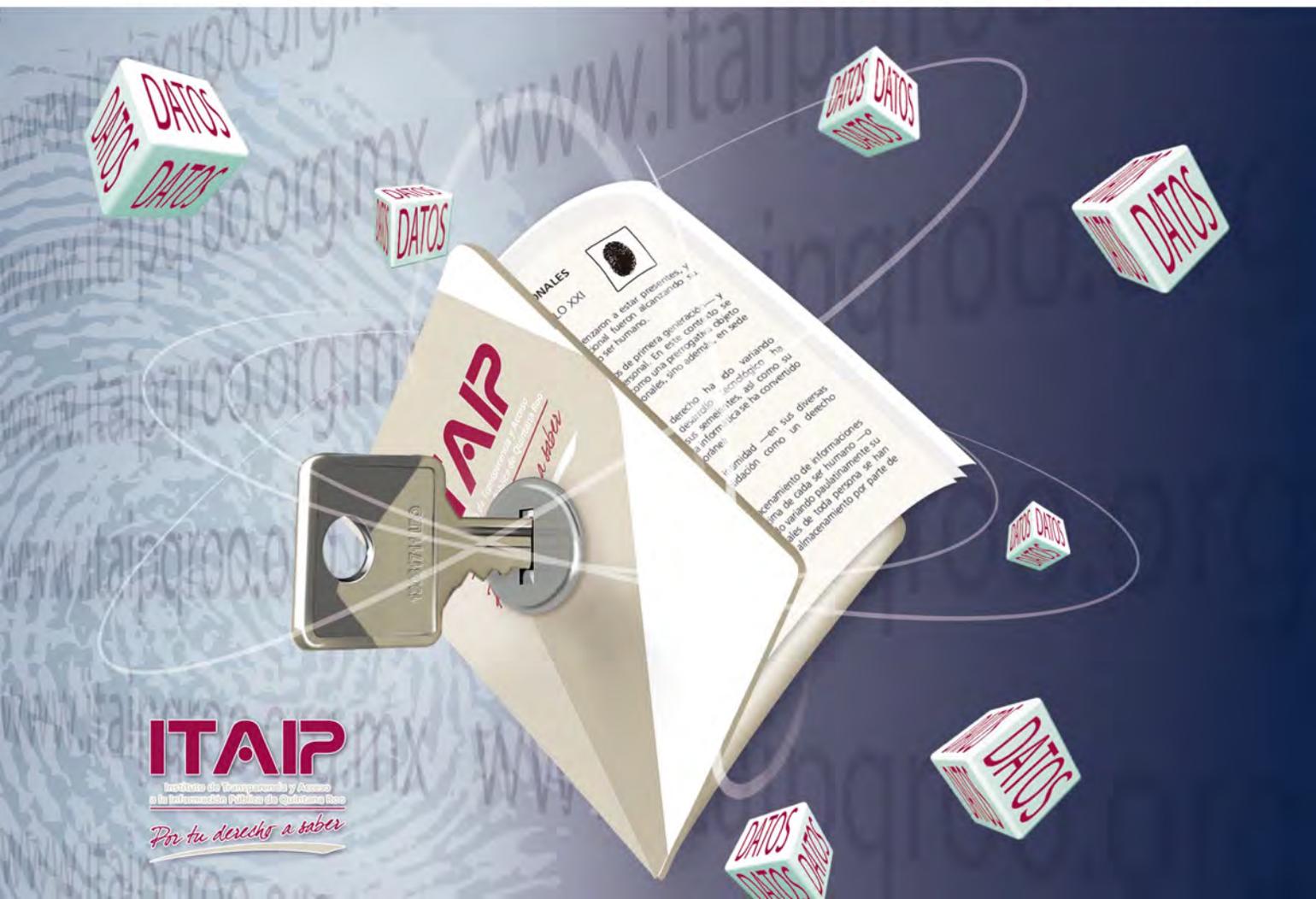


PROTECCIÓN DE DATOS PERSONALES COMO MEDIO DE PREVENCIÓN DEL DELITO

07

Idearios de Transparencia

Dra. Ximena Punte de la Mora



ITAIP

Instituto de Transparencia y Acceso
a la Información Pública de Guatemala

Por tu derecho a saber

PROTECCIÓN

DE DATOS PERSONALES

COMO MEDIO DE PREVENCIÓN DEL DELITO

ITAIIP

**Instituto de Transparencia y Acceso
a la Información Pública de Quintana Roo**

Por tu derecho a saber



Primera Edición: Año 2011
Número Siete de la Colección Idearios de Transparencia de la Colección Poder Ciudadano:
del Concepto a la Cultura

Registro ISBN (Número Internacional Normalizado del Libro) ante la Dirección de Reservas de Derechos del Instituto Nacional del Derecho de Autor (INDAUTOR) EN TRÁMITE, según formato de solicitud de asignación de número ISBN-02-A, de fecha 14 de enero de 2011, recibido en las oficinas del INDAUTOR el 25 de enero de 2011 y al que se le asignó el número de trámite 024839 y número de folio 000041.

Coordinadora de la Impresión: MDC. Leyda María Brito Alpuche

CONTENIDO

- 1. Nuevos escenarios para el Derecho: las Tecnologías de la Información y la Comunicación**
- 2. Derecho a la protección de datos personales**
 - a) Antecedentes
 - b) Diferentes “generaciones” del derecho a la protección de datos personales
 - c) Concepto y variantes de la protección de datos personales: autodeterminación informativa,
 - d) Libertad informática, habeas data
 - e) Objeto
- 3. Preguntas básicas del derecho a la protección de datos personales**
 - a) ¿Qué se protege?
 - b) ¿De qué se protege?
 - c) ¿De quién se protege?
 - d) ¿Cómo se protege?
- 4. Configuración del derecho a la información y protección de datos personales, como derechos humanos en el Sistema Jurídico Mexicano**
- 5. Acceso a la información judicial en México, aspecto fundamental de la democracia**
- 6. Problemas actuales de la política criminal: Protección de Datos Personales como medio de prevención del delito**
- 7. Información reservada y confidencial como límite al acceso a la información**
- 8. Las redes sociales y la comisión del delito**
- 9. Policía, Estado de Derecho y Código de Buenas Prácticas en México**
- 10. Fuentes consultadas**

1. Nuevos escenarios para el Derecho: Las Tecnologías de la Información y la Comunicación

En la actualidad podemos afirmar que estamos viviendo en una “nueva revolución comunicativa a la vez que económica y productiva”,¹ así, el advenimiento de redes digitales y de la informática, significa un importante paso en términos evolutivos e incluso históricos para el ser humano. Este modelo que ha seguido la sociedad actual en la mayor parte del mundo, se caracteriza por la importancia social, económica y cultural que adquieren las nuevas tecnologías de la información y las comunicaciones. Es, en este escenario, en el que surge un nuevo derecho, el derecho a controlar esta información a partir del almacenamiento, tratamiento y transmisión de

datos personales, contenidas en bases de datos específicamente por medio de la llamada “tecnología informática”,² es decir, por medio de las computadoras, por la posibilidad prácticamente ilimitada de su disposición, alteración, cesión, y elaboración de perfiles informáticos con base en la información personal.³



1. Martínez Martínez, Ricard, *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas, 2004, p. 45.

2. Este término fue acuñado en 1962 por Philippe Dreyfus, y “puede definirse globalmente como la tecnología de la información; es decir, no sólo su tratamiento técnico por medio de un instrumento, como ocurría ya con las distintas formas de registro mecánico, con los archivos, mecanográficos de funcionamiento manual, con los aparatos criptográficos; sino su transposición a un proceso puramente intelectual de control, de movimiento combinatorio y de traducción a una nueva fórmula”, Frosini, Vittorio, *Informática y Derecho*, Bogotá, Temis, 1988, p. 32.

3. Aunque éste es un problema que surge con el advenimiento de la tecnología informática reciente, existen antecedentes que nos indican los daños ocurridos a las personas cuyos datos se encuentran registrados en archivos, que se remontan a 1919 con la Constitución alemana de Weimar, que en su artículo 129, señalaba el deber de nombrar a los funcionarios de por vida, de que en su expediente no se anotarían los hechos que le fueran desfavorables (sino hasta después de haberle dado ocasión de justificarse respecto a ellos), además reconoce que “el funcionario tendrá derecho a examinar su expediente personal”. Otros antecedentes los podemos encontrar desde la época de Aristóteles el cual consideraba los archivos como indispensables en un Estado modelo; Napoleón entendía que un buen archivero era tan importante como un buen general de artillería. Aunque desde otras épocas pasadas existían los registros de la información personal, el peligro de invadir una esfera de intimidad personal por el manejo inadecuado de esta información se consideraba mínimo. Véase Puccinelli, Oscar, *Protección de Datos de Carácter Personal*, Buenos Aires, Astrea, 2004, p. 11.

Sin embargo, el peligro en el manejo que se le puede dar a la información personal se acelera con el uso de las nuevas tecnologías de información, las cuales “dramáticamente reducen el costo de generar, almacenar, transmitir y procesar información en todos los sectores de la economía”,⁴ transformando “la manera de concebir la organización y la estructura misma de nuestras sociedades”.⁵ La técnica incide en la forma social y también en cuestiones estructurales, es decir, incide en las pautas de comportamiento que conocemos con el nombre de cultura. “Las dimensiones social, cultural y tecnológica se relacionan y se mezclan para hacer florecer la comunicación humana”.⁶

Hay autores, como Fernández Rodríguez, que analizan más allá de la conexión tecnológica y se centran en una interconexión de

los seres humanos a través de la tecnología inaugurando la “era de la inteligencia interconectada”.⁷

En este contexto, podemos señalar que el tratamiento automatizado de la información facilita la organización y disposición de la misma, pero también facilita las potenciales lesiones a los derechos de las personas, y ello ocurre con la utilización de cualquier tipo de datos, especialmente los datos de carácter nominativo o personal.



4. Wolfed, David A., *Globalization, Information and Communication Technologies and Local and Regional Systems of Innovation*. Toronto, Department of Political Science, University of Toronto, 2004 p. 2.
5. Cremades García, Javier (Coord.), *Régimen jurídico de Internet*, Madrid. La ley, 2001. p. 120.
6. Fernández Rodríguez, José Julio, *Lo público y lo privado en Internet*. Intimidad y libertad de expresión en la red, México, Universidad Nacional Autónoma de México, 2004, p. 15.
7. Tapscot, Don, *The Digital Economy: Promise and Peril in the Age of Network Intelligence*, Nueva York, McGraw-Hill, 1996. p. 9.

2. Derecho a la protección de datos personales

a) Antecedentes

Desde mediados del siglo XX, el desarrollo de las tecnologías de la información hacía posible ya la habilidad para computarizar ciertos procedimientos y decisiones, tal y como sucedió en Alemania en 1958 referente a ciertos montos que los empleados podían deducir del pago de sus impuestos.⁸ El primer claro ejemplo de procesamiento de información que se produjo en la Administración Pública fue en 1972 cuando el gobierno noruego decidió implementar un sistema donde el ciudadano estaba facultado para solicitar un beneficio social a fin reducir los costos de compra de vivienda. El solicitante sólo debería introducir su número de identificación personal, el sistema procesaba

automáticamente la información y determinaba si la persona tenía o no acceso a este beneficio con base a su información personal, impuestos generados, sistema de seguridad social, costos de construcción determinados, entre otros datos.⁹

Con estos antecedentes, podemos mencionar que el derecho a la protección de datos personales tiene dos características que lo particularizan: que se trata de un derecho de reciente configuración, y que además, su delimitación se ha producido con el paso del tiempo, razón por la cual ha tomado su derecho fundamental en los últimos años.

