte uno del otro, cuando se afecta la intimidad, se agravia a la vida privada.[2292]

El derecho a la vida privada es "el derecho fundamental de los individuos que consiste en no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público". [2293]

El derecho a la vida privada está definido con alcance normativo en la Ley de Responsabilidad Civil para La Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal (Ley de Responsabilidad Civil del Distrito Federal), misma que señala en su artículo 9 que se entiende como vida privada "aquella que no está dedicada a una actividad pública y que, por ende, es intrascendente y sin impacto en la sociedad de manera directa, y en donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia ni les afecta".[2294]

La Ley de Responsabilidad Civil del Distrito Federal indica también que este derecho se materializa al momento que se protege del conocimiento ajeno a la familia, domicilio, papeles o posesiones y todas aquellas conductas que se llevan a efecto en lugares no abiertos al público, cuando no son de interés público o no se han difundido por el titular del derecho.[2295] Finalmente, la citada ley también previene que, como parte de la vida privada se tendrá derecho a la intimidad.[2296]

1. Contenido

El derecho a la vida privada protege —dentro del ámbito de las relaciones familiares— a aquellas decisiones que solo conciernen a la familia y en las cuales el Estado no puede intervenir injustificadamente.[2297] Este derecho, según Villanueva, contiene algunas peculiaridades que es conveniente puntualizar: a) es un derecho esencial inherente del individuo, independientemente del sistema jurídico particular o contenido normativo con el que está tutelado por el derecho positivo; b) es un derecho extra patrimonial, que no puede comerciarse o intercambiarse como los derechos de crédito, pues forma parte de la personalidad jurídica del individuo, razón por la que es intransmisible e irrenunciable y c) es un derecho imprescriptible e inembargable.[2298]

Además, el Tribunal Europeo de Derechos Humanos ha señalado que la noción de "vida privada" comprende elementos que hacen referencia a la identidad de la persona tales como el nombre, su foto, su integridad física y moral, y que la garantía que ofrece el artículo 8 del Convenio está destinada principalmente a asegurar el desarrollo, —sin inje-

2292 Tesis: 1a. CXLIX/2007. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVI. Julio de 2007, p. 272.

2293 Villanueva E. y Gómez P. (2012). *Libertad de expresión en Latinoamérica*. Novum. México, p. 52.

2294 Artículo 9. Es vida privada aquella que no está dedicada a una actividad pública y, que por ende, es intrascendente y sin impacto en la sociedad de manera directa; y en donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia ni les afecta.

2295 Artículo 10. El derecho a la vida privada se materializa al momento que se protege del conocimiento ajeno a la familia, domicilio, papeles o posesiones y todas aquellas conductas que se llevan a efecto en lugares no abiertos al público, cuando no son de interés público o no se han difundido por el titular del derecho.

2296 Artículo 11. Como parte de la vida privada se tendrá derecho a la intimidad que comprende conductas y situaciones que, por su contexto y que por desarrollarse en un ámbito estrictamente privado, no están destinados al conocimiento de terceros o a su divulgación, cuando no son de interés público o no se han difundido por el titular del derecho.

2297 Tesis: 1a. CCXI/2017 (10a.). Décima época. *Semanario Judicial de la Federación*. Libro 49. Diciembre de 2017. Tomo I, p. 407.

2298 Villanueva, E. (2014). "Derecho a la vida privada", en Ferrer Mac-Gregor, Eduardo, Martínez Ramírez, Fabiola, *et al.*, (coords.). *Diccionario de derecho procesal constitucional y convencional*. 2a. ed. México. Instituto de investigaciones Jurídicas Universidad Nacional Autónoma de México, p. 385.

rencias externas— de la personalidad de cada individuo en la relación con sus semejantes. Existe, por tanto, una zona de interacción entre el individuo y los demás que incluso en un contexto público, puede formar parte de la "vida privada".[2299]

En cuanto al núcleo de su protección, el bien jurídicamente protegido de este derecho, según Villanueva, "está constituido por la necesidad social de asegurar la tranquilidad y la dignidad necesaria para el libre desarrollo del ser humano, a fin de que cada quien pueda llevar a cabo su proyecto vital". [2300] Su intromisión, en términos de lo previsto por el Código Civil Federal, dará lugar a una reclamación de reparación por daño moral.[2301] Sin embargo, este derecho no reviste un carácter absoluto ya que puede ceder ante determinadas circunstancias.

En cuanto a los supuestos en los que puede ceder el derecho a la vida privada destacan aquellos relacionados con personas públicas. Mientras que un particular desconocido para el público puede aspirar a una protección especial de su derecho a la vida privada, no sucede lo mismo con las personas públicas,[2302] pues deben resistir mayor nivel de injerencia en su intimidad que las personas privadas o particulares, al existir un interés legítimo por parte de la sociedad de recibir y de los medios de comunicación de difundir información sobre ese personaje público, en aras del libre debate público.[2303]

Un caso paradigmático que evidencia esta afirmación (y que demuestra además que encontrar respuesta a estos problemas de esta dimensión puede resultar muy complejo) es el de la princesa Carolina de Hannover, quien invocando la protección a sus derechos de privacidad (primero en tribunales alemanes y luego ante el Tribunal Europeo de Derechos Humanos) intentó evitar la publicación de fotografías tomadas sin su autorización por la prensa mientras vacacionaba, y en la que se hacía referencia a los problemas de salud del padre de Carolina, el príncipe Rainiero III de Mónaco.

En sede interna, los tribunales alemanes (esto es, tanto la Corte Federal de Justicia, *Bundesgerichtshof*, como el Tribunal Constitucional Federal, *Bundesverfassungsgericht*), invocaron el concepto de "figura de la sociedad contemporánea por excelencia" para justificar la intrusión en la vida privada que ejerce funciones oficiales y cuya publicación contribuye a un debate de interés general, porque la salud del príncipe de Mónaco era un tema sobre el que la prensa legítimamente podía publicar por ser de interés general. En contraste, la Tercera Sala del Tribunal Europeo de Derechos Humanos, en su decisión de 2004,[2304] consideró inapropiado invocar dicho concepto en este caso para dar debido cumplimiento a la obligación de garantizar una efectiva protección del derecho al respeto de la vida privada establecido convencionalmente, en particular, si la intrusión de la vida privada de una persona no está relacionado con el ejercicio de funciones oficiales y solo tiene por

2299 Tribunal Europeo de Derechos Humanos casos "Schüssel vs. Austria". Número 42409/1998, 21 febrero 2002. Von Hannover, aps. 50 y 53 y Sciacca, ap. 29, previamente mencionadas y "Petrina vs. Rumanía", número 78060/2001, ap. 28, 14 octubre 2008.

2300 Villanueva, E. (2014). "Derecho a la vida privada", en Ferrer Mac-Gregor, Eduardo, Martínez Ramírez, Fabiola, *et al.,* (coords.). *Diccionario de derecho procesal constitucional y convencional*. 2a. ed. México. Instituto de investigaciones Jurídicas Universidad Nacional Autónoma de México, p. 385.

2301 Artículo 1916. Por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, o bien en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas.

2302 "Minelli vs. Suiza" (Dec.). Número 14991/2002, 14 junio 2005, y Petrenco, previamente mencionada, ap. 55

2303 Tesis: 1a. XLI/2010. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXXI. Marzo de 2010, p. 923.

2304 ECTHR, *Von Hannover vs. Alemania*, sentencia de 7 de Febrero de 2012, RJD 2004-VI, 41.

objeto satisfacer la curiosidad pública, pues en el caso quedó constancia de que dicha persona, si bien era figura pública, en esos momentos se encontraba en un lugar aislado con el objetivo de desarrollar actividades familiares y la publicación de esas fotografías y el artículo respectivo no contribuía de modo alguno al debate público propio de una sociedad democrática.

Finamente, es importante citar que el derecho a la vida privada, además, se encuentra correlacionado con otros derechos fundamentales elevados a rango constitucional, como el derecho al honor (a modo de referencia, se remite a la lectura de la voz "derecho al honor" en esta misma obra) y el derecho de réplica, que "es una garantía que permite proteger la dignidad del individuo frente a intervenciones arbitrarias o ilegales en su vida privada, así como ataques a su honra o reputación".[2305]

2. Reconocimiento constitucional y en tratados internacionales

En México, el derecho a la vida privada está regulado por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), cuyo primer párrafo establece:

> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.

