

La protección de los datos personales en la Argentina

1er. Taller de Protección de Datos Personales

INAI, 06/07/18

Normas constitucionales federales

Art. 38.- (Partidos políticos) *Los partidos políticos son instituciones fundamentales del sistema democrático. Su creación y el ejercicio de sus actividades son libres dentro del respeto a esta Constitución, la que garantiza... **el acceso a la información pública** y la difusión de sus ideas.*

Art. 41.- (Derecho al ambiente) *Todos los habitantes gozan del derecho a un ambiente sano, equilibrado, apto para el desarrollo humano... Las autoridades proveerán a la protección de este derecho, a la utilización racional de los recursos naturales, a la preservación del patrimonio natural y cultural y de la diversidad biológica, y a la **información y educación ambientales.***

Art. 42.- (Derechos de consumidores y usuarios) *Los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, a la protección de su salud, seguridad e intereses económicos; a **una información adecuada y veraz;** a la libertad de elección, y a condiciones de trato equitativo y digno.*

Normas constitucionales federales

Art. 43.- (Amparo individual) *Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares...*

(Amparo colectivo y de clase) *Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general...*

(Hábeas data) *Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.*

(Hábeas corpus) *Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de hábeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato...*

Normas constitucionales estatales

Ciudad Autónoma de Buenos Aires (art. 16)

Provincia de Buenos Aires (art. 20)

Córdoba: (art. 50)

Chaco (art. 19)

Chubut (art. 56)

Jujuy (art. 23)

La Rioja (art. 30)

Río Negro (art. 20)

Salta (art. 22)

San Juan (art. 26)

San Luis (art. 21)

Tierra del Fuego (art. 45)

La legislación subconstitucional

1996: Primera ley de protección de datos personales (Vetada totalmente por el Poder Ejecutivo)

2000: Ley 25.326, “de protección de los datos personales” (Veto de dos artículos por el Poder Ejecutivo, incluidos dos incisos del art. 29, referido a aspectos básicos de la independencia del órgano de control: la forma de elección, requisitos para el cargo, duración y estabilidad de su titular).

Fuente: Lortad española de 1992

2001: Decreto presidencial n° 1558, reglamentario de la ley.

2002: Creación del órgano de control previsto en la ley (la Dirección Nacional de Protección de Datos Personales) dentro de la órbita del Ministerio de Justicia y Derechos Humanos.

2008: Ley 26.343, incorpora el art. 47 consagrando un excepcional derecho al olvido de datos de solvencia patrimonial y de crédito para los deudores entre 01/01/2000 y 10/12/2003.

2017: Proyecto integral de reforma a la ley 25.326 incorporando las novedades del RGPD europeo

La ley 25.326

Ámbito de aplicación

Artículo 1° — (Objeto).

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

Decreto 1558/91:

A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

La ley 25.326

Ámbito de aplicación

Art. 44 — (Ámbito de aplicación).

Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.

Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.

La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

(Capítulo I: Disposiciones Generales); (Capítulo II: Principios generales relativos a la protección de datos); (Capítulo III: Derechos de los titulares de datos); (Capítulo IV: Usuarios y responsables de archivos, registros y bancos de datos), (Art. 32: Sanciones penales)

Quedan fuera a falta de adhesión provincial:

Capítulo V: Control (administrativo) Capítulo VI Sanciones administrativas (art. 31) y Capítulo VII Acción de protección de los datos personales

La ley 25.326

Ámbito de aplicación

1) El órgano de control sólo tiene jurisdicción sobre bancos de datos del sector público federal y sobre bancos de datos de titularidad privada interconectados en redes interjurisdiccionales.

2) El proceso de hábeas data se reguló solo para los juicios que se tramiten ante el fuero federal, y en la mayoría de las provincias no fue regulado ante la falta de urgencia debido a que se utilizan para encauzar a la acción las reglas preexistentes del amparo, las que deben ser necesariamente adaptadas a esta garantía.

3) La ley se aplica en todo el país sólo en los principios generales del tratamiento de datos y falta:

a) el dictado de leyes en los estados federados que dispongan la creación de órganos de control que tengan jurisdicción sobre los bancos de datos que están fuera de la competencia del órgano de control federal, y

b) la adecuación de las normativas procesales locales preexistentes.