El derecho a la protección de datos personales se formula por

primera vez con el término «autodeterminación informativa» en Alemania, con una sentencia del Tribunal Constitucional Alemán del 15 de diciembre de 1983 (*Informationselle Selbstbestimmungsrecht*) al declarar la inconstitucionalidad de la Ley de Censo de la Población (*Volkszählungsgesetz*).¹⁰ Dicha sentencia establece una definición y naturaleza del derecho a la autodeterminación informativa, enunciando en su fundamento jurídico segundo lo siguiente: “El derecho general de la personalidad... abarca... la facultad del individuo, derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida... la

8. El monto mayor a deducir estaba estipulado en 562 marcos alemanes, modificándose posteriormente a 564 marcos alemanes, debido a que la primera cantidad no se podía dividir en los 12 meses del año, por lo tanto el sistema tenía que retener todo lo que tenía que ser deducido en los 12 meses en fracciones de marcos para hacer la suma de determinación exacta. En cambio 564 marcos puede ser dividido en 12, lo que la suma de retención de impuestos sea la misma en cada mes y no se tenga que hacer una determinación especial.

9. Se elaboraron aproximadamente 100,000 decisiones anualmente, estando las apelaciones limitadas a la revisión de los datos conforme a los que se había realizado tal determinación. Jon Bing, “Code, Access and Control, en Klang Mathias y Murria Andrew, Human Rights in the Digital Age, Great Britain, Gals House Press, 2005, p. 204.

10. Esta ley pretendía requerir los datos sobre los nombres de los ciudadanos, fecha de nacimiento, ideología política, religión, nacionalidad, tipo de convivencia con otras personas, domicilio, clase de trabajo, ingresos, profesión aprendida, duración del periodo de estudios, dirección del trabajo, los medios de locomoción utilizados para ir al trabajo, tiempo promedio utilizado para ese recorrido, duración de la jornada laboral, clase, extensión, dotación y usos de la vivienda, número y uso de las habitaciones, cuantía de los alquileres mensuales. Además reprime con la aplicación de sanciones cualquier negativa a suministrar la información. El Tribunal Constitucional superó los parámetros anteriores vinculados a la teoría de las esferas, consagrando la tesis de que ya no existían datos sin interés, sino que todos merecían protección en tanto sirvieran para configurar una radiografía de los ciudadanos. Véase Gils Carbó, Alejandra M., *Régimen Legal de las bases de datos y habeas data*, Buenos Aires, Editorial La Ley, 2001, p. 14.

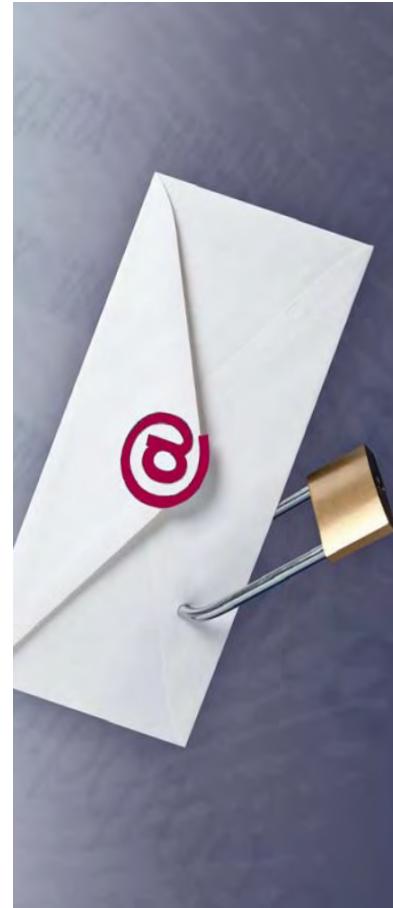
eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos de protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión de sus datos personales".¹¹

En dicha sentencia, el Tribunal Constitucional Alemán desarrolló criterios definidos para la protección de datos personales, los cuales mencionaremos de manera breve:

- Cada ciudadano tiene el derecho originario de decidir por sí mismo sobre la revelación y utilización de sus datos personales.
- Deja de existir el término "fecha irrelevante" bajo las condiciones del procesamiento automatizado de los datos, puesto que toda fecha relacionada con una

persona se encuentra bajo la protección de la Constitución, independientemente si se trata de una información sensible o no.

- Los ciudadanos deben saber quién, qué y con qué finalidad alguna persona sabe sobre él.
- Las limitaciones sobre el derecho a la autodeterminación informativa requieren el fundamento explícito en una ley.
- La recolección y tratamiento de los datos personales se encuentra bajo una estricta finalidad, los datos solamente pueden ser recolectados y guardados para un fin determinado; la recolección de datos sin una finalidad determinada es ilícita.¹²



11. Este término es empleado también por Lucas Murillo de la Cueva, Pablo, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990, pp. 27 y ss. Cabe señalar a principios de la década de los 70's se había introducido en Alemania el término Automationsgerechten Rechtssetzung (legislación orientada a la automatización) a la introducida por Fiedler y otros, considerados como "padres de la informática y el derecho". Klang Mathias y Murria Andrew, *Human Rights in the Digital Age*, Great Britain, Gals House Press, 2005, p. 203.

12. Cfr. García Corona, Irene Gabriela, *"La protección de datos personales en la Comunidad Europea desde la perspectiva alemana y española"*, en *Derecho de acceso a la información pública*, Ernesto Villanueva e Issa Pla (eds.), México, UNAM, 2004, pp. 88 y ss. en concreto p. 103.

b) Diferentes “generaciones” del derecho a la protección de datos personales

Por esta razón, destacaremos el corto pero intenso camino que ha seguido la configuración del derecho a la protección de datos personales para ser considerado como fundamental siguiendo el esquema que propone Puente Escobar,¹³ considerando seis etapas sucesivas:

1. Orígenes de la protección de datos. En 1967 en el seno del Consejo de Europa se constituye una comisión consultiva para estudiar las tecnologías de la

información y su incidencia en los derechos de las personas, trabajo que se plasma en la resolución 509 de la Asamblea del Consejo de Europa sobre los derechos humanos y los logros científicos y tecnológicos que puede ser considerada como el origen de lo que posteriormente se le conoce como protección de datos personales.¹⁴

2. Primeros desarrollos en la protección de datos (leyes de primera generación, 1970 – 1975). En este periodo las disposiciones normativas se limitan a crear instrumentos de protección para restringir el uso desenfrenado de la tecnología. Así, la primera norma vinculante en esta materia le corresponde al *Land de Hesse*, del 7 de octubre de 1970.¹⁵

Por su parte la primera ley nacional sobre protección de datos fue aprobada por el Parlamento Sueco el 11 de mayo de 1973, la

cual incorpora bases de datos públicas y privadas, contiene principios de protección y crea la primera autoridad específica en la materia (Datainspektionen). En 1974 en Estados Unidos se promulga la Privacy Act, pero sólo incorpora las bases de datos de organismos públicos.

3. Nuevos desarrollos en la protección de datos (segunda generación, 1975 – 1980). En este periodo se observa la necesidad de una protección de la información personal, especialmente a los datos sensibles. En el periodo comprendido entre 1977 y 1979 la República Federal de Alemania, Francia, Dinamarca, Austria y Luxemburgo adoptan leyes nacionales de protección de datos de carácter nacional.

Al mismo tiempo, el Parlamento Europeo aprueba en 1979 la Resolución de 8 de mayo sobre la tutela de los derechos del individuo

13. Puente Escobar, Agustín, “Breve descripción histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal”, en Piñar Mañas, José Luis, et. al., Protección de Datos de Carácter Personal en Iberoamérica, Valencia, Tirant Lo Blanch, 2005, pp. 37 – 67, en concreto pp. 39 y ss.

14. Se considera como el origen de este derecho puesto que vinculó las nuevas tecnologías con la intimidad de las personas, específicamente en lo que respecta al derecho a la intimidad.

15. Esta ley alemana es de carácter estatal (*lander*) no nacional, se refiere exclusivamente a los ficheros de organismos públicos y crea la figura del Comisario Parlamentario de Protección de Datos, con las funciones similares a las de un *Ombudsman*.

frente al creciente progreso técnico en el sector de la informática primer documento en materia de protección de datos dentro de lo que después sería la Unión Europea.

La madurez de la protección de datos (tercera generación, 1980 – 1998). En este periodo se contemplan una serie de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como medidas de seguridad por parte de los responsables de los mismos.

En el nivel internacional se crea la Recomendación de la OCDE sobre la Circulación Internacional de datos personales para la protección de la intimidad (conocida como las Directrices de la OCDE) en septiembre de 1980, y el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento de sus datos de carácter personal, el 28 de enero de 1981. En el ámbito

internacional, se aprueban leyes en Suiza (1981), Gran Bretaña (1984), Finlandia (1987), Holanda (1988), Islandia (1989), Alemania unificada (1990), Portugal (1991) y España (1992). En Europa Central y Oriental se empieza a reconocer este derecho a nivel constitucional siendo las primeras leyes las de Hungría y Checoslovaquia (ambas en 1992).

Durante este tiempo, en el ámbito de la Unión Europea, se gesta la adopción del texto de mayor relevancia en el marco de la protección de datos, se trata de la Directiva 95/46/CE de 24 de octubre, 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.

5. Unificación de las leyes de protección de datos y nuevos desarrollos (1998 – 2000). Debido al impacto que tuvo la Directiva 95/46/CE en el establecimiento de una legislación uniforme en la

materia, esta etapa se caracteriza por el incremento de la cooperación entre los Estados miembros y de las instituciones comunitarias con terceros Estados. Además países de Europa Central y Oriental como Polonia, la República Checa, Hungría o Eslovenia adoptan nuevas leyes en este periodo.

6. Situación actual. La configuración de la protección de datos como derecho fundamental. Situación que se logra principalmente por dos razones: En el ámbito Europeo, el derecho a la protección de datos es reconocido como derecho fundamental por el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea, signada en Niza el 7 de diciembre de 2000. Además del pronunciamiento de sentencias que le otorgan a este derecho un ámbito propio como las Sentencias del Tribunal Constitucional Español 290/2000 y 292/2000.

c) Concepto y variantes de la protección de datos personales: autodeterminación informativa, libertad informática, habeas data.

En la actualidad, ante el imparable desarrollo social, específicamente el avance en la sociedad de la información, “se exigen respuestas jurídicas precisas, adecuadas a los nuevos fenómenos sociales que la vida moderna ofrece a las personas”,¹⁶ configurándose en un nuevo derecho denominado “derecho a la protección de datos personales”¹⁷ “derecho a la

intimidad informática”,¹⁸ “derecho a la autodeterminación informativa”,¹⁹ “derecho a la libertad informática”²⁰ entre otras denominaciones.