Este derecho protege, dentro del ámbito de las relaciones familiares, a aquellas decisiones que solo conciernen a la familia y en las cuales el Estado no puede intervenir injustificadamente.[2306]

El derecho a la vida privada también figura en el primer párrafo del artículo sexto de la CPEUM como un límite a las libertades de expresión y comunicación:

> Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

En un sentido amplio, la protección constitucional de la vida privada implica poder conducir parte de la vida protegido de la mirada y las injerencias de los demás y guarda conexiones de variado tipo con pretensiones más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos: el derecho de poder tomar libremente ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular.[2307]

Además de estar previsto en la CPEUM, existen diversos tratados internacionales que reconocen el derecho humano a la vida privada y familiar. Entre ellos destacan los siguientes instrumentos.

2305 *Cfr.*, Otálora, J. (2013). "El derecho de réplica. Artículo 6 de la Constitución Política de los Estados Unidos Mexicanos", en *Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana*. México, SCJN-UNAM. Instituto de Investigaciones Jurídicas-Fundación Konrad Adenauer. Tomo II, p. 1084.

2306 Tesis: 1a. CCXI/2017 (10a.). Décima época. *Semanario Judicial de la Federación*. Libro 49. Diciembre de 2017. Tomo I, p. 407.

2307 Tesis: 1a. CCXIV/2009. Novena época. *Semanario Judicial de la Federación y su Gaceta*. Tomo XXX. Diciembre de 2009, p. 277.

La Declaración Universal de Derechos Humanos tutela este derecho en su artículo 12, al reconocer lo siguiente:

> Artículo 12.
>
> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

La Convención Americana sobre Derechos Humanos en su artículo 11 dispone lo siguiente:

> Artículo 11. Protección a la honra y de la dignidad
>
> Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
>
> Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
>
> Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticas precisa lo siguiente:

> ARTÍCULO 17.-
>
> Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
>
> Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

La Convención de Derechos del Niño, en su artículo 16, previene lo siguiente:

> Artículo 16
>
> 1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.
>
> 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

Según esta noción, las personas tienen derecho a gozar de un ámbito de proyección de su existencia que quede reservado de la invasión y la mirada de los demás, que les concierna solo a ellos y les provea de condiciones adecuadas para el despliegue de su individualidad (para el desarrollo de su autonomía y su libertad).[2308]

3. Desarrollo en resoluciones de la Corte Interamericana de Derechos Humanos

El derecho a la vida privada ha sido estudiado de la mano con el derecho al honor y en contraposición con las libertades de prensa y expresión en diversos fallos emitidos por la Corte Interamericana de Derechos Humanos (Corte IDH):

A. Caso "Escher y otros vs. Brasil"

En el caso "Escher y otros vs. Brasil" se imputó responsabilidad internacional al Estado de Brasil por la interceptación, monitoreo y divulgación de conversaciones telefónicas de diversos ciudadanos por parte de la policía militar del estado de Paraná. Los hechos del presente caso se producen en un contexto de conflicto social relacionado con la reforma agraria en varios estados de Brasil, entre ellos Paraná.[2309]

En relación con el derecho a la vida privada, la Corte IDH ha declarado que incluye diversos ámbitos de la vida de las personas y que el mismo se caracteriza por estar exento

2308 Tesis: 1a. CCXIV/2009. Novena época. Semanario Judicial de la Federación y su Gaceta. Tomo XXX. Diciembre de 2009, p. 277.

2309 Caso "Escher y otros vs. Brasil". Disponible en: http://www.corteidh.or.cr/cf/Jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=277&lang= Fecha de consulta: el 21 de agosto de 2018.

de intromisiones: "13. El artículo 11 de la Convención prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, enunciando diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias". En ese sentido, la Corte ha sostenido que "el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública".

En cuando a su concreción práctica, la Corte IDH destacó lo siguiente: "En definitiva, la protección a la vida privada se concreta en el derecho a que sujetos distintos de los interlocutores no conozcan ilícitamente el contenido de las conversaciones telefónicas o de otros aspectos, como los ya mencionados, propios del proceso de comunicación".

La Corte IDH también distingue que la divulgación de cintas grabadas constituyó una violación a la privacidad de las víctimas: "La divulgación de las cintas grabadas configuró una violación del derecho a la honra y a la dignidad de toda persona, en el cual se incluye su privacidad, según el artículo 11 de la Convención Americana, leído en conjunto con los artículos 30 y 32.2 del mismo instrumento".

La Corte IDH resolvió que: "2. El Estado violó el derecho a la vida privada y el derecho a la honra y a la reputación reconocidos en el artículo 11 de la Convención Americana, en relación con el artículo 1.1 de la misma, en perjuicio de los señores Arlei José Escher, Dalton Luciano de Vargas, Delfino José Becker, Pedro Alves Cabral y Celso Aghinoni, por la interceptación, la grabación y la divulgación de sus conversaciones telefónicas, en los términos de los párrafos 125 a 146 y 150 a 164 de la presente sentencia".[2310]

B. "Caso de las masacres de Ituango vs. Colombia"[2311]

El caso se refiere a la responsabilidad internacional del Estado por los actos de tortura y asesinato de pobladores en el municipio de Ituango, así como a la falta de investigación para esclarecer los hechos y sancionar a los responsables.[2312]

En relación con la violación al derecho a la vida privada, la Corte IDH señaló lo siguiente: "192. La Corte ha considerado que en el presente caso se consumó una violación de especial gravedad del derecho a la propiedad privada por la quema de los domicilios de los pobladores de El Aro (*supra* párrafo 182). Debido a las consideraciones señaladas anteriormente, y en virtud del desarrollo del derecho internacional de los derechos humanos en esta materia, este tribunal considera necesario hacer algunas precisiones adicionales sobre la inviolabilidad del domicilio y la vida privada, desde la perspectiva del artículo 11.2 de la Convención".

En lo relativo al alcance del derecho a la vida privada, la Corte IDH indica lo siguiente: "194. La Corte considera que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. En este sentido, el domicilio y la vida privada se encuentran intrínsecamente ligados, ya que el domicilio se convierte en un espacio en el cual se puede desarrollar libremente la vida privada".

En este caso, la Corte IDH hizo referencia a casos resueltos en el ámbito europeo: 195. La Corte Europea de Derechos Humanos, en casos sobre hechos similares a los del caso *sub judice*, ha tra-

2310 Cfr. Corte IDH. Caso "Escher y otros vs. Brasil". Excepciones Preliminares. Fondo, reparaciones y costas. Sentencia de 6 de julio de 2009. Serie C. No. 200.

2311 Corte IDH. "Caso de las Masacres de Ituango vs. Colombia". Sentencia de 1 de julio de 2006. Serie C. No. 148.

2312 Ficha Técnica: Masacres de "Ituango vs. Colombia". Disponible en: http://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=330. Fecha de consulta: 23 de agosto de 2018.

tado el tema de la propiedad privada conjuntamente con el derecho al respeto de la vida privada y familiar y del domicilio, lo cual es garantizado por el artículo 8 del Convenio Europeo de Derechos Humanos / 196. De manera ilustrativa, este tribunal considera pertinente señalar que, en el caso "Ayder vs. Turquía", la Corte Europea estableció que, en circunstancias similares a los hechos del presente caso, la destrucción deliberada de domicilios y otras propiedades por parte de las fuerzas armadas turcas, lo cual causó que las víctimas se vieran obligadas a abandonar el pueblo, constituyó una interferencia grave e injustificada en la vida privada y familiar y en el uso y disfrute pacífico de sus posesiones. En el mismo sentido, en el caso "Bilgin vs. Turquía", el Tribunal Europeo declaró una violación del derecho a la propiedad privada conjuntamente con el derecho al respeto de la vida privada y familiar y del domicilio debido al incendio provocado por las fuerzas de seguridad turcas que destruyó la vivienda y posesiones de la víctima, la cual, al verse privada de su sustento, se vio forzada a desplazarse. Igualmente, en el caso "Selçuk y Asker vs. Turquía", la Corte Europea reconoció que la deliberada destrucción por parte de las fuerzas de seguridad del ejército turco de la propiedad de las víctimas, las cuales fueron obligadas a abandonar su lugar de residencia, constituyó una violación de los derechos a la propiedad privada, así como una injerencia abusiva o arbitraria en las vidas privadas y en el domicilio de ellas.