Hasta el momento, de 24 estados federados, sólo cinco dictaron leyes , de los cuales sólo uno –la Ciudad Autónoma de Buenos Aires- estableció su órgano de control (la Defensoría del Pueblo) y reguló la acción. Algunas de las restantes sólo regularon el hábeas data (Chubut, Chaco, Río Negro y San Juan).

La ley 25.326

Ámbito de aplicación

Decisión de adecuación (Directiva 95/46):

La Unión Europea otorgó a la Argentina el 30/06/03 el estatus de extracomunitario con nivel de protección adecuado a los fines de la transmisión internacional de datos (Decisión 2003/490/EC,).

El dictamen del GT 29 de la Directiva 95/46/CE, de 2002, al aconsejar tal certificación, objetó:

- a) la ausencia -por entonces total y por cierto hoy todavía predominante– de órganos de control de los estados federados, y,
- b) la falta de independencia del órgano de control nacional (Su director fue sólo designado por concurso público (decreto 1898/02), para 2002 a 2006).

Adhesión al Convenio 108:

En 2017 la Argentina solicitó al Consejo de Europa que fuera invitada a adherir al Convenio N° 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

El Comité Consultivo del Consejo de Europa opinó que era viable la adhesión.

En la reunión N° 1295 del Consejo de Europa, el Comité de Ministros aceptó la solicitud.

El Senado de la Nación le dio media sanción a la ley de adhesión siendo girado a Diputados en 2018

Control administrativo

Ley 25.326

Art. 29. — (Órgano de Control).

1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones: a) Asistir y asesorar... b) Dictar las normas y reglamentaciones...c) Realizar un censo de archivos... y mantener el registro permanente de los mismos... d) Controlar la observancia de las normas sobre integridad y seguridad de datos...e) Solicitar información a las entidades públicas y privadas... f) Imponer sanciones administrativas... g) Constituirse en querellante en las acciones penales que se promovieran... h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos para su inscripción en el Registro creado por esta ley.

2. *El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.* (vetado)

3. *El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia* (vetado)

El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

Control administrativo

Decreto 1558/01

Art. 29.

1. Créase la Dirección Nacional de Protección de Datos Personales, en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos, como órgano de control de la Ley N° 25.326.

El Director tendrá dedicación exclusiva en su función, ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones.

2. La Dirección Nacional de Protección de Datos Personales se integrará con un Director Nacional, Nivel "A" con Función Ejecutiva I, designado por el Poder Ejecutivo Nacional, por el plazo de cuatro (4) años, debiendo ser seleccionado entre personas con antecedentes en la materia, a cuyo fin facúltase al Ministro de Justicia y Derechos Humanos, o a quien lo sustituya en sus funciones, a efectuar la designación correspondiente, como excepción a lo dispuesto por el ANEXO I del Decreto N° 993/91 y sus modificatorios.

Control administrativo

Ley 27.275 y DNU 746/17

La Ley 27.275, “de acceso a la información pública”, creó un órgano de control unipersonal, la “Agencia de Acceso a la Información Pública”, como ente autárquico con autonomía funcional y en el ámbito del Poder Ejecutivo nacional.

Su director cuenta con mandato por 5 años y puede ser reelegido por una única vez.

El director es propuesto y designado por el Poder Ejecutivo nacional mediante un procedimiento de selección público, abierto y transparente que garantice la idoneidad del candidato.

Mediante la Resolución 274-E/2017 del 19 de julio de 2017, el Poder Ejecutivo Nacional propuso a Eduardo Bertoni como director y el 17 de agosto de 2017 se realizó la audiencia pública para evaluar sus antecedentes.

El 29 de agosto de 2017, en cumplimiento de la ley, se publicó en el Boletín Oficial el Decreto 685/2017 que oficializó la designación de Eduardo Bertoni como director de la Agencia de Acceso a la Información Pública.