El poder informático se refleja en la capacidad que tienen las computadoras de acumular una gran cantidad de información sobre cualquier aspecto de la vida cotidiana. Pierini apunta sobre algunas de las consecuencias que tiene el uso de la información proveniente de registros electrónicos al señalar que esta información que es proporcionada por los mismos individuos a bancos de datos públicos y privados²¹ para razones determinadas, puede ser utilizada sin su autorización para fines no establecidos previamente invadiendo la “zona de reserva del individuo y por consiguiente afectando su derecho a la privacidad”²². Más adelante, el mismo autor menciona también

que aquél que posea la mejor tecnología será capaz de concentrar el mayor número de información referida a la intimidad de las personas y podrá transformarse en un dictador de sus actos, debido a que contará con la información de sus datos necesarios, “pudiendo ejercer incluso coacción moral y coaccionar su acción bajo la amenaza de la publicidad de datos reservados o sensibles con el consecuente perjuicio individual y general”.²³

Los instrumentos tecnológicos permiten ampliar y multiplicar las fuentes de conocimiento e información de quienes los poseen, dificultando correlativamente las posibilidades de defensa de quienes desean sustraerse a la curiosidad ajena, es por ello que en opinión de Fernández Segado, “ya no se configura el derecho a la privacidad tan solo como una

16. Herrán Ortiz, Ana Isabel, *El derecho a la protección de datos personales en la Sociedad de la Información*, Bilbao, Universidad de Deusto, 2003, p. 13

17. Herrán Ortiz, Ana Isabel, op. cit., p. 12.

18. Ruiz Miguel, Carlos, *La configuración constitucional del derecho a la intimidad*, Madrid, Tecnos, 1995, pp. 94 y ss.

19. Término que consagró la Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983 (*Informationale Selbstbestimmungsrecht*).

20. Frosini, Vittorio, *Informática y Derecho*. Bogotá, Temis, 1988, pp. 35 y ss.

21. La noción actual de bancos de datos la podemos definir como depósitos electrónicos de datos y de información. Cabe hacer un importante señalamiento entre los conceptos de dato e información. El término dato hace referencia a cualquier conjunto de letras, números o signos que tienen al menos un significado. Los datos conforman entes reales y objetivos, lo que significa que existen independientemente de sus potenciales usuarios. La información, en cambio, puede ser definida como todo dato que interviene, desencadena o participa en una decisión. Cfr. Pierini, Alicia, et al., op. cit., p. 28.

22. Pierini, Alicia, et al., et al., *Habeas Data. Derecho a la intimidad*, Buenos Aires, Editorial Universidad, 2002, p. 221.

23. Pierini, Alicia, et al., op. cit., p. 223.

separación y defensa del individuo como parte de la sociedad, sino como un nuevo derecho social de libertad; no es ya únicamente el derecho a negar la información sobre sí mismo, sino también el derecho a pretenderla, es decir, la libertad informática se nos perfila como un derecho de disponer de la información, de preservar la propia identidad informática, consentir, controlar, y en su caso, rectificar los datos informativos concernientes a la propia personalidad”.²⁴

Pérez Luño por su parte lo llama «libertad informática» aludiendo a un nuevo derecho de tercera generación, que tiene por finalidad “garantizar la facultad de las personas de conocer y acceder a las informaciones que les conciernen archivadas en bancos de datos; controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o

indebidamente procesados, y disponer sobre su transmisión”,²⁵ con este derecho, “el individuo tutela su propia identidad informática, concretándose en las garantías de acceso y control de las informaciones procesadas en bancos de datos por parte de las personas a las que conciernen”.²⁶ Westin a pesar de que utiliza el término de «*information control*» para referirse a la protección de datos personales, lo conceptualiza de manera similar al apuntar que se trata del “derecho de los individuos, grupos e instituciones para determinar por sí mismos cuándo y con qué extensión la información acerca de ellos es comunicada a otros”²⁷.

Frosini se refiere a este derecho como una nueva forma que presenta el derecho a la libertad personal, es decir, “el derecho de controlar las informaciones sobre la propia persona, e incluso se pronuncia por una nueva denominación: el derecho de

«*habeas data*»”. Con el nombre de *habeas data* se refieren Ekmekdjian y Pizzolo al conceptualizar “un instrumento diseñado para controlar la calidad de la información personal contenida en bancos de datos, corregir o cancelar los datos inexactos o indebidamente procesados y disponer sobre su posible transmisión”.²⁸

Sin embargo, debemos puntualizar que cuando se alude al término de *habeas data* se hace referencia a “una garantía procesal constitucional que tiende en realidad a la protección judicial específica de aquellos derechos a la autodeterminación y a la libertad informática”.²⁹ *El habeas data* “se erige en una acción – proceso de naturaleza cautelar de amparo constitucional, que con carácter sumario y extraordinario, permite hacer efectivos derechos específicos en relación a «información sensible no registrable»: derecho de acceso,

24. Fernández Segado, Francisco, *La dogmática de los derechos humanos*, Lima, Ediciones Jurídicas, 1994, p. 277.

25. Pérez Luño, Antonio Enrique, *Los derechos humanos en la sociedad tecnológica*, en Lozano Mario et al., *Libertad informática y leyes de protección de datos personales*, Madrid, CEC, 1989, p. 140.

26. Pérez Luño, Antonio Enrique, *Manual de Informática y Derecho*, Barcelona, Ariel, 1996, p. 72.

27. Westin, Alan F., *Privacy and Freedom*, New York, Atheneum, 1967, p. 7 y ss.

28. Ekmekdjian Miguel y Pizzolo, Calogero, “*Habeas data*”. El derecho a la intimidad frente a la revolución informática, Buenos Aires, Depalma, 1996, p. 23.

29. Puccinelli, Óscar, *El Habeas Data* ..., p. 102.

30. Zúñiga Urbina, Francisco, “El derecho a la intimidad y sus paradigmas” *Ius et Praxis*, Chile, Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, año 3, núm. 1, p. 301.

derecho de actualización de datos, derecho a la rectificación, derecho a la confidencialidad y derecho a la exclusión”;³⁰ por lo tanto, más que un derecho el habeas data constituye una garantía procesal constitucional de carácter judicial (en los países que lo tienen contemplado) pero con características propias.³¹

Este derecho es llamado también «protección de datos personales», y se refiere a “aquella parte de la legislación que protege un derecho fundamental de libertad, en particular el derecho individual a la intimidad respecto al procesamiento manual de los datos”.³² Al respecto, Téllez Aguilera considera que “son elementos característicos del contenido y definición de este derecho fundamental los derechos del afectado a consentir sobre el uso y la recogida de sus datos personales y a saber de los mismos”.³³ Los derechos más

importantes son conocidos mediante las siglas ARCO: Acceso, Rectificación, Cancelación y Oposición.

Cualquiera que sea la terminología que se adopte, podemos decir que la protección de datos personales considerada como la protección jurídica de las personas en lo que concierne al tratamiento de sus datos de carácter personal, o de otra forma, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para confeccionar una información que, identificable con él, afecta a su entorno personal, social o profesional, en los límites de su intimidad, incide en un “derecho fundamental de elevado contenido”,³⁴ por las variantes que representa y por la amplitud de sus postulados.

d) Objeto

Una primera aproximación a la protección de datos personales podría conducir al equívoco de que este término ha sido diseñado para tutelar los datos en sí, pero esta precisión no es correcta. El objeto que pretende tutelar la protección de datos personales en sentido amplio es la seguridad jurídica del individuo, para que su información sea empleada exactamente para los fines que autorizó de manera expresa; en un sentido más restringido se protege “un conjunto de bienes jurídicos que son específicamente atacados por las actividades de recolección, tratamiento y transmisión de los datos nominativos a partir de una serie de principios, derechos y garantías que suelen establecerse en las normas específicas que lo regulan”.³⁵

Cabe aclarar las sensibles variaciones que tiene la

31. Para una visión más amplia del impacto de la figura del habeas data en Iberoamérica véase Puente de la Mora, Ximena, “Habeas data como mecanismo de protección de los datos personales en Iberoamérica”, De Iure, Colima, Instituto Universitario de Investigaciones Jurídicas, Universidad de Colima, año 5, segunda época, núm., 3, 2005.

32. Hondius, Fritz W., “A decade of international Protection”, en Netherlands of International Law Review, vol. 30, núm., 2, 1983, p. 105.

33. Téllez Aguilera, Abel, Nuevas tecnologías, intimidad y protección de datos, Madrid, Edisofer, 2001, p. 75.

34. Davara Rodríguez, Miguel Ángel, La protección de datos personales en el sector de las telecomunicaciones, Madrid, Fundación Airtel, 2000, p. 9.

35. Puccinelli, Oscar, *El Habeas Data...*, p. 103.

36. Estadella Yuste, Olga, *La protección a la intimidad frente a la transmisión internacional de datos personales*, Madrid, Tecnos, 1995, p. 32.

configuración jurídica del derecho a la intimidad informática o protección de datos personales en los distintos países que lo regulan. Al respecto, Estadella Yuste aclara que aunque el derecho individual a la protección de datos puede variar en algunos aspectos en las leyes nacionales o internacionales, este derecho mantiene ciertas características comunes en el sentido de que se encuentra relacionado con “aquellos datos que hacen referencia a una persona física identificada o identificable y que han sido objeto de una actividad realizada, en parte o en su totalidad con ayuda de procedimientos automatizados, es decir, operaciones de registro de datos, aplicaciones a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión”.³⁶

Debido a lo anterior, este derecho de protección de datos personales

se entiende como un “derecho instrumental”.³⁷

Podemos decir entonces que el objeto que se pretende tutelar es la persona, frente a las afectaciones de sus derechos fundamentales que pudieran sufrir a partir del tratamiento de datos por parte de terceros, que pueden ser las autoridades estatales, las empresas privadas e incluso los particulares.

e) Características

La protección de datos personales entendida como la protección jurídica de las personas en lo concerniente al tratamiento de sus datos, también puede entenderse como “el amparo debido a los ciudadanos contra la posible utilización por terceros en forma no autorizada, de sus datos personales susceptibles de

tratamiento, para confeccionar una información que, identificable con él afecta a su entorno personal, social o profesional, en los límites de su intimidad”,³⁸ cualquiera que sea la definición que pueda emplearse incide directamente en un derecho fundamental de elevado contenido. Es por este mismo contenido que el derecho a la protección de datos posee características que lo distinguen de los otros derechos vinculados como el derecho a la información, tales como:

a) que los datos sean susceptibles de tratamiento o que se encuentren en un soporte susceptible de tratamiento (es decir que sea fácil su manipulación);

b) que se tenga la posibilidad de identificar el resultado del tratamiento de los datos con su titular (excepto en el caso de

37. Puccinelli, Óscar, *El Habeas Data...*, p. 69.

38. Téllez Aguilera, Abel, *Nuevas Tecnologías, Intimidad y Protección de Datos*, Madrid, Edisofer, 2001, p. 75.

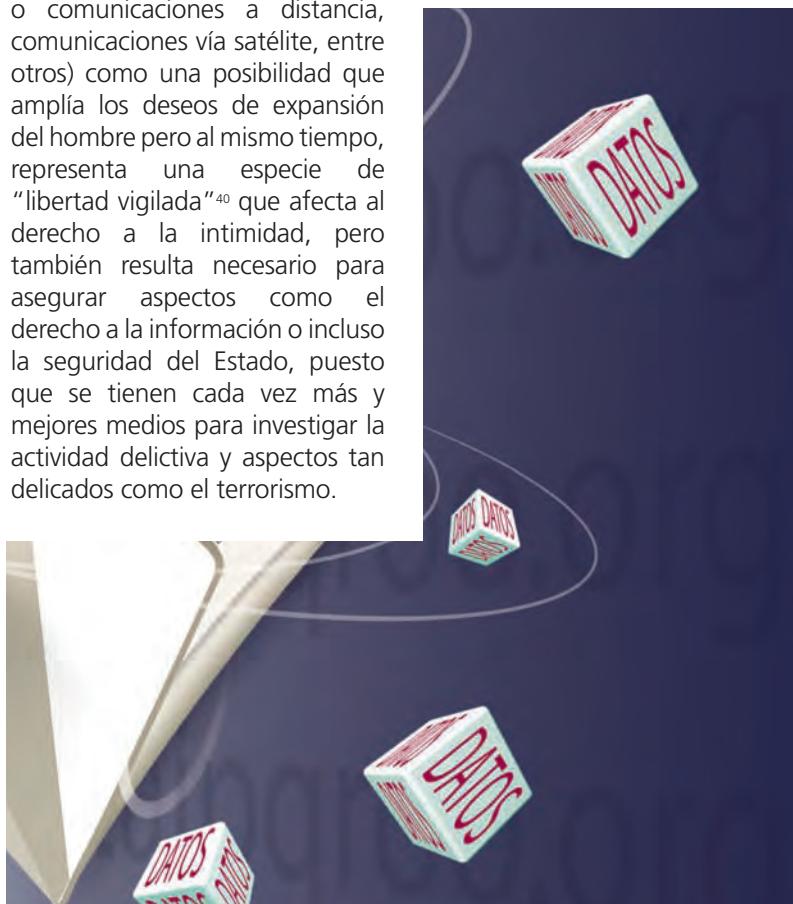
39. Conde Ortiz, Concepción, *La protección de datos personales*, Madrid, Dhykinson, 2005, p. 29.