Finalmente, la Corte IDH consideró que la destrucción de los domicilios de los habitantes constituye una violación grave al derecho a la vida privada y al domicilio: "197. En el presente caso, reconociendo los avances en esta materia en el derecho internacional de los derechos humanos, y por las consideraciones anteriores, la Corte estima que la destrucción por parte de los paramilitares, con la colaboración del Ejército colombiano, de los domicilios de los habitantes de El Aro, así como de las posesiones que se encontraban en su interior, además de ser una violación del derecho al uso y disfrute de los bienes, constituye asimismo una grave, injustificada y abusiva injerencia en su vida privada y domicilio. Las presuntas víctimas que perdieron sus hogares perdieron también el lugar donde desarrollaban su vida privada. Por lo anterior, el Tribunal considera que el Estado colombiano incumplió con la prohibición de llevar a cabo injerencias arbitrarias o abusivas en la vida privada y el domicilio".

C. Caso "Tristán Donoso vs. Panamá"[2313]

El caso se refiere a la responsabilidad internacional del Estado por la divulgación de una conversación telefónica de Santander Tristán Donoso, así como por la condena penal impuesta debido a sus declaraciones.[2314]

En el Caso "Tristán Donoso vs. Panamá", la Corte IDH en relación con el derecho a la vida privada destacó, en primer lugar, que este derecho se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública: "55. El artículo 11 de la Convención prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, enunciando diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias. La Corte ha sostenido que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. Aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección del derecho a la vida privada".[2315]

2313 Corte IDH. Caso "Tristán Donoso vs. Panamá". *Convocatoria de audiencia*. Resolución de la presidenta de la Corte Interamericana de Derechos Humanos de 9 de junio de 2008.

2314 Ficha Técnica: "Tristán Donoso vs. Panamá". Disponible en: http://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=253. Fecha de consulta: 23 de agosto de 2018.

2315 *Cfr.* Corte IDH. Caso "Tristán Donoso vs. Panamá". *Excepción Preliminar, fondo, reparaciones y costas*. Sentencia de 27 de enero de 2009 Serie C. No. 193, párrafo 55.

En lo que respecta al alcance del derecho a la vida privada, la Corte IDH destacó: "56. El derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias; por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática".[2316]

Finalmente, la Corte IDH destacó que existió una injerencia arbitraria en la vida privada y, en los siguientes términos, estableció los requisitos que deben revestir dichas afectaciones a la vida privada: "76. La divulgación de la conversación telefónica por parte de un funcionario público implicó una injerencia en la vida privada del señor Tristán Donoso. La Corte debe examinar si dicha injerencia resulta arbitraria o abusiva en los términos del artículo 11.2 de la Convención o si resulta compatible con dicho tratado. Como ya se indicó (…), para ser compatible con la Convención Americana una injerencia debe cumplir con los siguientes requisitos: estar prevista en ley, perseguir un fin legítimo, y ser idónea, necesaria y proporcional. En consecuencia, la falta de cumplimiento de alguno de dichos requisitos implica que la medida es contraria a la Convención".[2317]

D. Caso "D'Amico y Fontevecchia vs. Argentina"[2318]

El caso se refiere a la responsabilidad internacional del Estado por la sanción judicial impuesta a Jorge Fontevecchia y Hector D'Amico debido a una publicación que supuestamente habría afectado la vida privada del entonces presidente de Argentina.[2319]

En lo que concierne al derecho a la vida privada, la Corte IDH destacó que este derecho tiene el siguiente alcance: "28. Por su parte, el artículo 11 de la Convención Americana reconoce que toda persona tiene, entre otros, derecho a la vida privada y prohíbe toda injerencia arbitraria o abusiva en ella, enunciando diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias. El ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública y comprende, entre otras dimensiones, tomar decisiones relacionadas con diversas áreas de la propia vida libremente, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público".[2320]

Respecto de la concepción del derecho a la privacidad, la Corte IDH menciona: "48. Por su parte, el artículo 11 de la Convención Americana reconoce que toda persona tiene, entre otros, derecho a la vida privada y prohíbe toda injerencia arbitraria o abusiva en ella, enunciando diversos ámbitos de la misma como la vida privada de sus familias, sus domicilios o sus correspondencias. El ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública y comprende, entre otras dimensiones, tomar decisiones relacionadas con diversas áreas de la propia vida libremente, tiene un espacio de tranquilidad

2316 *Cfr.* Corte IDH. Caso "Tristán Donoso vs. Panamá". *Excepción Preliminar, fondo, reparaciones y costas*. Sentencia de 27 de enero de 2009 Serie C. No. 193, párrafo 56.

2317 *Cfr.* Corte IDH. Caso "Tristán Donoso vs. Panamá". *Excepción Preliminar, fondo, reparaciones y costas*. Sentencia de 27 de enero de 2009 Serie C. No. 193, párrafo 76.

2318 Corte IDH. Caso "Fontevecchia y D`Amico vs. Argentina". Convocatoria de audiencia. Resolución del presidente de la Corte Interamericana de Derechos Humanos de 27 de julio de 2011.

2319 Ficha Técnica: "Fontevecchia y D'amico vs. Argentina". Disponible en: http://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191 Fecha de consulta: 23 de agosto de 2018.

2320 Corte IDH. Caso "Fontevecchia y D'Amico vs. Argentina". *Fondo, reparaciones y costas*. Sentencia de 29 de noviembre de 2011. Serie C. No. 238, párrafo 28.

personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público".[2321]

En cuanto a la obligación de los Estados de garantizar el derecho a la vida privada y adoptar medidas para su protección, la Corte IDH indicó: "49. El artículo 11.2 de la Convención Americana protege al individuo frente a la posible interferencia arbitraria o abusiva del Estado. Sin embargo, eso no significa que el Estado cumpla sus obligaciones convencionales con el solo hecho de abstenerse de realizar tales interferencias. Además, el artículo 11.3 de la Convención impone a los Estados el deber de brindar la protección de la ley contra aquellas injerencias. En consecuencia, el Estado tiene la obligación de garantizar el derecho a la vida privada mediante acciones positivas, lo cual puede implicar, en ciertos casos, la adopción de medidas dirigidas a asegurar dicho derecho, protegiéndolo de las interferencias de las autoridades públicas así como también de las personas o instituciones privadas, incluyendo los medios de comunicación".[2322]

En lo que corresponde al choque del derecho a la vida privada y la libertad de expresión, la Corte IDH dispuso lo siguiente: "50. En este contexto, la Corte debe encontrar un equilibrio entre la vida privada y la libertad de expresión que, sin ser absolutos, son dos derechos fundamentales garantizados en la Convención Americana y de la mayor importancia en una sociedad democrática. El Tribunal recuerda que el ejercicio de cada derecho fundamental tiene que hacerse con respeto y salvaguarda de los demás derechos fundamentales. En ese proceso de armonización le cabe un papel medular al Estado, buscando establecer las responsabilidades y sanciones que fueren necesarias para obtener tal propósito. La necesidad de proteger los derechos que pudieran verse afectados por un ejercicio abusivo de la libertad de expresión requiere la debida observancia de los límites fijados a este respecto por la propia Convención".[2323]

E. Casos "Fernández Ortega y Rosendo Cantú respecto de México"

Los casos "Fernández Ortega y Rosendo Cantú" se relacionan con la violación sexual que ambas mujeres indígenas sufrieron por parte de elementos del ejército mexicano presentes en el estado de Guerrero. Respecto del derecho a la vida privada la Corte DIH determinó que este también se veía violentado en los contextos de violaciones sexuales. Sobre los razonamientos en este sentido, en ambos casos expresó que:

> […] en cuanto a la alegada violación, […], del artículo 11 de la Convención Americana, la Corte ha precisado que, si bien esa norma se titula "Protección de la Honra y de la Dignidad", su contenido incluye, entre otros, la protección de la vida privada. Por su parte, el concepto de vida privada es un término amplio no susceptible de definiciones exhaustivas, pero que comprende, entre otros ámbitos protegidos, la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos. La Corte considera que la violación sexual […] vulner[a] valores y aspectos esenciales de su vida privada, supuso una intromisión en su vida sexual y anuló su derecho a tomar libremente las decisiones respecto con quien tener relaciones sexuales, perdiendo de forma completa el control sobre sus decisiones más personales e íntimas, y sobre las funciones corporales básicas.[2324]

2321 Corte IDH. Caso "Fontevecchia y D'Amico vs. Argentina". *Fondo, reparaciones y costas*. Sentencia de 29 de noviembre de 2011. Serie C. No. 238, párrafo 48.