Control administrativo

Ley 27.275 y DNU 746/17

DNU n° 746/2017 (reforma a la Ley de Ministerios)

Nueva ubicación y funciones de la Agencia de Acceso a la Información pública

Nuevo art. 19 ley 27.275: La AAIP funcionará con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros y velará “por el cumplimiento de los principios y procedimientos establecidos en la presente ley, garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover medidas de transparencia activa y actuar como Autoridad de Aplicación de la Ley de Protección de Datos Personales N° 25.326.”

Agregado al art. 24: “t) Fiscalizar la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.”

Nueva atribución del Jefe de Gabinete de Ministros: Art. 16 del Título V, inc 32. “Garantizar el efectivo ejercicio del derecho de acceso a la información pública y controlar la aplicación de la Ley N° 25.326 de Protección de los Datos Personales.”

Control administrativo

Estructura de la AAIP

Estructura

De acuerdo a las competencias y funciones de la AAIP (art. 24 inc. a de la ley 27.275) se aprobó el 16/11/17 mediante la Decisión Administrativa JGM N°1002/17 el primer nivel organizativo de la estructura de la Agencia. En tal sentido se creó:

- a) la Dirección Nacional de Acceso a la Información Pública (DNAIP),
- b) la Dirección Nacional de Protección de Datos Personales (DNPDP) y
- c) la Dirección de Informática e Innovación (DII).

El 5/11/17 mediante la Resolución 1E/2017 se aprobó la estructura organizativa de segundo nivel operativo de la AAIP, conformada por dos direcciones con nivel 3 de función ejecutiva:

- a) Dirección de Políticas de Información Pública y
- b) Dirección de Protección de la Privacidad.

Control administrativo

Disposiciones DNPDP

- 18 sobre normas registrales
- 6 sobre régimen sancionatorio
- 5 sobre inspección y control
- 3 sobre guías de buenas prácticas y modelos
- 5 sobre organización interna
- 3 sobre el Registro Nacional “No llame”
- 9 sobre regulaciones especiales

(Implementación de Medidas de Seguridad en bases privadas; Confidencialidad de datos sensibles o de menores destinados a difusión pública: Aprobación de cláusulas contractuales tipo de transferencia internacional para la cesión y prestación de servicios. Declaración de países con legislación adecuada; Contrato modelo de transferencia internacional de datos personales con motivo de la cesión de datos personales; Contrato modelo de transferencia internacional de datos personales con motivo de prestación de servicios; Obligación de brindar información en comunicación de publicidad y formularios utilizados para la recolección de datos personales; Opción para el ejercicio del derecho de retiro o bloqueo ley N^a 25.326 en toda comunicación que se efectúe con fines publicitarios; Videovigilancia. Condiciones de licitud para su recolección y tratamiento; condiciones de licitud para la recolección de licitud para la recolección de datos personales a través de VANTs o drones).

Control administrativo

Dictámenes DNPDP

2003: 13

2004: 25 (69 contando aprobación de consentimientos informados investigaciones clínicas y farmacológicas)

2005: 22 (249 contando aprobación de consentimientos informados investigaciones clínicas y farmacológicas)

2006: 28 (285 contando aprobación de consentimientos informados investigaciones clínicas y farmacológicas)

2007: 20 (154 contando aprobación de consentimientos informados investigaciones clínicas y farmacológicas)

2008: 38

2009: 49

2010: 30

2011: 27

2012: 22

2013: 27

2014: 16

2015: 21

2016: 16

2017: 5

La ley 25.326

Control judicial

- 1) La vía judicial contra las decisiones del órgano de control se tramitan ante la justicia federal (art. 44)
- 2) La “acción de protección de los datos personales o hábeas data” está prevista contra organismos nacionales, y en los supuestos de bancos interconectados en redes nacionales o internacionales.

Está regulada entre los arts. 33 a 43 de la ley (procedencia, legitimación activa y pasiva, competencia, procedimiento aplicable, requisitos de la demanda, trámite, contestación del informe, ampliación de la demanda y sentencia) y sus disposiciones deben integrarse con otras de la ley, el CPCCN y la ley de amparo

- a) la posibilidad de desdoblamiento del trámite, en una fase inicial, para acceder a los datos objeto de tratamiento y en una segunda fase, para operar sobre ellos, para lo cual debe ampliarse la demanda, y
 - b) la regulación de cautelares específicas (en concreto, la anotación de controversia y el bloqueo de los datos cuestionados).
- 3) En los planos estadales el trámite de la acción se rige por las leyes locales de amparo o de hábeas data.