finés estadísticos no se tutela la información si no se vincula con la persona que la proporcionó, en el de fines históricos o en cualquier otro que se someta a la información contenida en la base de datos a un proceso de disociación que hagan imposible verificar el titular de los datos); y, finalmente,

c) que el manejo o acceso a los datos resulte sin consentimiento de su titular.³⁹

El tratamiento de los datos comprende un conjunto de 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, y obliga a considerar el desarrollo de las tecnologías de la información (telecomunicaciones,

o comunicaciones a distancia, comunicaciones vía satélite, entre otros) como una posibilidad que amplía los deseos de expansión del hombre pero al mismo tiempo, representa una especie de "libertad vigilada"⁴⁰ que afecta al derecho a la intimidad, pero también resulta necesario para asegurar aspectos como el derecho a la información o incluso la seguridad del Estado, puesto que se tienen cada vez más y mejores medios para investigar la actividad delictiva y aspectos tan delicados como el terrorismo.



40. Gonzáini Osvaldo, Alfredo, *Habeas data*. Protección de datos personales. Buenos Aires, Ribinzal Culzoni, 2001. p. 71.

41. Esta consideración es importante puesto que si una persona acude a un Restaurante y le solicitan, sólo para fines de calidad, que llene una encuesta de preferencia del mismo, los datos proporcionados solamente deberán utilizarse para este fin y no para fines mercantiles o para la utilización de esta información por parte de alguna otra empresa.

3. Preguntas básicas del derecho a la protección de datos personales

a) ¿Qué se protege?

La protección de datos personales busca controlar o defender la autodeterminación informativa, es decir, que el uso de la información personal contenida en bases de datos sea exactamente el que el individuo autorizó. En torno a este objetivo, podemos decir que se tutelan principalmente los siguientes aspectos:

- 1) La decisión del individuo de proporcionar o no los datos que revelen información personal y en su caso la utilización que se hará de los mismos;
- 2) Se protege que los datos proporcionados por la persona sean utilizados exactamente para

los fines que se autorizaron.⁴¹ Tutelándose también con esta garantía que la información que proporciona una persona no sirva para la elaboración de perfiles de la misma, para después utilizarse para su categorización o incluso como prueba en contra en algún juicio, es por esto que de manera más específica se busca tutelar “la información que pudiera surgir de la relación entre datos”.⁴²

Cabe hacer un importante señalamiento entre los conceptos de dato e información. El término dato hace referencia a cualquier conjunto de letras, números o signos que tienen al menos un significado. Los datos conforman entes reales y objetivos, lo que significa que existen independientemente de sus potenciales usuarios. La información, en cambio, puede

ser definida como todo dato que interviene, desencadena o participa en una decisión. Por lo tanto, la información personal se entiende como “toda información que se refiere a cualquier dato del sujeto que es o puede ser identificado por medio de informaciones como el nombre, la dirección, la edad, fecha de nacimiento o el número telefónico”.⁴³

3) Existe una categoría de datos especialmente protegidos, que la doctrina llama “datos sensibles”, dicho nombre obedece a que se trata de la información más delicada concerniente a la persona, su “contenido se refiere a cuestiones privadas y cuyo conocimiento puede ser generador de perjuicio o discriminación”.⁴⁴ Por tal motivo, toda publicidad respecto de información relacionada con

42. Puccinelli, Óscar, El Habeas Data..., p. 103

43. Estadella Yuste, Olga, El derecho de acceso a los ciudadanos a los archivos y registros administrativos, Madrid, Instituto Nacional de la Administración Pública, Ministerio para las Administraciones Públicas, 1989, p. 130.

44. Pierini Alicia, et al., op. cit., p. 24.

45. Idem. Dichos autores señalan como ejemplo al Presidente de una asociación de homosexuales que hace pública su condición de tal, razón por la cual deja de ser privada o “sensible” dicha opción

preferencias y comportamientos sexuales, filiación política o gremial, religión, raza, salud, entre otros aspectos, encuadra exactamente en los parámetros a proteger para evitar que la información en cuestión sea borrada y/o evitada su publicidad, “salvo que existan actividades claras de la persona que determinen que las cuestiones no son «sensibles» para ella o que la misma se encargue de exponerlo públicamente, en esta hipótesis dejaría de ser relevante la protección del ámbito de privacidad de esta información puesto que es el propio individuo quien se encarga de divulgarla”.⁴⁵

En resumen, podemos decir que con el derecho a la protección de datos se tutela lo siguiente:

- Se protege información personal del individuo registrada en bases de datos.
- Se protegen datos personales

c) ¿De quién se protege?

Es importante precisar que este derecho se formula para ser ejercido “contra cualquiera que realice las actividades de acceso, registro, tratamiento y transferencia de datos, y que por tal virtud los datos trasciendan a terceros”,⁴⁶ ya sean autoridades estatales, empresas o los propios particulares, siempre y cuando no se trate de bases de datos para uso doméstico o privado.

d) ¿Cómo se protege?

Una vez definidos los contenidos básicos del derecho a la protección de datos personales, es necesario mencionar los instrumentos que se pueden utilizar para su debida tutela,

dependiendo de los intereses de cada Estado, de tradición jurídica, en resumen, del nivel de protección que deseen brindar a sus ciudadanos. Así, este derecho puede ser tutelado o protegido a través de ciertos mecanismos, entre los que podemos mencionar:

- Normas generales o específicas, convencionales, constitucionales o legales que establezcan:

» *Reglas mínimas para el tratamiento de datos y para la habilitación de las bases y bancos de datos, específicamente limitado a sus actividades de tratamiento de datos a las necesarias para la finalidad en la que sean autorizados:*

» *Derechos de los registrados;*

*Sanciones de tipo administrativas y penales para quienes infrinjan ciertos aspectos de las normas;*⁴⁷

45. Idem. Dichos autores señalan como ejemplo al Presidente de una asociación de homosexuales que hace pública su condición de tal, razón por la cual deja de ser privada o “sensible” dicha opción en cuanto al conocimiento general, debiéndose cuidar que tal dato no se transforme en discriminador. Para cualquier otra persona, el registro de ese dato en sí mismo implica una “cuestión sensible” y privada, la cual debe ser resguardada y protegida.

46. Puccinelli, Oscar, *El Habeas Data...*, p. 103

47. Véase art. 8 de los Principios de la ONU, art. 10 del Convenio Europeo de 1981 y art. 24 de la Directiva Europea 95/46 de la CE.

- Normas sectoriales que traten aspectos muy puntuales, como el secreto estadístico, la información genética, etc.;
- Los contratos acuerdo respecto del tratamiento de determinados datos;
- Los códigos de conducta o de ética tanto de las empresas como de los particulares;
- Los convenios y tratados regionales e internacionales, donde se fijen ciertas reglas comunes de tratamiento y transmisión de datos personales entre diferentes países.



4. Configuración del derecho a la información y protección de datos personales, como derechos humanos en el Sistema Jurídico Mexicano⁴⁸

Además de la influencia de la tecnología en la sociedad de la información y su innegable vinculación con la protección de datos personales, contenidos en bases de datos; debemos considerar también el impacto que tiene la libertad de la información, más específicamente derecho de acceso a la información que tiene la sociedad y su posible conflicto con la protección de la privacidad del individuo, particularmente en lo que respecta a su información personal.

El derecho a la información en sentido amplio y como garantía fundamental comprende, de acuerdo al posicionamiento de Jorge Carpizo y Ernesto Villanueva tres aspectos básicos a saber⁴⁹:

1. *El derecho a atraerse de información.* Incluye las facultades de acceso a los archivos, registros y documentos públicos y la decisión de qué medio se lee, se escucha o se contempla.

2. *El derecho a informar.* Comprende las libertades de expresión y de imprenta y el de constitución de sociedades y empresas informativas.

3. *El derecho a ser informado.* Incluye las facultades de recibir información objetiva y oportuna, la cual debe ser completa, y con carácter universal, sin exclusión alguna.

La protección de datos personales en México se ha configurado

jurídicamente desde un inicio como contrapeso al derecho de acceso a la información. El derecho a la información lo vemos plasmado explícitamente en el sistema jurídico mexicano desde el año 1977 con texto bastante breve y poco clarificador al enunciar: “El derecho a la información será garantizado por el Estado”, producto de una iniciativa presidencial del cinco de octubre de ese año, así como del dictamen de las Comisiones Unidas de Estudios Legislativos y Primera de Puntos Constitucionales de la Cámara de Diputados. De aquí se desprende que el derecho a la información es una garantía social, correlativa a la libertad de expresión, que se instituyó con motivo de la llamada “Reforma Política” y que consiste

48. A partir del Decreto de Reforma publicado en la Gaceta Parlamentaria, año XIV número 3162-IV del miércoles 15 de diciembre de 2010, se reforma el artículo 1 de la Constitución mexicana para reconocer que en México se reconocen los derechos humanos en lugar del término garantías que se utilizaba anteriormente. El texto del citado artículo reformado queda en los siguientes términos: “En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales sobre derechos humanos 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”.

49. Cfr. Carpizo, Jorge y Villanueva Ernesto, “El derecho a la información. Propuestas de algunos elementos para su regulación en México”, en Valadés, Diego y Gutiérrez Rivas Rodrigo, Derechos Humanos. Memoria del IV Congreso Nacional de Derecho Constitucional III, México, Universidad Nacional Autónoma de México, 2001, pp. 71 – 102. Véase también Villanueva Ernesto, Temas selectos de derecho a la información, México, Universidad Nacional Autónoma de México, 2004, pp. 9 y ss.

50. Véase semanario Judicial de la Federación y su Gaceta, t. XI, abril de 2000, tesis: P.LXI/2000, p. 71.

en que el Estado permita que, a través de los diversos medios de comunicación, se manifieste de manera regular la diversidad de opiniones de los partidos políticos.⁵⁰

Posteriormente y debido a la imperiosa necesidad que se registraba en nuestro país de transparentar sobre todo el tema de cuentas públicas de los funcionarios gubernamentales, después de un proceso democrático sin precedentes, en el que la Cámara de Diputados el 6 de marzo aprueba por unanimidad (1 abstención, 425 votos en total) y la Cámara de Senadores aprueba también por unanimidad el 24 de abril (111 votos, 0 abstenciones) y lo ratifican congresos de diferentes Estados de la República;⁵¹ finalmente se modifica el texto de la reforma al artículo 6 constitucional y se publica el 20 de julio de 2007 en los siguientes términos:

Artículo 6º de la Constitución Mexicana...“Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, 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 federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. 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.⁵²

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.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

51. Tamaulipas, Coahuila, Morelos, Quintana Roo, Nayarit, Aguascalientes, Colima, Zacatecas, Chihuahua, Querétaro, Baja California Sur, Durango, Chiapas, Nuevo León, Guanajuato, San Luis Potosí, Estado de México, Puebla, Sinaloa, Sonora, Jalisco, Hidalgo, los cuales aprobaron por unanimidad (excepto Quintana Roo quien aprobó por mayoría) en un plazo bastante breve, del 28 de abril al 07 de junio de 2007.