2322 Corte IDH. Caso "Fontevecchia y D'Amico vs. Argentina". *Fondo, reparaciones y costas*. Sentencia de 29 de noviembre de 2011. Serie C. No. 238, párrafo 49.

2323 Corte IDH. Caso "Fontevecchia y D'Amico vs. Argentina". *Fondo, reparaciones y costas*. Sentencia de 29 de noviembre de 2011. Serie C. No. 238, párrafo 50.

2324 Caso "Rosendo Cantú y otra vs. México". Excepción preliminar, fondo, reparaciones y costas. Sentencia de 31 de agosto de 2010. Serie C. No. 216, párrafo 119 y Caso "Fernández Ortega y otros vs. México". Excepción preliminar, fondo, reparaciones y costas. Sentencia de 30 de agosto de 2010. Serie C. No. 215, párrafo 129.

F. Caso "Karen Atala Riffo y niñas vs. Chile"

El caso "Atala" estaba relacionado con la separación de las hijas de la jueza Atala en un proceso de tuición presentado por el padre de las hijas debido a que la jueza había decidido convivir con su pareja (mujer), por lo que el aspecto determinante en la injerencia arbitraria que había sido plasmada en la sentencia a nivel interno, había sido la orientación sexual de Atala. Sobre este punto, resaltó que la orientación sexual es parte de la intimidad de una persona. Así, el Tribunal Interamericano expresó:

> 167. El Tribunal constata que durante el proceso de tuición, a partir de una visión estereotipada sobre los alcances de la orientación sexual de la señora Atala […] se generó una injerencia arbitraria en su vida privada, dado que la orientación sexual es parte de la intimidad de una persona y no tiene relevancia para analizar aspectos relacionados con la buena o mala paternidad o maternidad. Por tanto, la Corte concluye que el Estado vulneró el artículo 11.2, en relación con el artículo 1.1. de la Convención Americana, en perjuicio de Karen Atala Riffo.[2325]

G. Caso "Artavia Murillo y otros vs. Costa Rica"

El caso versaba sobre la imposibilidad que tenían algunas parejas costarricenses para poder acceder al procedimiento de fecundación *in vitro* para poder constituir una familia de manera asistida. En Costa Rica existía una prohibición de llevar a cabo esta técnica de reproducción asistida, siendo que tenía mayor impacto en personas de recursos económicos escasos debido a que dependían del sector público para poder llevarla a cabo. Sobre el derecho a la vida privada, la Corte IDH estimó que el derecho también incluido el derecho a poder ser padres o madres y la capacidad de tomar la decisión, así consideró que:

> 143. El ámbito de protección del derecho a la vida privada ha sido interpretado en términos amplios por los tribunales internacionales de derechos humanos, al señalar que éste va más allá del derecho a la privacidad. La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad. Además, la Corte ha señalado que la maternidad forma parte esencial del libre desarrollo de la personalidad de las mujeres. Teniendo en cuenta todo lo anterior, la Corte considera que la decisión de ser o no madre o padre es parte del derecho a la vida privada e incluye, en el presente caso, la decisión de ser madre o padre en el sentido genético o biológico.[2326]

H. "Ramírez Escobar y otros vs. Guatemala"

El caso estaba relacionado con las adopciones internacionales de niñas y niños guatemaltecos. En el caso concreto, se había producido la pérdida de la patria potestad por parte de las autoridades con base a estereotipos (por ejemplo, por orientación sexual o condición de pobreza) lo que derivó en que Osmín Ramírez y su hermano fueran dados en adopción a parejas de Estados Unidos. En el caso la Corte IDH expresó que la adopción de carácter internacional al haberse producido invadía la vida privada de las víctimas:

2325 Caso "Atala Riffo y niñas vs. Chile". Fondo, reparaciones y costas. Sentencia de 24 de febrero de 2012. Serie C. No. 239, párrafo 167.

2326 Caso "Artavia Murillo y otros (fecundación in vitro) vs. Costa Rica". Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 28 noviembre de 2012. Serie C. No. 257, párrafo 143.

239. Las adopciones de los hermanos Ramírez se llevaron a cabo en violación de garantías mínimas del debido proceso, tales como el derecho a ser oído, y en incumplimiento de los requisitos materiales y procesales mínimos que los Estados deben respetar y garantizar en el marco de un procedimiento de adopción internacional. La forma como se llevaron a cabo los procedimientos de adopción de J.R. y de Osmín Tobar Ramírez afectó de manera casi irremediable la vida privada y familiar de la familia Ramírez, los derechos de los niños y su derecho a ser oído. Por tanto, la Corte concluye que el Estado violó el derecho a ser oído, el derecho a la vida familiar libre de injerencias arbitrarias y a la protección de la familia establecidos en los artículos 8.1, 11.2 y 17.1 de la Convención, en relación con el artículo 1.1 del mismo instrumento, en perjuicio de Flor de María Ramírez Escobar, Gustavo Tobar Fajardo y Osmín Tobar Ramírez, así como en relación con el artículo 19 de la Convención Americana en perjuicio de este último.[2327]

Videovigilancia

José Soto Galindo

La videovigilancia es un método de control y vigilancia pública y privada que utiliza cámaras de video fijas o móviles para observar de manera remota y/o videograbar áreas geográficas o espacios determinados con la intención de prevenir, disuadir o sancionar conductas anómalas o registrar incidentes y situaciones de urgencia. La videovigilancia se utiliza como una herramienta para inhibir y/o sancionar la realización de conductas contrarias a leyes, normas y reglamentos o para garantizar la seguridad de personas o cosas. El uso de la videovigilancia puede significar un registro de imágenes de personas que las identifiquen o las hagan identificables y cuya obtención y almacenamiento represente un tratamiento de datos personales.

La autoridad de protección de datos en México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), describió la videovigilancia como "el uso de cámaras de video fijas o móviles con o sin sonido, o de sistemas cerrados de televisión que involucren la colocación de una o varias cámaras en espacios privados o públicos, limitadas a la supervisión o monitoreo de ese espacio y de las personas que en él se encuentran". El INAI distingue dos tipos de videovigilancia:

a) en tiempo real, sin grabaciones de por medio, y

b) la que guarda (graba) las imágenes en dispositivos de almacenamiento digital o análogo.

1. Relación con la protección de datos

El INAI ha sugerido la presentación de un aviso de privacidad mínimo, con excepción de cuando la videovigilancia se realice dentro de espacios privados como un domicilio particular, que informe a las personas susceptibles de ser captadas por el sistema de video sobre el tratamiento que se dará a las imágenes captadas. "En su instalación es necesario lograr un equilibrio entre el fin que estos sistemas de seguridad persiguen y el respeto a la privacidad, honor y la propia imagen de las personas, en virtud de que es un medio particularmente invasivo ya que, por ejemplo, puede llegar a identificar patrones de conducta y otros aspectos de la vida privada de las personas", dice su modelo de aviso de privacidad corto para videovigilancia.

2327 Caso "Ramírez Escobar y otros vs. Guatemala". Fondo, reparaciones y costas. Sentencia de 9 de marzo de 2018. Serie C. No. 351, párrafo 239.

La autoridad de protección de datos en España, la Agencia Española de Protección de Datos (AEPD), recomienda que al realizarse un tratamiento de imágenes "con fines de seguridad a través de los diversos sistemas existentes de captación, debe valorarse en primer lugar la legitimación para utilizar dichos sistemas de captación, así como los principios de limitación de la finalidad y minimización de datos".