Tipos y subtipos de hábeas data

Acción, derecho y proceso de Hábeas Data

1) Es necesario distinguir entre:

- a) El hábeas data como acción procesal constitucional;
- b) El o los derechos de fondo que puede albergar y
- c) El o los procesos aptos para vehiculizarla.

2) En Latinoamérica es regulado:

a) sólo como derecho (Colombia),

b) sólo como garantía específica (Brasil, Argentina y Bolivia) o

c) como derecho y como garantía, ya sea de manera conjunta (Paraguay y Venezuela) o separada (Perú y Ecuador).

Tipos y subtipos de hábeas data

Tipología genérica:

Propios: (en defensa de los datos personales) o ***Impropios*** (en defensa del derecho de acceso a la información pública o el ejercicio del derecho de réplica).

Individuales: (ejercidos a título personal) o ***Colectivos*** (en representación plural, ya sea de un sector determinado –clase- o indeterminado de personas).

Ortodoxos (ejercidos por titulares de datos) o ***Heterodoxos*** (ejercidos entre responsables o encargados de tratamiento)

Tipos y subtipos de hábeas data

HÁBEAS DATA INFORMATIVO

No está destinado a operar sobre los datos registrados, solamente procura recabar la información necesaria para permitir a su promotor decidir a partir de ésta.

Subtipos:

EXHIBITORIO, dirigido a conocer qué datos de carácter personal se encuentran almacenados en determinado sistema de información y verificar el cumplimiento de los demás requisitos legales.

FINALISTA, reconocido a fin de determinar para qué se creó el registro y establecer si las categorías de los datos almacenados se corresponden con la finalidad declarada en el acto de su creación.

AUTORAL, cuyo propósito es inquirir acerca de quién proporcionó los datos con que cuenta la base o banco de datos.

LOCALIZADOR, destinado a indagar sobre la existencia y ubicación de bancos y bases de datos.

Tipos y subtipos de hábeas data

HÁBEAS DATA ADITIVO

Tiene por finalidad agregar al sistema de información datos de carácter personal no asentados en éste.

Subtipos:

ACTUALIZADOR, que es el diseñado para actualizar datos vetustos pero ciertos (v.gr., abogado designado juez, cuyo perfil de ejercicio profesional –y de identidad– es sustancialmente diferente),

ACLARATORIO, que es el destinado a aclarar situaciones ciertas pero que pueden ser incorrectamente interpretadas por quien acceda a los datos contenidos en el registro (v.gr., colocación del carácter de deudor no principal, o de que la deuda está controvertida en banco de datos de información crediticia), y

INCLUSORIO, cuya finalidad es la de operar sobre un registro que ha omitido asentar los datos del interesado, quien se encuentra perjudicado por dicha omisión (v.gr., el titular de un establecimiento hotelero cuyo dato no figura en un banco de datos oficial destinado a los turistas)

Tipos y subtipos de hábeas data

HÁBEAS DATA RECTIFICADOR O CORRECTIVO

Dirigido a corregir no sólo a los datos falsos (aquellos que no se corresponden siquiera mínimamente con la realidad), sino también a los inexactos o imprecisos (v.gr., el dato registrado es incompleto o puede dar lugar a más de una interpretación).

HÁBEAS DATA EXCLUTORIO O CANCELATORIO

Diseñado con el objeto de eliminar total o parcialmente los datos almacenados respecto de determinada persona, cuando por algún motivo no deben permanecer en el sistema de información de que se trate.

Ello puede ocurrir en múltiples supuestos, como en el caso de la registración de cualquier tipo de datos que no se correspondan con la finalidad del banco o base de datos, de datos falsos que el registrador se niega a rectificar o actualizar, del tratamiento ilegal de los datos sensibles, etc.