52. El subrayado añadido es nuestro.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

Como se puede observar, gracias a esta reforma constitucional específicamente a la fracción II del mencionado artículo sexto se abren las puertas formalmente para el reconocimiento de este derecho en México, y para tratar de unificar algunas disposiciones existentes en algunas constituciones de entidades federativas en la República Mexicana como las de los Estados de Colima, Guanajuato, Tlaxcala, Morelos, Oaxaca, D.F. y Coahuila, puesto que cada uno de ellos

hasta la fecha conceptualizan este derecho en términos, con condiciones y alcances diferentes.

Constitucionalmente, México cuenta con dos artículos que se consideran pilares fundamentales de nuestro sistema, el artículo 14 y el 16 que fundamenten sobre todo las garantías de seguridad jurídica de los ciudadanos. Con el fin de dotar a la protección de datos personales de una autonomía y configuración constitucional plena, el 1 de junio de 2009 se reformó el mencionado artículo 16 para incluir en uno de sus párrafos este derecho, quedando la redacción en los términos siguientes:

“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.**⁵³

Estas disposiciones constituyen la culminación de una serie de esfuerzos legislativos y diferencias de opiniones de las diferentes fracciones parlamentarias en México, puesto que se tenían diversas perspectivas entre lo que se debería considerar como fundamento de protección. Algunos legisladores insistían que con la redacción original de este artículo era suficiente protección y otros consideraban que no entraba en el ámbito de protección, que era necesario una redacción aún más específica al texto original que estaba en los siguientes términos:

53. Párrafo segundo del artículo 16 de la Constitución de los Estados Unidos Mexicanos, subrayado añadido.

Artículo 16 Constitucional. “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”.

Sin embargo, el Congreso de la Unión determinó que las disposiciones existentes en la Ley Federal de Transparencia y Acceso a la Información respecto a la regulación de los datos personales en poder de las autoridades gubernamentales no era suficiente, y que existía el peligro de que un ámbito muy importante de protección de la información personal contenida en bases de datos en poder de las entidades privadas quedaba con un margen de discrecionalidad bastante amplio y que se prestaba para la comisión de muchas arbitrariedades que repercutirían en propiciar una inseguridad jurídica al ciudadano.

Es por ello que la protección constitucional se extendió también este año al ser los datos personales materia de regulación federal, no para cada uno de los estados.

Por lo tanto, el 30 de abril de 2009 se publica en el Diario Oficial de la Federación la reforma al artículo 73 Constitucional, al agregarse una fracción para quedar en los siguientes términos:

Artículo 73 Constitucional. El Congreso tiene la facultad para legislar:

“... XXIX-O En materia de protección de datos personales en posesión de los particulares...”.

La importancia de este tema radica en que el derecho de acceso a la información pública, como una de las vertientes del derecho a la información en sentido amplio, ha convertido a México en un referente

internacional por dos razones: primera, por su diseño institucional ya que en virtud de la LAI se crea el Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI), como un órgano “encargado de promover y difundir el ejercicio del derecho a la información, resolver sobre la negativa a las solicitudes de acceso a la información; y proteger los datos personales en poder de las dependencias y entidades”⁵⁴; y segunda, y por el contenido normativo tanto de esta ley federal como de las leyes estatales en la materia que coinciden en sus postulados básicos de normatividad.

Las bases del régimen de la información gubernamental en México, contenidas en la ley en comento son las siguientes:⁵⁵

- La información en posesión del Estado es pública.

54. Artículo 33 de la LAI del 30 de abril de 2002.

55. Debido a la importancia que la LAI tiene en México, se dedicará un apartado especial al análisis de las disposiciones más importantes en el epígrafe 4 del Capítulo IV del presente trabajo.

- La información reservada o confidencial constituye la excepción
- La entrega de información no estará condicionada a que se motive o justifique su uso, ni se requiere demostrar interés alguno, o acreditar personalidad jurídica.
- Un extenso ámbito de aplicación que comprende al conjunto de órganos federales: Poder Ejecutivo, Legislativo y Judicial, los órganos constitucionales autónomos (la Comisión Nacional de Derechos Humanos, Universidades Públicas Autónomas, Instituto Federal Electoral, Banco de México), tribunales administrativos, de manera indirecta a los partidos políticos, y en general a toda persona que reciba recursos públicos.

• Se protegen los datos personales, contenidos en las bases de datos en poder de las autoridades gubernamentales y en las dependencias que acabamos de mencionar en el apartado anterior.

La importancia de esta ley, y por consiguiente el rol que juega México en la promoción de esta materia, es que esta normativa es la única en el mundo que tiene un ámbito de aplicación tan extenso.⁵⁶

Así, “las legislaciones sobre transparencia (en realidad el principio de publicidad de actos y normas, y por tanto, inmerso en el más amplio y trascendente de seguridad jurídica) el canon hermenéutico que prima sobre cualquier dinámica que de estas normas puede desprenderse es el de *máxima publicidad de la información* (las cursivas son nuestras)”.⁵⁷

La información a pesar de que “debe considerarse como bien social y éste debe estar subordinado a un interés público”⁵⁸ no constituye un derecho absoluto, pues restaría la posibilidad de que existieran disposiciones similares o antagónicas; en opinión de Nogueira Alcalá, para los preceptos jurídicos puede haber limitaciones intrínsecas o extrínsecas, “los límites intrínsecos son aquellos que derivan de las propias particularidades de estos derechos y se encuentran generalmente contenidos en las disposiciones constitucionales que los delimitan y configuran”⁵⁹, mientras que “los límites extrínsecos o externos derivan de la coexistencia de derechos de libertad de información con otros derechos fundamentales que forman parte del mismo sistema de derechos”⁶⁰ entre ellos el derecho a la vida

56. La experiencia internacional, salvo el caso de Suecia, consiste en limitar el acceso a los diferentes documentos administrativos. En general se considera que los Poderes Legislativo y Judicial se autorregulan. Véase Fernández Ramos, Severiano, “Algunas proposiciones para una Ley de Acceso a la Información”, Boletín Mexicano de Derecho Comparado, México, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, vol., XXXV, núm. 105, 2002, pp. 891.

57. Nava Gomar, Salvador, “Información reservada”, Derecho Comparado de la Información, México, UNAM, Instituto de Investigaciones Jurídicas, Fundación Honrad Adenauer, Comisión Estatal de Acceso a la Información Pública de Sinaloa, núm. 4, enero-junio 2004, p. 92.

58. García Murillo, José Guillermo, *Derecho a la Información*. Consideraciones jurídicas para reglamentarlo en México, Guadalajara, Centro Universitario de Ciencias Sociales y Humanidades de la Universidad de Guadalajara, 2004, p. 95.

59. Nogueira Alcalá, Humberto, *El derecho a la libertad de opinión e información y sus límites*, Chile, Lexis Nexis Cono Sur, 2002, p. 123.

60. Idem.

privada y por tanto, la protección de datos personales que deben ser respetadas tanto por el Estado, como por los medios de comunicación e incluso los particulares cuando actúan de manera individual o a través de empresas o corporaciones.

La Suprema Corte de Justicia de la Nación en México ha delimitado a través de sus decisiones que el derecho a la información "no es absoluto, sino que como toda garantía se haya sujeto a limitaciones o excepciones que se sustentan fundamentalmente, en la protección de la seguridad nacional y en el respeto tanto de los intereses de la sociedad como a los derechos de los gobernados, limitaciones que, han dado origen a la figura jurídica del secreto de información".⁶¹ Así el derecho del hombre a manifestar sus ideas tiene limitaciones específicas tendientes a equilibrar

el derecho del individuo frente a terceros y la sociedad "puesto que el ejercicio de este derecho no debe menoscabar la moral, los derechos de tercero, que implique el honor, la dignidad y el derecho a la intimidad de éste, en su familia y decoro, provocar algún delito o perturbar el orden público".⁶² En este sentido, nuestro máximo tribunal reconoce que el derecho a la información específicamente tiene como limitaciones los derechos de terceros, además de que una vertiente de éste, como lo es la libertad de expresión tiene también limitaciones que tienen que ver con el honor y la intimidad personal y familiar. Con estas decisiones con el reconocimiento del derecho a la información con carácter de derecho fundamental y con la publicación de leyes específicas como la LAI, en México se va construyendo un importante camino en materia de

transparencia y acceso a la información gubernamental que debe considerar con la misma importancia las limitaciones a estos derechos, para no considerarlos como absolutos. La protección de datos personales además de ser un límite para el acceso de información constituye también un derecho del individuo que cada sistema jurídico debe tutelar.



61. Semanario Judicial de la Federación y su Gaceta, Novena Época, Pleno, XI, abril de 2000, p. 74.

62. Semanario Judicial de la Federación y su Gaceta, Novena Época, Tribunales Colegiados de Circuito, XIV, septiembre de 2001, p. 1309.

5. Acceso a la información judicial en México, aspecto fundamental de la democracia

Los retos que presenta el Poder Judicial respecto al tema de transparencia son muchos, incluso sobre la opinión pública ya que existen consideraciones de que nuestro sistema judicial funciona bajo la cultura del secreto.

En este sentido el concepto de información reservada plantea una serie de necesarias restricciones en materia judicial, como la tutela de situaciones de orden público, familiar, protección a los secretos industriales o comerciales, casos en los que de acuerdo al Código de Procedimientos Civiles del D.F. el juez puede celebrar audiencia en forma secreta. El acceso a la información también resulta limitado para las partes en el caso

del desarrollo de las audiencias, interrogatorios de testigos, y alegatos de las partes.

Así, la misma Suprema Corte de Justicia de la Nación publica en su página web un Diagnóstico de Percepción Ciudadana sobre Transparencia Judicial en el que reconoce que para la población en general resulta insuficiente la publicación a través de Internet del Semanario Judicial de la Federación y su Gaceta, así como la consulta de tesis aisladas y de la jurisprudencia.

La SCJN va más allá y formula unas Conclusiones sobre Transparencia Judicial, observa que una parte de la población percibe como inexistentes o en el mejor de los casos ineficaces, los

esfuerzos que el Poder Judicial de la Federación ha venido realizando con el objeto de dotar de transparencia a sus acciones. Reconoce que otro sector de la población ha manifestado que se deben llevar a cabo nuevas acciones para lograr plena transparencia.

Actualmente, los problemas que se suscitan al tratar de garantizar una seguridad jurídica plena, eficaz y eficiente pueden conllevar serios obstáculos para garantizar al mismo tiempo la transparencia gubernamental como en el caso del Poder Judicial y todas sus sentencias y demás resoluciones, escenario que nos puede llevar, de no conducirlo adecuadamente, a reservar información sin fundamentación adecuada, y por

supuesto de limitar enormemente el acceso a información judicial que actualmente se tiene y garantiza.