2. Antecedentes

El uso de cámaras de video como herramienta de control y de seguridad tuvo su origen en la gestión del capital de trabajo a partir de los experimentos del ingeniero estadounidense Frank B. Gilbreth para monitorizar tanto a operarios como a la élite profesional a principios del siglo XX. A Gilbreth se le conoce como el pionero en el estudio de movimientos, que buscaba optimizar procesos productivos y aumentar la eficacia (en la misma línea de Frederick W. Taylor o de los ingenieros japoneses Taiichi Ohno y Eiji Toyoda para el llamado Sistema de Producción Toyota). Gilbreth utilizó tecnologías visuales y cámaras cinematográficas para mejorar y acelerar la producción industrial.

Pasaron muchos años para que esta manera de control y vigilancia se instaurara en espacios públicos. Los primeros ejercicios de implementación se desarrollaron en los setenta y en 1985 se instaló el primer sistema público de videovigilancia en la ciudad balneario de Bournemouth, Inglaterra, con motivo de la conferencia anual del Partido Conservador del Reino Unido. Un año antes, esa ciudad a 180 kilómetros de Londres, había vivido un ataque del Ejército Republicano Irlandés (IRA) que dejó cinco muertos. Para la segunda década del siglo XXI, los equipos de videovigilancia se han mimetizado con el mobiliario público.

En México, el Censo Nacional de Gobierno, Seguridad Pública y Sistema Penitenciario Estatales 2016 del INEGI contabilizó 36,194 cámaras de vigilancia pública en las entidades federativas (casi 30 equipos de videovigilancia por cada 100,000 habitantes). Las entidades con el mayor número de cámaras de videovigilancia ese año fueron la Ciudad de México (15,010), el Estado de México (10,000), Guanajuato (2,189), Michoacán (1,260) y Jalisco (870).

3. La videovigilancia en México

En el régimen jurídico mexicano no existe una ley de carácter general o federal que regule la instalación y el uso de la videovigilancia. Esta tarea ha quedado a cargo de los órganos legislativos estatales y de las administraciones municipales. Tampoco existen leyes generales o federales respecto a la videovigilancia realizada por particulares en espacios públicos o privados, con excepción de normas de protección de datos personales o de los derechos a la vida privada, el honor y la propia imagen, y tampoco regímenes que garanticen que la información generada por los equipos y sistemas de videovigilancia se tratará con principios mínimos, como los de confidencialidad, integridad, proporcionalidad, idoneidad y seguridad.

Para el Sistema Nacional de Seguridad Pública (SNSP), la videovigilancia funciona como un método de disuasión, pues opera con "el principio de que, si el delincuente percibe mayor certeza de ser capturado, disminuirán las posibilidades de involucrarse en alguna actividad criminal" (SNSP, 2016. Norma Técnica para Estandarizar las Características Técnicas y de Interoperabilidad de los Sistemas de videovigilancia para la Seguridad Pública). Además, esta herramienta ofrece a las autoridades elementos probatorios sobre la comisión de delitos y acarrea beneficios sociales: "Derivado de la reducción de la criminalidad,

un incremento en la sensación de seguridad puede acarrear impactos benéficos para la cohesión social en una comunidad, e incluso, en una ciudad o un estado".

La videovigilancia urbana es parte de un paquete de tecnologías para el control y la vigilancia que incluye desde detectores sonoros de disparos de armas de fuego, botones de pánico para alertar a la policía y a las instancias de protección civil de incidentes en la vía pública, cinemómetros y cámaras para captar conductas que infrinjan reglamentos de tránsito con fines sancionatorios.

La Ciudad de México cuenta, desde 2008, con la Ley que regula el uso de tecnología para la seguridad pública del Distrito Federal, la cual norma la ubicación, instalación y operación de equipos y sistemas tecnológicos a cargo de la Secretaría de Seguridad Pública. La tesis I.1o.P. J/3 (10a.) señala que el sistema de videovigilancia pública puede ser prueba para acreditar la detención en flagrancia si para la captura de un delincuente se utilizan las cámaras de monitoreo remoto y en tiempo real, si éstas registran el hecho delictivo, se observa detalle a detalle y sin interrupción el recorrido del individuo y se le detiene en un tiempo razonable después de cometer la falta.

Respecto a la observancia del reglamento de tránsito en la Ciudad de México, la Suprema Corte de Justicia de la Nación determinó, en mayo de 2018, que la aplicación de sanciones por infringir normas de vialidad a partir de imágenes captadas por el sistema público de videovigilancia no viola el derecho de audiencia previa, pues los ciudadanos infractores pueden ejercer su derecho a defenderse de forma posterior a la imposición de la sanción.

La Ley de Videovigilancia del Estado de Yucatán, promulgada en julio de 2018, regula la videovigilancia y establece "bases normativas para la adquisición, ubicación, instalación y operación de las cámaras de videovigilancia y los sistemas y equipos tecnológicos complementarios, así como para la recopilación, sistematización, resguardo, custodia, administración, uso, suministro e intercambio de la información que de ellos provenga". Esta ley contempla que los ciudadanos tienen derecho a ser informados sobre los puntos donde se realizan actividades de videovigilancia pública, a ejercer derechos de protección a la vida privada y a los datos personales, y a solicitar acceso a las grabaciones resultado de la videovigilancia "en las que figuren o en las que razonablemente consideren que existen datos sobre alguna afectación que hayan sufrido, así como, en su caso, a la rectificación, cancelación u oposición al tratamiento que corresponda" (artículo 4, fracciones I, II y III).

La Secretaría de Seguridad de Pública de Yucatán tiene la atribución de "autorizar las solicitudes de instalación de cámaras fijas y móviles de videovigilancia realizadas por instituciones de los sectores público, privado o social, o por la comunidad en general" (artículo, fracción XII). Los particulares, cuando estén constituidos como empresas de seguridad privada, tienen la obligación de "inscribir en el registro estatal las cámaras fijas y móviles de videovigilancia y los sistemas o equipos tecnológicos complementarios que utilicen para el desempeño de sus funciones" (artículo 15, fracción II). Para el desarrollo de conjuntos residenciales, la ley impone la instalación de un sistema de videovigilancia que deberá estar acorde con los lineamientos desarrollados por la autoridad. Estos sistemas de videovigilancia privada podrán ser conectados a la red de videovigilancia pública (artículo 23). Los particulares no estarán obligados a colaborar con las autoridades públicas en el caso de que sus sistemas de estos sistemas de vigilancia capten hechos posiblemente delictivos, "salvo que se trate de un requerimiento jurisdiccional" (artículo 15, último párrafo).

Otros estados con una legislación específica sobre videovigilancia son Aguascalientes, Baja California Sur, Colima y Durango, Guadalajara y Sayula tienen reglamentos municipales. (Arteaga Botello, 2016).

Visitas de verificación

Luis Manuel Pérez de Acha y
Denise Tron Zuccher

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) podrá realizar visitas de verificación para asegurar el cumplimiento de la legislación en materia de protección de datos personales. Esta facultad debe ser ejercida dentro del procedimiento de verificación previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) cuando se trate de sujetos del sector público.

Las visitas de verificación presentan tres etapas: orden de visita, desarrollo de la verificación y acta de verificación. En este apartado serán analizadas las dos primeras.

1. Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Derecho a la inviolabilidad del domicilio

El artículo 16 de la Constitución de los Estados Unidos Mexicanos (CPEUM) establece como un "derecho subjetivo público de los gobernados el que no puedan ser molestados en su persona, papeles o domicilio y la inviolabilidad de éste".[2328] Ese derecho puede ser restringido mediante actos de molestia, siempre que se respeten las garantías previstas en el propio texto constitucional[2329] mediante mandamiento escrito emitido por autoridad competente, en el que funde y motive la causa legal del procedimiento.

Las visitas de verificación reciben una protección especial desde la CPEUM, respecto de otros actos de molestia. En tanto se trata de una excepción al derecho sustantivo a la inviolabilidad del domicilio, deberán sujetarse a lo dispuesto por el párrafo 16 del artículo 16 que regula las visitas domiciliarias, el cual remite al párrafo 11 del mismo precepto, relativo a los cateos en materia penal.

a) Procedimiento de verificación

Las visitas de verificación que realice el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) deberán practicarse dentro del procedimiento de verificación previsto en los artículos 59 y 60 de la LFPDPPP. Cabe recordar que el INAI es la autoridad responsable de vigilar el debido cumplimiento de la LFPDPPP y de asegurar que los particulares (personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales)[2330] cumplan con las obligaciones que les impone este ordenamiento. Es en el ejercicio de estas atribuciones que se justifican las visitas de verificación.