Tipos y subtipos de hábeas data

HÁBEAS DATA RESERVADOR

Relacionado con los datos sensibles, tiende a asegurar que un dato correcta y legítimamente almacenado sea mantenido en confidencialidad y en consecuencia sólo se comuniquen a quienes se encuentran legalmente autorizados y exclusivamente en los supuestos en que tales sujetos han sido habilitados para ello.

HÁBEAS DATA DISOCIADOR

Opera cuando los datos deben ser sometidos a técnicas de disociación, como lo disponen diversas normas (v.gr. secreto estadístico)

HÁBEAS DATA ENCRIPADOR

A fin de brindar mayor seguridad y agilidad a la operación sobre determinados datos puede ser necesario acudir a técnicas de encriptación, lo que implica que el dato queda “oculto” para quienes no cuenten con la clave para descifrarlos.

Tipos y subtipos de hábeas data

HÁBEAS DATA BLOQUEADOR

Emparentado al hábeas data reservador y al exclutorio. Procura “trabar” el tratamiento –generalmente en lo relativo a la transmisión o cesión a terceros– de los datos asentados en un registro.

HÁBEAS DATA ASEGURADOR

A fin de que se adopten las medidas de seguridad necesarias respecto del sistema de información a fin de evitar fugas o alteraciones ilegales de la información almacenada.

HÁBEAS DATA RESARCITORIO

En algunos casos aislados pueden incorporarse pretensiones resarcitorias adicionales a las principales, como la rectificación o exclusión de los datos.

Tipos y subtipos de hábeas data

HÁBEAS DATA IMPUGNATIVO

Su objetivo es impedir tratamientos o modificar el resultado de éstos cuando incidieron decisivamente en decisiones judiciales o administrativas

Subtipos:

OBJETOR DE TRATAMIENTOS, que se refiere al derecho del registrado a oponerse al tratamiento de sus datos, y

IMPUGNADOR DE VALORACIONES PERSONALES AUTOMATIZADAS, que refiere a la facultad del registrado para impugnar las decisiones judiciales o administrativas fundadas exclusivamente en valoraciones que de sus datos realice el registrador basado exclusivamente en el tratamiento automatizado de datos personales o para descubrir y eventualmente cuestionar las técnicas algorítmicas que determinaron determinado perfilado, en el ámbito privado.

Tipos y subtipos de hábeas data

HÁBEAS DATA BLOQUEADOR

Emparentado al hábeas data reservador y al exclutorio. Procura “trabar” el tratamiento –generalmente en lo relativo a la transmisión o cesión a terceros– de los datos asentados en un registro.

HÁBEAS DATA ASEGURADOR

A fin de que se adopten las medidas de seguridad necesarias respecto del sistema de información a fin de evitar fugas o alteraciones ilegales de la información almacenada.

HÁBEAS DATA RESARCITORIO

En algunos casos aislados pueden incorporarse pretensiones resarcitorias adicionales a las principales, como la rectificación o exclusión de los datos.

La responsabilidad de los servicios de intermediación (proveedores de acceso y de contenido) en la jurisprudencia de la Corte Suprema

1. “Prete, Priscila c/Yahoo! de Argentina S.R.L. s/Daños y perjuicios” (responsabilidad de los buscadores sitios y de imágenes).
2. “Da Cunha, Virginia c/ Yahoo!” (responsabilidad de los buscadores de sitios y de imágenes)
3. “Jujuy.com” (responsabilidad de los bloggers).
4. “Sujarchuk, Ariel Bernardo c/ Warley, Jorge Alberto s/ daños y perjuicios” (responsabilidad de los bloggers)
5. “Belén Rodríguez” (2014)
 - La libertad de expresión se aplica a Internet y a los buscadores,
 - No hay responsabilidad objetiva como se pretendió en el caso Jujuy.com.
 - No hay obligación de monitorear contenidos
 - Responsabilidad es subjetiva a partir del conocimiento efectivo por parte del buscador del contenido ilícito mediante el sistema de “notice & take down”. Distingue entre contenidos detectables a la vista y los restantes.
 - El buscador de imágenes no genera responsabilidad pues es un mero vínculo entre la imagen reducida y la imagen disponible en el sitio original (al igual que el buscador de texto).