Recientemente, el Presidente de la República, propuso al Congreso de la Unión un paquete de reformas que buscan reforzar sobre todo el papel del ejército en labores de "seguridad interior" y propone que el Poder Judicial avale las decisiones del Ejecutivo, pues se buscará que atienda de forma inmediata, en un plazo que no exceda de ocho horas, las solicitudes de medidas cautelares, providencias precautorias y técnicas de investigación formuladas por la autoridad competente.

Aunque las iniciativas anteriores todavía no han sido aprobadas, debemos tener cuidado en el grado de avance que como país se ha alcanzado en esta materia, de tener sumo cuidado en el



6. Problemas actuales de la política criminal: Protección de Datos Personales como medio de prevención del delito

En la discusión académica se ha suscitado un tema de especial relevancia tendiente a combatir, y en su caso prevenir la comisión de los delitos, y la importancia que tiene la protección de los datos personales en este tema. Como punto de partida para nuestro análisis mencionaremos las cuatro tesis para explicar los problemas actuales de la política criminal, según Claus Roxin:⁶³

Primera tesis: las penas no son de ninguna manera un medio adecuado para luchar contra la criminalidad. Tomando en cuenta, según el citado autor, que en todas las sociedades existe siempre una cierta medida de delincuencia, donde una gran

parte de los delitos tiene su origen en relaciones conflictivas en estrechos núcleos sociales, en extremas situaciones caracterizadas por fuertes afectos o gran miedo, las normas pierden su fuerza de motivación.

Por ejemplo el combate a la delincuencia organizada es muy difícil ganarlo a través de la sanción individualizada del autor, ya que la organización fundamental, originaria de estos actos delictivos permanece y a menudo se sustrae de la acción persecutoria de la autoridad.

Es decir, el derecho penal está para evitar un estado de anarquía, pero se espera demasiado al decir que sólo aumentando las penas se

va a reducir sustancialmente la criminalidad.

Segunda tesis: las penas privativas de libertad son además un medio particularmente problemático en la lucha contra la criminalidad, para explicar esta afirmación Roxin basa su consideración en cuatro aspectos fundamentales: existe una pequeña posibilidad de educar hacia una vida responsable en sociedad a una persona que se encuentra privada de ella; tiene además un efecto múltiple disociador (puesto que el delincuente es sustraído de su vida familiar y laboral); se debe calcular también el efecto negativo que puede tener la pena privativa de la libertad (puesto que en el centro penitenciario convive con el

63. Véase Díaz Aranda, Enrique, Problemas Fundamentales de Política Criminal y Derecho Penal, 1ª. Reimpresión, México, Instituto de Investigaciones Jurídicas de la UNAM, 2002, pp. 88 y ss.

ambiente criminal todo el tiempo); y la última consideración es de tipo económico porque debido a la pesada carga que significa para el Estado la operatividad de estos centros penitenciarios difícilmente queda tiempo para los programas de reinserción a la sociedad.

Tercera tesis: la prevención es más efectiva que la pena.

En esta consideración queremos hacer una especial mención debido a la poca efectividad de las penas privativas de libertad, la prevención constituye un arma muy importante a través de la política social, medios policiacos, legislativos y técnicos, en donde se ponga especial atención, por ejemplo, a los niños de familias más necesitadas para evitar que cuando crezcan se involucren con la delincuencia.

Cuarta tesis: el sistema de reacción penal se debe ampliar y, sobre todo, complementarlo con

sanciones penales similares de carácter social constructivo. En México tenemos esencialmente la pena privativa de la libertad y la multa. En países como Alemania la multa constituye un 85% de las sanciones aplicadas, debiéndose incorporar por ejemplo para las personas que cometan delitos menos graves la posibilidad de conmutar las penas privativas de la libertad por trabajo a la comunidad.

Así, en nuestro país existe una obligación de proporcionar seguridad pública a través de la Federación, el Distrito Federal, los Estados y los Municipios, que coordinados establecerán un sistema nacional de seguridad pública, mediante la actuación de instituciones policiacas regidas por los principios de honradez, legalidad, eficiencia y profesionalismo. Su actuar debe estar siempre estrictamente regulado por disposiciones normativas que garanticen una relación biunívoca;

por una parte, el conocimiento del ciudadano de sus derechos y obligaciones y la posibilidad de conocer el quehacer público de sus autoridades, y por la otra, el establecimiento de obligaciones claras por parte del Estado de hacer ciertas acciones y también de respetar los derechos de la población que vive dentro de él, y a su vez que existan ciertos límites de injerencia para conocer del ciudadano sólo aquella información que necesite para su correcto funcionamiento para garantizar así lo que se conoce como Estado de Derecho.

En este contexto y como tuvimos oportunidad de analizar, en México se garantiza a nivel constitucional el derecho de acceso a la información pública gubernamental, es decir, las personas tienen el derecho en todo momento de preguntar la información que desee sobre el actuar de sus autoridades, cuántos recursos dedica al

cumplimiento de determinadas acciones, cuántas personas colaboran en una dependencia determinada, etc., por mencionar algunos ejemplos. Sin embargo hay cierta información que no se puede hacer pública, nos referimos a la información clasificada como reservada y la información confidencial.



7. Información reservada y confidencial como límite al acceso a la información

El artículo 13 de la Ley Federal de Transparencia (y sus correlativos en los demás Estados de la República, ver Artículo 21, 22 y ss. de la Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo) señalan que podrá clasificarse como información reservada aquella cuya difusión pueda:

I. Comprometer la seguridad nacional, la seguridad pública o la defensa nacional;

II. Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluye aquella información que otros estados u organismos internacionales entreguen con carácter de confidencial al Estado Mexicano;

III. Dañar la estabilidad financiera, económica o monetaria del país;

IV. Poner en riesgo la vida, la seguridad o la salud de cualquier persona, o

V. Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado.

Por su parte el artículo 14 del citado ordenamiento señala que también se considerará como información reservada:

I. La que por disposición expresa de una Ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial;

II. Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal;

III. Las averiguaciones previas;

IV. Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado;

V. Los procedimientos de responsabilidad de los servidores públicos, en tanto no se haya

dictado la resolución administrativa o la jurisdiccional definitiva, o

VI. 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.

Cuando concluya el periodo de reserva o las causas que hayan dado origen a la reserva de la información a que se refieren las fracciones III y IV de este artículo, dicha información podrá ser pública, protegiendo la información confidencial que en ella se contenga. Cabe señalar que no podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves y que esta información podrá permanecer clasificada por un periodo máximo de 12 años.

El acuerdo de clasificación de la información deberá fundamentarse señalando el artículo, inciso, fracción y/o párrafo que expresamente otorgue el carácter de información reservada y además establecer el periodo de reserva. Para clasificar una información no es suficiente con que la información se encuentre encuadrada dentro de las hipótesis normativas que señala la Ley Federal de Transparencia (o las de los Estados de la República, según sea materia federal o estatal) sino que se debe demostrar que su divulgación provoca afectación a los intereses de determinada dependencia, lo que se conoce como Prueba de Daño.



Solicitud número 0002200057907	Respuesta de la Unidad de Enlace de la Secretaría de Seguridad Pública
<p>“Solicito información a su dependencia sobre el gasto total en blindajes para vehículos, ventanas, puertas, etcétera, erogado durante el periodo 2000 a 2007. Le solicito me desglose el gasto por vehículo o ventana reforzado. Asimismo, solicito me informe cuántos vehículos blindados ha adquirido su dependencia en el mismo periodo y cuántos más está en proceso de adquirir.”</p>	<p>En respuesta a su solicitud, hacemos de su conocimiento que la Dirección General de Recursos Materiales y Servicios Generales, comunicó que la información solicitada se encuentra clasificada como reservada por un periodo de 6 años, con fundamento en el artículo 13 fracciones I y IV de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.</p> <p>Lo anterior, en virtud de que el difundir la información solicitada puede ocasionar los siguientes daños:</p> <p>El daño presente, se origina por el hecho de proporcionar información clasificada como reservada por disposición expresa de la Ley, lo que representaría un acto indebido de esta autoridad, debiéndose tomar en consideración que de difundirse la información solicitada, se coloca en un elevado riesgo a los servidores públicos usuarios de los vehículos de que se trata, haciéndolos vulnerables a un ataque en su contra.</p> <p>El daño probable, atentar contra la política de seguridad pública, al menoscabar o limitar la capacidad de las autoridades para prevenir la comisión de delitos; así como la seguridad e integridad de personas, incluyendo la de los servidores públicos que utilizan dichos vehículos, propiciar el ajuste de cuentas, ejecuciones u otras análogas, capaces de poner en riesgo la vida y la seguridad, específicamente de los servidores públicos de esta dependencia de la Administración Pública Federal.</p> <p>El daño específico, radica en una flagrante violación de preceptos legales que ameritan sanciones administrativas y penales, en virtud de estar obligados a conservar la información que por disposición expresa se encuentra clasificada como reservada, además de existir la obligación ineludible de conducirnos con secrecía y confidencialidad en materia de seguridad pública. Motivo por el cual, la reserva de la información contribuye como un factor de éxito para que los sistemas en materia de seguridad pública den los resultados para los cuales fueron creados</p>

La Prueba de Daño puede tratarse de cualquiera de las siguientes hipótesis:

a) Daño presente. Cuando se trata de una afectación inmanente y que pueda perdurar por el periodo de reserva.

b) Daño probable: la que su divulgación pudiera ocasionar una afectación al correcto funcionamiento del fin legítimo que persigue el Estado.

c) Daño específico: cuando su divulgación afecte concretamente el funcionamiento de una determinada dependencia, en el ámbito específico de su competencia.

En cambio el artículo 18 de la Ley Federal de Transparencia señala como información confidencial la entregada con ese carácter por los particulares y los datos personales que requieran consentimiento de

los individuos para su difusión, distribución o comercialización. Sin embargo, no se considerará con este carácter la que se encuentre disponible en fuentes de acceso público.

La información confidencial no tiene plazo de clasificación, ni aplica el principio de máxima publicidad.

Un caso práctico divulgado por la Secretaría de Seguridad Pública en las Jornadas de Transparencia y Seguridad Pública,⁶⁴ ejemplifica cómo se puede acreditar que una solicitud de información puede contravenir los intereses del Estado y de cierta dependencia:

Con el propósito de garantizar el acceso a la información se han suscitado casos resueltos por los tribunales que entran en conflicto con otros derechos fundamentales como la intimidad informática o el derecho al honor. Un caso

estadounidense que nos permitirá indagar el conflicto o colisión que puede surgir en algunas circunstancias concretas entre el derecho a la información y otros derechos.

*Caso The Florida Star v. B.J.F.*⁶⁵

Este caso tiene lugar en el Estado de Florida en Estados Unidos de Norteamérica, el 29 de octubre de 1983 cuando un periódico *The Florida Star* publicó el nombre de una mujer violada, infringiendo una ley de ese Estado que prohibía “imprimir, publicar, o radiodifundir el nombre de la víctima de un delito sexual”,⁶⁶ un cronista había obtenido el nombre de la víctima por la oficina de prensa del Departamento de Policía.

La mujer implicada demandó al Departamento de Policía con quien rápidamente llegó a un arreglo, y demandó también al

64. Jornadas de Transparencia y Seguridad Pública, Organizadas por el Instituto de Acceso a la Información Pública del Estado de Guanajuato, 2008, material disponible en: <http://www.iaaip-gto.org/bs/transparencia/material-de-transparencia.htm>

65. *The Florida Star v. B.J.F.*, 491 U.S. 524 (1989); 109 S.Ct. 2603.