Son dos los supuestos bajo los cuales el INAI podrá iniciar el referido procedimiento: i) por el incumplimiento a las resoluciones dictadas en el procedimiento de protección de derechos y ii) cuando se presuman violaciones a la LFPDPPP. Estos supuestos definen el objeto y alcance de las visitas de verificación.

2328 Tesis 1a./J. 22/2002, *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XV, abril de 2002, p. 430.

2329 Artículo 16, primer párrafo, Constitución Federal.

2330 Artículo 2º, LFPD. La legislación también se refiere a estos sujetos como "responsable", de acuerdo con el artículo 3º, fracción XIV, LFPD.

Dentro del procedimiento de verificación, el INAI podrá realizar diversas visitas[2331] para allegarse de elementos de convicción relacionados con el objeto de dicho procedimiento.

La Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN) se pronunció sobre la constitucionalidad de la facultad otorgada al INAI para practicar visitas de verificación, al resolver que no obstante que el artículo 16, decimosexto párrafo de la Constitución Federal señala que únicamente se podrán practicar visitas domiciliarias para vigilar el cumplimiento de "reglamentos sanitarios y de policía", debe entenderse que tal disposición permite la práctica de visitas para corroborar el cumplimiento "de cualquier norma jurídica que otorgue facultades a las autoridades administrativas para regular la conducta de los particulares y cerciorarse de que se ajusta a las normas de orden público aplicables".[2332]

En este mismo caso, la SCJN sostuvo que las visitas de verificación en esta materia no vulneran el derecho a la inviolabilidad del domicilio,[2333] como tampoco vulneran el principio de reserva de ley, en tanto es el RLFPD[2334] el ordenamiento que las regula.[2335]

b) Orden de visita

Las órdenes de visita deben cumplir con los requisitos previstos en los artículos 16, párrafos primero y decimoprimero de la Constitución Federal, 63 de la LFPA, 133 del RLFPD y 63 de los Lineamientos de los Procedimientos. Por tanto, en la orden de visita debe constar lo siguiente:

- Objeto de la visita
- Alcance de la visita
- Fundamentación y motivación
- Autoridad que emite la orden
- Lugar en donde se practicará la visita
- Nombre del sujeto visitado
- Nombre de los visitadores

En términos de la SCJN, el objeto de la orden de visita "[…] no solo debe concebirse como propósito, intención, fin o designio, que dé lugar a la facultad comprobatoria que tienen las autoridades correspondientes, sino también debe entenderse como cosa, elemento, tema o materia, esto es, lo que produce certidumbre en lo que se revisa". Por ello, continúa la misma jurisprudencia, el objeto de la orden "[…] no debe ser general, sino determinado, para así dar seguridad al gobernado y, por ende, no dejarlo en estado de indefensión".[2336] Si bien esta tesis se refiere a la materia fiscal, también resulta aplicable a las visitas de verificación practicadas por el INAI.

La orden de visita establece los límites a los cuales deberán sujetarse los verificadores al momento de practicar la visita a fin de evitar un ejercicio arbitrario de esta facultad. En jurisprudencia de la Segunda Sala de la SCJN se sostuvo que "el objeto de una orden

2331 Artículo 132, RLFPD.

2332 Sentencia del amparo directo en revisión 888/2017. Segunda Sala. SCJN, p. 36.

2333 Tesis 2a. CXXXIX/2017 (10a.), *Gaceta del Semanario Judicial de la Federación*. Décima época. Libro 46. Tomo I, septiembre de 2017, p. 780.

2334 Artículos 132 a 136, RLFPD.

2335 Tesis 2a. CXLI/2017 (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima época. Libro 46. Tomo I, septiembre de 2017, p. 777.

2336 Tesis 2a./J. 59/97, *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo IV, diciembre de 1997, p. 333.

de verificación constituye la delimitación del actuar de la autoridad, a fin de determinar dónde empezarán y dónde terminarán las actividades que ha de realizar durante la verificación correspondiente, dado que la determinación del objeto configura un acto esencial para la ejecución de las facultades de inspección de la autoridad fiscalizadora, pues tiende a especificar la materia de los actos que ejecutará". Este criterio señala que la orden debe precisar "el rubro a inspeccionar y su fundamento legal, a fin de que la persona verificada conozca las obligaciones a su cargo que van a revisarse, en acatamiento a la garantía de seguridad jurídica prevista en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos".[2337]

El objeto de la orden de visita debe ser determinado y específico, a fin de brindar seguridad jurídica al particular. Por tanto, no serán admisibles aquellas que resulten generales o imprecisas.[2338] El objeto de la orden deberá concordar con la situación del sujeto visitado frente a las obligaciones que le impone la LGPDPPSO, esto es, debe determinar de manera precisa cuáles son las obligaciones legales materia de la verificación.

El particular debe conocer, desde el momento en que se le entrega la orden de verificación, cuáles son las obligaciones a su cargo que serán revisadas, ya que esto determinará los límites impuestos a los visitadores para practicar la diligencia.[2339] Así mismo, el objeto de la orden constreñirá el alcance de los datos, informes o documentos que se le requieran al particular.[2340]

El grado de precisión del objeto y del alcance de la orden de visita dependerá de la legislación secundaria respectiva.[2341] Por ejemplo, en materia fiscal, la SCJN ha resuelto que la orden debe especificar el alcance temporal de la revisión, esto es, deberán señalarse las contribuciones y los periodos que serán verificados por las autoridades.[2342] Sin embargo, en otras materias como son las visitas a los centros de trabajo, existe jurisprudencia de un pleno de circuito que señala que en estos casos la orden de visita "no merece el mismo grado de precisión de su objeto que el necesario para la validez de una orden de visita domiciliaria en materia fiscal", porque aquellas visitas se fundan en un interés público, sustentado en la obligación constitucional de salvaguardar los derechos de los trabajadores en su centro laboral.[2343]

En las visitas de verificación practicadas en materia de protección de datos personales en posesión de los particulares, la definición del objeto de la visita deberá respetar el derecho humano a la seguridad jurídica del particular visitado, además de otorgar los elementos necesarios para que éste tenga certeza del alcance de la diligencia. Si la orden de visita es "lo que produce certidumbre en lo que se revisa", debe cumplir con una serie de requisitos que están definidos desde el artículo 16 de la Constitución Federal y que deben respetarse a fin de otorgar seguridad jurídica al particular.

Al tratarse de un acto de molestia, la orden de visita debe encontrarse debidamente fundada y motivada en términos del artículo 16, primer párrafo de la Constitución Federal,

2337 Tesis 2a./J. 175/2011 (9a.), *Semanario Judicial de la Federación y su Gaceta*. Décima época. Libro IV. Tomo 4, enero de 2012, p. 3545.

2338 Tesis 2a./J. 59/97, *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo IV, diciembre de 1997, p. 333.

2339 Tesis: PC.IV.A. J/7 A (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima época, libro 14, t. II, enero de 2015, p. 1554.

2340 Tesis: PC.XXXIII.CRT J/2 A (10a.), *Gaceta del Semanario Judicial de la Federación*. Décima época. Libro 14. Tomo II, enero de 2015, p. 1143.

2341 Tesis: PC.IV.A. J/7 A (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima época, libro 14, t. II, enero de 2015, p. 1554.

2342 Tesis: 2a./J. 57/99, *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo IX, junio de 1999, p. 343.

2343 Tesis: PC.IV.A. J/7 A (10a.), *Gaceta del Semanario Judicial de la Federación*, Décima época, libro 14, t. II, enero de 2015, p. 1554.

que establece: “Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento”.

El artículo 16 constitucional exige que tanto la autoridad que emite la orden de visita, como aquellas que la practican, cuenten con las facultades expresas para tales efectos. Para cumplir con la garantía de fundamentación es necesario que la orden de visita señale la disposición legal en que están previstas las facultades de la autoridad emisora de la misma.[2344] Es requisito también que en la orden conste firma autógrafa de quien la emite.