66. 109 S.Ct. 2603 y 491 U.S. 524 (1989).

periódico que realizó la publicación, sosteniendo que: 1) la publicación le había producido daños emocionales; 2) había oído hablar de ella a compañeros de trabajo y conocidos; c) su madre había recibido varias amenazas telefónicas en las que un hombre le decía que violaría nuevamente a su hija; 4) todos estos hechos la habían llevado a tener que cambiar de casa, número telefónico y solicitar la protección judicial.

En su defensa, *The Florida Star* argumentó que había obtenido el nombre de la víctima del delito en cuestión por la propia policía, y que la violación de su regla interna de no publicar esta clase de delitos había pasado inadvertida. La decisión en primera instancia fue condenar al periódico al pago de una indemnización y multa, misma que fue ratificada en segunda instancia. La Suprema Corte de

Florida rechazó discrecionalmente el recurso presentado y consideró inconstitucional la ley de Florida, revocando por seis votos contra tres la condena que pesaba sobre el periódico.

La Corte Suprema estadounidense reconoce la tensión existente entre la libertad de expresión que protege la primera enmienda constitucional y la privacidad personal.⁶⁷ En este caso la Corte sostuvo principalmente los siguientes puntos:

- a) La imposición de una indemnización de daños sobre el recurrente viola la enmienda primera.⁶⁸
- b) El rol de la prensa no está directamente comprometido, debido a que la información proviene de un informe preparado y obtenido de la policía.
- c) La sensibilidad y el significado

de los intereses que se presentan entre la enmienda primera y la privacidad aconsejan resolverlas sobre *principios limitados, que no se apliquen más allá del contexto apropiado para el caso actual* (las cursivas son nuestras). Reconoce la Corte que existió un daño a la privacidad de la actora.

- d) Si un periódico obtiene por medios legales información verdadera acerca de un tema de relevancia pública, el Estado no puede constitucionalmente penar la publicación de esa información, excepto la necesidad de promover un interés estatal del orden más alto.
- e) La Corte Suprema admite como una consecuencia inevitable que su decisión significará, en última instancia, la violación de un derecho constitucional del que es titular la demandante.

67. Lo anterior debido al pronunciamiento que el juez Marshall –quien condujo la opinión de la Corte–, apoyado por los jueces Brennan, Stevens, Blackmun y Kennedy sostuvo que: La tensión entre el derecho a la libertad de expresión que otorga la enmienda primera, de un lado, y la protección que varios estatutos y la doctrina del common law conceden a la privacidad personal contra la publicación de informaciones verdicas, del otro, es un tema que hemos tocado varias veces en los últimos años”, 109 S.Ct. 2603, 2707. Cabe señalar que la primera enmienda constitucional estadounidense establece que “El Congreso no legislará respecto al establecimiento de una religión o la prohibición del libre ejercicio de la misma; ni pondrá coartadas a la libertad de expresión o de prensa; ni coartará el derecho a la gente a reunirse”.

68. La Corte Suprema Estadounidense señaló que “En la primera enmienda no existe algo llamado idea falsa. No importa cuán pernicioso pueda parecerse una opinión, no dependemos para su corrección de la conciencia de los jueces o los jurados sino de su confronte con otras ideas”, *Gertz v. Robert Welch Inc.* 418 U.S. 323, 240. El juez White formuló un voto disidente con el que coincidieron el Presidente Rehnquist y la juez O'Connor, en el que manifiesta que “no hay un interés público en publicar el nombre, la dirección, y el número de teléfono de personas que son víctimas de crímenes y no hay interés público en inmutar a la prensa de responsabilidad en los raros casos en los que los esfuerzos estatales para proteger la privacidad fallaron” 109 S.Ct. 2603, 2610.

Dicho posicionamiento de la Corte Suprema no fue compartido unánimemente.⁶⁹

Aunque la diferencia primordial con el caso argentino Pérez Arriaga, fue que la Corte Suprema estadounidense reconoce que existe una violación a la privacidad de la demandante, pero también reconoce que existe un interés superior, debemos recalcar que en ninguna sentencia se valoró que era innecesaria la difusión del nombre de la víctima del caso, en esta ocasión de la víctima de violación, además de las consecuencias que esto le ocasionó en su vida privada y pública. La importancia radicaba en la difusión de la noticia, pero no en la publicación de los datos personales.

Además la posición de la Corte Suprema en el caso en cuestión exonera la responsabilidad de los entes difusores de la noticia,

debido a que el gobierno fue el que emitió la información, salvo en el caso de “intereses del más alto orden”, sin embargo nunca se especifica exactamente qué abarcan. Es evidente que el derecho a la información puede colisionar con el derecho a la privacidad, más específicamente con la protección de los datos personales; sin embargo, como vimos al inicio de este apartado se han propuesto diversas soluciones: jerarquización, ponderación y máxima razonabilidad, pero debemos considerar que “la jerarquización, por su grado de abstracción y apriorismo, conduce con cierta facilidad a soluciones injustas, puesto que no tiene en cuenta las circunstancias del caso. La ponderación es una técnica más apegada a la realidad: postula la necesidad de decidir los conflictos caso por caso”,⁷⁰ aunque esta técnica no está exenta de peligros, puesto que se

corre el riesgo de que “la ponderación, termine resultando, más que una armonización, una suerte de jerarquización *ad causam*”⁷¹.

Resulta relevante señalar que la Suprema Corte de Justicia de la Nación en México, no ha tenido pronunciamientos abundantes al respecto, pero ha mencionado el criterio de la ponderación de los derechos en presencia para resolver el caso concreto, en una sentencia donde se analiza la vulneración al derecho al honor, entendiéndose por éste el bien objetivo que hace que la persona sea merecedora de confianza, así nuestro máximo tribunal enfatiza lo siguiente:

“El límite entre la libertad de expresión y de conducta ilegal del agente sólo puede establecerse mediante la *ponderación* de los hechos en presencia, para determinar si la restricción que se

69. Cianciardo, Juan, El conflictivismo en los derechos fundamentales, Pamplona, Eunsa, 2000, p. 56.

70. idem

71. Semanario Judicial de la Federación y su Gaceta, Novena Época, Tribunales Colegiados de Circuito, XVII, marzo de 2003, p. 1709.

impone al derecho a la información está o no justificada por la limitación que sufrirá el otro del derecho a la intimidad. Dada su función institucional, *cuando se produzca una colisión entre ambos derechos, el de la información goza de una posición preferente*, y las restricciones a ese derecho deben interpretarse de tal modo que su contenido esencial no resulte desnaturalizado. *Tal valor preferente no es, sin embargo, absoluto*. Si se le reconoce como garantía de la opinión pública, sólo puede legitimar intromisiones en otros derechos fundamentales que guarden congruencia con esa finalidad, o sea, que *resulten relevantes para la opinión pública*. Carecerá de protección cuando se ejercite de manera desmesurada a ese fin⁷² (las cursivas señaladas en esta tesis son nuestras).

Cuando se presentan colisiones de derechos fundamentales, estamos de acuerdo que “el acceso a la información: es un instrumento de justicia, es un derecho que sirve, sobre todo a los que no tienen privilegios, canonjías ni palancas... es una verdadera herramienta de empoderamiento y, por lo tanto, de democratización...”⁷³, además de que el interés que se está protegiendo es un interés público, de divulgar cualquier actividad que realice algún órgano de gobierno, independientemente del ámbito o nivel en que se desenvuelva. Sin embargo, esta consideración no debe ser absoluta, pues resulta indispensable la consideración de las circunstancias concretas y específicas de cada caso en lo particular, para considerar que sólo exista una intervención pública, aplicando el principio de

máxima razonabilidad, cuando ésta sea idónea, indispensable y proporcionada. En el caso en que el derecho a la información colisione con el derecho a la privacidad de los individuos (en cualquiera de sus manifestaciones: informática, de comunicaciones, de domicilio, entre otros) la afectación debe obedecer en todas las circunstancias a la protección de un verdadero interés público.

Nos queda claro también que cuando se trata del ejercicio de recursos públicos por ejemplo para la realización de programas gubernamentales, la divulgación de la información personal de los beneficiados por estos programas resulta una consecuencia inevitable. En lo que no podemos coincidir es que esta regla de publicidad se siga de manera absoluta, sin importar si se trata

72. Marván Laborde María, “Mensaje presentado en la XXVII Sesión Ordinaria de la Conferencia Nacional de Gobernadores”, Guanajuato, Gto., 6 de marzo de 2006, IFAI/Comunicado 009/06.
73. Bayley, David H. Democratizing the Police Abroad: What to do and How to do it. National Institute of Justice. NCJ, 188742, June 2001. <http://www.ncjrs.gov/pdffiles1/nij/188742.pdf>

de la divulgación personal, de una afectación a las esferas privadas e íntimas del individuo, sobre todo si ha existido como en los casos que analizamos, una afectación indiscutible, un daño a la persona en cuestión.

De lo expuesto se puede inferir que el derecho a la protección de datos personales está íntimamente relacionado con el control de las informaciones que nos afectan, toda vez que no solamente importa si un dato personal pertenece o no a la esfera privada de una persona (protegida por la intimidad como no interferencia), sino las posibilidades de relacionarlo con otros datos informáticamente y la finalidad de ese proceso. Esto significa que no es el conocimiento de determinados datos personales lo que pone en peligro la libertad de las personas, sino el uso que se haga de las informaciones resultantes de interrelacionarlos y del perfil que se obtenga.

El derecho a la protección de datos dispone de un contenido específico que confiere a la persona poder jurídico de imponer a terceros el deber de abstenerse a toda intromisión en la esfera privada de la persona, es decir, se pretende atribuir y garantizar el poder de control y disposición sobre los datos personales, con el propósito de impedir un tratamiento ilícito y lesivo para la dignidad y los derechos individuales del afectado.

En la sociedad de la información se favorece el uso creciente de la tecnología en todos los ámbitos de la vida del hombre, desde el laboral, económico, social, incluso en sus actividades cotidianas, desarrollándose nuevos instrumentos tecnológicos con una mayor capacidad de almacenamiento de la información. Este escenario ofrece al legislador nuevos

retos normativos ante la necesidad de conciliar los avances tecnológicos con los derechos y libertades de la persona. El derecho a la protección de datos personales es uno de estos retos del legislador contemporáneo.



8. Las redes sociales y la comisión del delito

Estamos viviendo un auge de las tecnologías de la comunicación, especialmente en lo que se refiere a las redes sociales virtuales. Una red social es un sistema que permite a los individuos interactuar con el grupo de personas que conocemos. La diferencia con las redes sociales virtuales (como Facebook, Twitter, Twenti, Hi5, MySpace o LinkedIn, entre otras) es que nos permite interactuar con nuestros contactos de manera independientemente del lugar o condición social, económica, política, cultural o educativa con cualquier persona que sea nuestro contacto, proveniente de cualquier parte del mundo. El tema resulta bastante complejo puesto que puede tener muy diversas consecuencias y repercusiones,

por mencionar algunas: el uso de las redes sociales en niños menores de 14 años, el uso empresarial para potencializar clientes dentro de las empresas, el uso de las redes sociales en el tiempo del trabajo, las intromisiones a la privacidad de personas que no son nuestros contactos, las consecuencias que tiene respecto a la libertad de expresión y los despidos que se han originado por expresiones de los superiores en las páginas personales de las redes sociales, el derecho a la imagen e incluso integridad en la red, las consecuencias que tendrán para los menores que usan actualmente las redes sociales en la solicitud de empleo en unos 5 ó 10 años, puesto que en los perfiles estamos incluyendo información que puede ser tomada por futuros empleadores para elaborar

perfiles informáticos y negar u otorgar plazas de trabajo no sólo con base en competencias académicas, sino conductuales basadas en nuestro comportamiento que hacemos público en las redes sociales, entre otros muchísimos temas que se pueden suscitar. Ya lo comentaba Carlos G. Gregorio "El mayor riesgo de las redes sociales es no saber cuáles son todos los riesgos".