La visita de verificación podrá llevarse a cabo en el establecimiento del responsable o en el lugar en que se encuentran sus bases de datos.[2345] Los Lineamientos de los Procedimientos señalan que la visita también podrá realizarse en el lugar en que se encuentre la información.[2346] Los visitadores deben sujetarse al lugar señalado en la orden para practicar la verificación, sin que resulte admisible que la definición del lugar resulte ambiguo o se deje a discreción de los visitadores.[2347] No existe limitación para que dentro de un procedimiento de verificación, el INAI realice diversas visitas en diferentes domicilios del particular.

Si bien la legislación no prevé expresamente que la orden de visita señale el nombre del sujeto visitado, es un requisito necesario en términos del artículo 16 constitucional.

En la orden de visita deberán constar los nombres del personal del INAI que llevará a cabo la visita de verificación. Lo anterior asegura que el sujeto verificado contará con información suficiente para asegurarse de que las personas que se introduzcan a su domicilio son aquellas que fueron facultadas para tales efectos.

c) Desarrollo de la visita

La visita de verificación iniciará con la entrega de la orden. La legislación de protección de datos no señala expresamente que la orden deba ser notificada de manera personal al sujeto visitado. Sin embargo, de la interpretación de diversos preceptos es posible considerar que es necesario que el INAI atienda este requisito, lo que implica que deberá actuar en términos de los artículos 8 y 10 de los Lineamientos de los Procedimientos que prevén las reglas para las notificaciones personales.

Cabe apuntar que las notificaciones personales deben realizarse previo citatorio, de esta forma se le otorga al particular la oportunidad de estar presente durante el desarrollo de la visita de verificación. La SCJN ha reconocido para la materia fiscal, la importancia de que la orden de visita sea notificada de forma personal y la necesidad del citatorio previo,[2348] como una formalidad que garantiza la protección al gobernado frente a una excepción al principio de inviolabilidad del domicilio, en los siguientes términos: “el objeto del citatorio no se constriñe únicamente a citar al contribuyente para que reciba una orden de visita domiciliaria, sino fundamentalmente para que el contribuyente o su representante conozca de manera cierta el tipo de diligencia administrativa que se realizará en su domicilio como excepción al principio de inviolabilidad domiciliaria”.[2349]

2344 Tesis 2a./J. 85/2007, *Semanario Judicial de la Federación y su Gaceta*. Décima época. Tomo XXV, mayo de 2007, p. 990.

2345 Artículo 133, RLFPD. El artículo 3, fracción II de la LFPD define bases de datos como: “El conjunto ordenado de datos personales referentes a una persona identificada o identificable”.

2346 Artículo 63, Lineamientos de los Procedimientos.

2347 Tesis: P. CXXVI/2000. *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XII, agosto de 2000, p. 146.

2348 Este requisito se encuentra expresamente previsto en el Código Fiscal de la Federación, artículo 44, fracción II.

2349 Tesis: 2a./J. 62/2002, *Semanario Judicial de la Federación y su Gaceta*. Novena época. Tomo XVI, julio de 2002, p. 377.

La visita de verificación deberá ser atendida por el responsable o por su representante legal en el caso de personas morales. El personal del INAI requerirá la presencia del responsable al momento en que se presenten en el domicilio visitado. En caso de que este no se encuentre, dejará citatorio en el que se especifique que el objeto del mismo es la notificación de una orden de visita. Solo en el supuesto de que el responsable no atienda el citatorio, la visita podrá iniciarse con la persona que se encuentre en el domicilio.

El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) señala que, al iniciar la visita, los verificadores deben identificarse ante el sujeto visitado, exhibirle la orden de visita, el oficio de comisión y entregarle copia de ambas.[2350] Estas formalidades necesariamente se observarán previo a que los verificadores tengan acceso al domicilio del sujeto visitado.

Para identificarse, los verificadores deben exhibir su credencial vigente con fotografía, expedida por la autoridad competente del INAI. Como antes quedó apuntado, es necesario que el nombre de los verificadores conste en la orden de visita. Estos requisitos salvaguardan la seguridad jurídica del sujeto visitado, a efecto de que tenga certeza de que las personas que se presentan en su domicilio están facultadas para desempeñar la función de verificación.[2351]

Un aspecto fundamental en las visitas de verificación son los testigos de asistencia. El nombramiento de los mismos debe llevarse a cabo desde el inicio de la visita, ya que solo de esta manera podrán cumplir con su finalidad "que es la de testificar sobre la veracidad de los hechos desarrollados durante la práctica de la visita".[2352] Este requisito, previsto en el artículo 16 de la Constitución Federal, supone la participación activa de los testigos durante todo el desarrollo de la visita, para que tengan certeza de los datos que en su momento se asienten en el acta de verificación. Lo anterior obliga al personal del INAI a solicitarle a la persona con quien se atienda la visita que designe a dos testigos, y solo en el supuesto de que ésta se niegue a hacerlo, serán los verificadores quienes los designen. El incumplimiento de estas formalidades tendrá como consecuencia la ilegalidad de la visita de verificación.

Una vez observado lo anterior, el personal del INAI podrá acceder al domicilio visitado y solicitar la información y documentación necesaria para cumplir con el objeto de la visita.[2353] Los verificadores están obligados a guardar confidencialidad sobre la información que conozcan en el curso de la visita.[2354]

Las visitas tendrán una duración máxima de 10 días,[2355] lo cual debe ser informado al visitado desde su inicio. Si la autoridad no señala expresamente cuál es la duración máxima que puede tener la visita, la misma resultará ilegal. Por otra parte, las actuaciones de los verificadores no podrán exceder los 10 días, ya que de lo contrario todas las actuaciones serán ilegales.

2. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

El INAI podrá practicar visitas de verificación a sujetos obligados, siempre que lo efectúe dentro del procedimiento de verificación,[2356] que tiene como objeto vigilar y verificar el

2350 Artículos 134, RLFPD y 63, Lineamientos de los Procedimientos.

2351 Tesis:ca (I Región) 8o.42 A (10a.), *Gaceta del Semanario Judicial de la Federación*. Décima época. Libro 39. Tomo III, febrero de 2017, p. 2378.

2352 *Semanario Judicial de la Federación*. Octava época. Tomo III, enero-junio de 1989, p. 884.

2353 Artículo 63, Lineamientos de los Procedimientos.

2354 Artículo 60, segundo párrafo, LFPDPPP.

2355 Este plazo también está previsto en el artículo 32 de la LFPA.

2356 Artículos 146 a 150 de la LGPDPPSO.

cumplimiento de la LGPDPPSO. El INAI podrá realizar las visitas que resulten necesarias para allegarse de la documentación e información que requiera, en cualquiera de los lugares que se especifican en el siguiente párrafo.

Las visitas de verificación, reguladas en los artículos 149 de la LGPDPPSO y 204 a 206 de los Lineamientos Generales, podrán practicarse en las oficinas e instalaciones de los sujetos obligados, o bien, en el lugar en el que estén ubicadas las bases de datos personales o en el que traten o procesen datos personales. Cada visita tendrá una duración máxima de cinco días hábiles.

Cabe señalar que el artículo 16 de la Constitución Federal no tutela las visitas de verificación que realiza el INAI a los sujetos obligados del sector público, de la forma en que lo hace para las visitas domiciliarias practicadas a particulares.

En jurisprudencia, un Tribunal Colegiado de Circuito sostuvo que el referido precepto constitucional "no incluye las formalidades que deben observarse con motivo del ejercicio de la función pública". En este sentido, las visitas de verificación a entidades públicas se realizan en contextos distintos a aquellas efectuadas a particulares, esto es, "las auditorías de las dependencias o entidades federales son actos internos de control a la gestión y no se encuentran dirigidas a una persona determinada, ni se practican en domicilios privados, sino en oficinas públicas".

En la citada jurisprudencia, a las visitas de verificación realizadas bajo la LGSO no les son aplicables las formalidades y garantías que tutela el artículo 16 constitucional, ya que los requisitos previstos en este precepto "obedecen y se justifican en razón de los valores y bienes jurídicos que se ponen en riesgo, como es la privacidad del domicilio de los gobernados".[2357]

De acuerdo con la legislación, la orden de verificación debe cumplir con los siguientes requisitos: encontrarse debidamente fundada y motivada, señalar el lugar en el que se practicará la visita, así como el objeto y alcance de la misma, y ser emitida por autoridad competente. Si bien la regulación no lo señala expresamente, la orden también deberá especificar el nombre del sujeto obligado y el nombre del personal del INAI que practicará la visita.

Al inicio de la visita, los verificadores deben identificarse con credencial vigente con fotografía y entregar la orden de visita y el oficio de comisión a la persona con la que se atienda la visita. Cumpliendo con estos requisitos, los verificadores podrán tener acceso a la información en poder de los sujetos obligados, los cuales están obligados a proporcionar la documentación e información que se les requiera, así como a permitir el acceso a sus bases de datos personales o tratamientos de estos. La legislación señala expresamente que los servidores públicos no podrán invocar la reserva o confidencialidad a efecto de impedir el acceso a la información o a las bases de datos en su poder.

En conclusión, es a través de las visitas de verificación que el INAI podrá constatar en el domicilio de los particulares y de los sujetos obligados, el debido cumplimiento de la legislación en materia de datos personales. Por lo que hace a los particulares, implica una excepción al derecho a la inviolabilidad del domicilio, lo que obliga al INAI a cumplir con una serie de formalidades previstas desde la Constitución Federal. Tanto en la LFPDPPP como en la LGPDPPSO, el cumplimiento de la legislación será una condición necesaria para que la información y documentación obtenida en las visitas goce de validez dentro del procedimiento de verificación.

2357 Tesis: I.4o.A. J/32, *Semanario Judicial de la Federación*. Novena época. Tomo XX, julio de 2004, p. 1370.

Vulnerabilidad

Andrés Velázquez Olavarrieta

En las recomendaciones en materia de seguridad de datos personales del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI)[2358] se define "vulnerabilidad" como la "falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas", por lo tanto, este término está ligado al de amenaza, siendo esta la "circunstancia o evento con la capacidad de causar daño a una organización". Tanto la vulnerabilidad como la amenaza están ligadas al termino de incidente (escenario donde una amenaza explota una vulnerabilidad o conjunto de vulnerabilidades), por lo tanto, partiendo de esta triada, para efectos prácticos, la vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma.

Las vulnerabilidades pueden tener distintos orígenes y todos hacen que las personas sean susceptibles a las amenazas. Las vulnerabilidades informáticas se pueden agrupar en función del diseño de la seguridad perimetral, debilidad en el diseño de protocolos utilizados en las redes, políticas de seguridad deficientes e inexistentes, implementación y errores de programación, descuido de los fabricantes, configuración inadecuada de los sistemas informáticos, desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática, y el uso.

Vulneración de datos personales

Andrés Velázquez Olavarrieta

Siendo que la vulnerabilidad es la "falta o debilidad de seguridad en un activo o grupo de activos que puede ser explotada por una o más amenazas",[2359] la vulneración de datos personales es la materialización de las amenazas pudiendo estar enfocadas a la pérdida o destrucción no autorizada de los datos personales en posesión de las personas físicas o morales que realizan el tratamiento de los datos, el robo, extravío o copia no autorizada de los mismos, su uso, acceso o tratamiento no autorizado, así como el daño, alteración o modificación no autorizada. Estas vulneraciones están comprendidas en el artículo 38 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y en el 63 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).

De acuerdo con el artículo 20 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), "las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos". La LGPDPPSO en el artículo 40 señala que "el responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los organismos garantes de las entidades federativas, las vulneraciones que afecten de forma significativa los derechos

2358 http://inicio.ifai.org.mx/MarcoNormativoDocumentos/RECOMENDACIONES%20EN%20MATERIA%20DE%20SEGURIDAD%20DE%20DATOS%20PERSONALES.pdf

2359 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, articulo 38.

patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos".

El artículo 41 de la misma Ley señala que al realizar la notificación, las empresas deben informar (al menos la naturaleza del incidente) los datos personales comprometidos, las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses, las acciones correctivas realizadas de forma inmediata y los medios donde puede obtener más información al respecto.

NOTAS

Web beacons

Andrés Velázquez Olavarrieta

El artículo 14 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP) establece que cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología para recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento deberá informar al titular, a través de una comunicación o advertencia colocada en un lugar visible, sobre el uso de esas tecnologías y el hecho de que a través de las mismas se obtienen datos personales, así como la forma en que se podrán deshabilitar, esto último salvo que dichas tecnologías sean necesarias por motivos técnicos.

El reglamento se refiere a los *web beacons*, es decir, a una imagen visible u oculta insertada dentro de un sitio *web* o correo electrónico que se utiliza para monitorear el comportamiento del usuario en estos medios. A través de éstos se puede obtener información como la dirección IP de origen, navegador utilizado, sistema operativo, momento en que se accedió a la página y, en el caso del correo electrónico, la asociación de los datos anteriores con el destinatario.

Los términos y funciones de *web beacons* y *cookies*[2360] están ligados porque las empresas los usan para brindar la mejor experiencia durante la navegación en su sitio, así como para guardar información sobre su acceso para mejorar la seguridad de una cuenta en caso de ser una empresa de transacciones financieras o comerciales (*e-commerce*) y hacer seguimiento de sus compras en línea, definir preferencias de contenido y personalizar información con base en los intereses de los usuarios.

Las funciones que realizan las *cookies* y/o *web beacons* están divididas en esenciales, complementarias, de desempeño, de mercadeo y de asociados. Las esenciales habilitan el sistema de autenticación y validación de forma segura, así como funciones de prevención de fraudes, las complementarias habilitan funcionalidades adicionales para determinar

2360 Un archivo de datos que se almacena en el disco duro del equipo de cómputo o del dispositivo de comunicaciones electrónicas de un usuario al navegar en un sitio de internet específico, el cual permite intercambiar información de estado entre dicho sitio y el navegador del usuario. La información de estado puede revelar medios de identificación de sesión, autenticación o preferencias del usuario, así como cualquier dato almacenado por el navegador respecto al sitio de internet.

preferencias definidas previamente aplicadas por el usuario como contenido, lenguaje y tamaño de texto.

Las funciones de desempeño llevan un seguimiento de los segmentos más visitados, así como el uso del sitio *web* y sus enlaces, lo que permite identificar un posible problema durante el uso del sitio y solucionarlo de manera expedita. Las de mercadeo aseguran que el usuario reciba información relevante sobre beneficios y promociones de la empresa que las usa e identifican al usuario de manera segura en sus diferentes contenidos para desplegar información personalizada. Las de asociados son definidas en el navegador como referencia para ayudar a proveer al usuario de información relevante en línea por las empresas asociadas a la página que visita originalmente.

Los sujetos obligados también deben alinearse a esta disposición toda vez que manejan información de terceros. Por ejemplo, al ingresar a la página de American Express México para continuar con el uso de su sitio de internet,[2361] la empresa expone "usted consiente que recabe y trate sus datos personales" y agrega: "American Express México le informa, a través de estos términos y condiciones sobre el uso que le da a las *cookies*, *web beacons* y/o tecnología similar con el propósito de que usted tenga pleno control y decisión sobre los datos personales que en su caso se traten de usted". Luego de ese aviso presenta las definiciones que hace de los términos[2362] y de qué forma los usa. Previamente había explicado sus principios de privacidad y protección de datos.[2363]

2361 https://www.americanexpress.com/mx/RegulatoryInfo/uso-de-cookies.html

2362 Utiliza las definiciones técnicas.

2363 https://www.americanexpress.com/mx/content/RegulatoryInfo/acuerdo-de-privacidad.html

NOTAS

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Diccionario de Protección de Datos Personales. Conceptos Fundamentales
se terminó de imprimir el 20 de noviembre de 2019,
en los Talleres Gráficos de México,
Canal del Norte 80, colonia Felipe Pescador,
Alcaldía Cuauhtémoc, C. P. 06280,
Ciudad de México.

Tiraje: 3,000 ejemplares.

Edición a cargo de
Dirección General de Promoción y Vinculación con la Sociedad