Sólo una red social, Facebook, cuenta con más de 500 millones de usuarios en el mundo, México, según cifras publicadas por el periódico El Universal en noviembre de 2010 tiene actualmente 12.5 millones de personas inscritas en esta red creada por Mark Zuckerberg, quien sostiene que la privacidad ya no es una norma social, sino

que los internautas han pasado a otra etapa social más moderna en donde compartir los datos personales se ha convertido en una costumbre.

Aunque no pretendemos agotar un tema tan interesante y apasionadamente extenso, consideramos importante señalar que existe la posibilidad de que las redes sociales sean también medios de comisión de actividades delictivas o por lo menos se proporcione información para tal efecto. La Secretaría de Seguridad Pública en México ha detectado delitos relacionados con las redes sociales, como: amenazas, difamación, corrupción, menores desaparecidos, daños a la moral, pedofilia, pornografía infantil, tráfico de menores, grooming, acoso cibernético, discriminación, solicitudes de informaciones, trata de menores, venta de órganos, rastreo de correos,

orientación ciudadana, secuestro y fraude.

Como podemos advertir el problema resulta complejo, pero ¿qué podemos hacer para evitar ser víctimas de delitos a través de las redes sociales? ⁷⁴

1. Procurar no “subir” fotos familiares, de automóviles ostentosos o donde se vean las fachadas de las casas particulares, así como “postear” las actividades cotidianas.

Actualmente, a través de estos medios la mayoría de los usuarios informan, mediante su perfil, dónde estudian, dónde viven y trabajan, e incluso, en algunos casos se detalla paso a paso lo que el individuo realiza durante el día, es por ello que los delincuentes utilizan este tipo de herramientas para realizar acciones que conllevan a la comisión de un delito.

2. Es importante detenerse a pensar en el peligro real que representa el poner datos personales y fotografías que identifican plenamente a un individuo en un sitio de acceso para otras personas, ya que no se sabe con claridad quién o quiénes están viendo nuestra información o para qué la están utilizando.

3. Los datos pueden servir para extorsión telefónica, al ubicar a las personas a diversas horas del día, saber qué tipo de vehículo tiene, quiénes son sus amistades, qué lugares frecuenta, todo lo cual le sirve a la delincuencia para cometer ilícitos.

4. Existen casos en que los delincuentes se hacen pasar por mujeres u hombres atractivos cuyo único propósito es “chatear” con las posibles víctimas para saber su teléfono, número de integrantes de su familia o datos

74. Recomendaciones publicadas por la Secretaría de Seguridad Pública y Protección Civil del Estado de Guerrero, disponibles en la página: <http://seguridadgro.gob.mx/5615>

que puedan servir para una posible extorsión.

5. Por ningún motivo se deben dar datos personales a alguien que no conocemos en persona, principalmente los menores de edad.

A pesar de que nuestro país no cuenta con una regulación que específicamente se refiera a las redes sociales, la corresponsabilidad de la familia resulta indispensable para poder crear conciencia de la importancia que tiene la información personal, del uso en general de Internet como medio de comunicación y en especial de las redes sociales, sobre todo en las personas más jóvenes, las cuales estadísticamente se demuestra que cuentan con el mayor número de registros en estas redes. La prevención resulta la mejor arma contra las actividades delictivas, seamos conscientes de

la responsabilidad que a cada uno nos corresponde en el ámbito de nuestras respectivas competencias y utilicemos y potencialicemos el uso de la tecnología hacia nuestro beneficio.



9. Policía, Estado de Derecho y Código de Buenas Prácticas en México

En un sistema democrático es necesario que los organismos de procuración y de administración de justicia protejan la información que pudiera causar daño tanto a su institución, así como al funcionamiento del Estado; pero también, estas instituciones deben informar de su actuación a la sociedad en general. Ya que la policía también debe rendir cuentas, ya lo decía David Bayle, uno de los teóricos más importantes en la materia “la actividad policial debe estar abierta a la observación y debe ser regularmente reportada hacia el exterior. Este requerimiento aplica a la información sobre el comportamiento individual de los oficiales y a las operaciones de la institución como un todo, especialmente al respecto de que

si la policía está logrando lo que se propuso desde una perspectiva costo-beneficio”.⁷⁵

En efectos prácticos una policía no transparente debilita la confianza de la sociedad en ella, y significa una menor efectividad para el combate al crimen. En nuestro país existe un referente técnico en materia de transparencia sobre la gestión policial gracias al Instituto para la Seguridad y Democracia (INSYDE), el cual propone dentro de su Código de Buenas Prácticas en México, nueve estándares de transparencia policial:

- 1) Los mecanismos de supervisión policial,
- 2) Criterios e informes de evaluación del desempeño,

- 3) Protocolos de uso de la fuerza,
- 4) Lugares y medios de acceso para presentar quejas,
- 5) Número, características y frecuencia de las quejas,
- 6) Plan de Seguridad Pública,
- 7) Convocatorias y resultados de los concursos de selección,
- 8) Programas de capacitación permanente, y
- 9) Convocatorias de ascensos, criterios y procesos de decisión y criterios de separación del cargo.

El Código de Buenas Prácticas también establece que se deberán adoptar medidas de índole técnico y organizativo para

75. Bayley, David H. Democratizing the Police Abroad: What to do and How to do It. National Institute of Justice. NCJ, 188742, June 2001. <http://www.ncjrs.gov/pdffiles1/nij/188742.pdf>

garantizar la protección de los datos personales y de otros análogos. La acumulación de toda la información personal relativa a inteligencia debe ajustarse también a los principios de la regulación de datos personales.

El Código de Buenas Prácticas y Alternativas para el Diseño de Leyes de Transparencia y Acceso a la Información Pública es una propuesta que, producto de un ejercicio de consulta y consenso, expone en un formato propio, no las mejores prácticas en materia de acceso a la información ya señaladas anteriormente, sino también las alternativas concretas para el diseño de leyes de acceso a la información pública en México, congruente con lo establecido por el artículo 16 constitucional y los demás relativos aplicables en la materia.

Como ejemplo de razonamientos aplicados a la resolución concreta de solicitudes de información relacionadas con la materia penal, podemos señalar uno de los casos citados por la Dra. María Marván Laborde,⁷⁶ comisionada del IFAI, en donde se requiere que la Secretaría de Seguridad proporcione cierta información y el razonamiento del IFAI al respecto:

Se solicita a la Secretaría de Seguridad Pública:

Documentos del expediente único que se vinculan al ingreso-traslado-ingreso de Joaquín Guzmán Loera al penal de máxima seguridad La Palma y posteriormente al de Puente Grande y las fotografías y documentos en los que consten los informes médicos y psicológicos.

La respuesta de la Secretaría de Seguridad Pública fue:

Clasifican como reservada toda la información bajo el supuesto de causar perjuicio a las actividades de prevención o persecución de los delitos y como confidencial la información personal del interno

Resolución del IFAI modifica el criterio de la dependencia:

El IFAI modifica la respuesta de la dependencia e instruye para que se entreguen en versión pública los documentos de carácter administrativo y confirma la clasificación como confidencial de la información personal

El razonamiento del IFAI al resolver sobre el caso planteado fue el siguiente:

El expediente único de cada

76. Jornadas de Transparencia y Seguridad Pública, op. cit.

interno que ingresa a los CEFERESOS integra documentos de carácter personal pero también de carácter administrativo.

En este sentido, solamente se dio acceso a la información a algunos documentos administrativos toda vez que no hay una afectación a las actividades de persecución y prevención de delitos ni actualizan alguna otra causal de reserva de la LFTAIPG.

De los documentos personales – expediente médico y psicológico– se confirmó su clasificación como confidencial en razón de que contienen datos personales que afectarían la vida privada del interno. La foto que está tanto en Internet y otros medios de comunicación no se reservó.

En otro caso citado por la Comisionada Marván Laborde, resuelto por el Secretariado Ejecutivo del Sistema Nacional de

Seguridad Pública se solicita lo siguiente:

Los datos estadísticos correspondientes de 1994 a 2003 desglosado por entidad federativa y por delito conforme a los formatos que son utilizados por el Sistema Nacional de Seguridad Pública para actualizar la información de incidencia delictiva.

La respuesta del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública fue la siguiente:

Clasifican la información como reservada por un periodo de 12 años.

Manifiestan que la información generada por el Secretariado solamente podrá ser intercambiada entre las instancias de seguridad pública.

Resolución del IFAI:

El IFAI revoca la respuesta de la dependencia e instruye para que se entreguen los datos estadísticos solicitados.

El razonamiento que hace el IFAI se basa en las siguientes consideraciones:

La divulgación y acceso a la información estadística solicitada no pone en riesgo la seguridad pública ni atenta contra el honor de las personas.

Revela aspectos del ejercicio gubernamental útiles para que los ciudadanos puedan evaluar el desempeño de las autoridades correspondientes.

Una forma de evitar el juego político en la presentación de estadísticas puede ser la regularización de periodos de publicación de las mismas. En México, como se pudo observar, el tratamiento de protección de

datos personales, transparencia y acceso a la información supone un tema sumamente novedoso, pero también de vital importancia, ya que debido al actuar de las corporaciones policíacas y la correcta difusión, puede derivar en la confianza de la sociedad, lo que a su vez repercute en que las políticas públicas en esta materia se cumplan de manera exitosa.



10. FUENTES CONSULTADAS

FUENTES BIBLIOGRÁFICAS

Carpizo, Jorge y Villanueva Ernesto, "El derecho a la información. Propuestas de algunos elementos para su regulación en México", en Valadés, Diego y Gutiérrez Rivas Rodrigo, *Derechos Humanos. Memoria del IV Congreso Nacional de Derecho Constitucional III*, México, Universidad Nacional Autónoma de México, 2001.

Cremades García, Javier (Coord.), *Régimen jurídico de Internet*, Madrid. La ley, 2001.

Conde Ortiz, Concepción, *La protección de datos personales*, Madrid, Dhykinson, 2005.

Cianciardo, Juan, *El conflictivismo en los derechos fundamentales*, Pamplona, Eunsa, 2000.

Davara Rodríguez, Miguel Ángel, *La protección de datos personales en el sector de las telecomunicaciones*, Madrid, Fundación Airtel, 2000.

Díaz Aranda, Enrique, *Problemas Fundamentales de Política Criminal y Derecho Penal*, 1ª. Reimpresión, México, Instituto de Investigaciones Jurídicas de la UNAM, 2002.

Estadella Yuste, Olga, *El derecho de acceso a los ciudadanos a los archivos y registros administrativos*, Madrid, Instituto Nacional de la Administración Pública, Ministerio para las Administraciones Públicas, 1989.

Estadella Yuste, Olga, *La protección a la intimidad frente a la transmisión internacional de datos personales*, Madrid, Tecnos, 1995.

Ekmekdjian Miguel y Pizziolo, Calogero, *"Habeas data". El derecho a la intimidad frente a la revolución informática*, Buenos Aires, Depalma, 1996.

Fernández Ramos, Severiano, "Algunas proposiciones para una Ley de Acceso a la Información", Boletín Mexicano de Derecho Comparado, México, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, vol., XXXV, núm. 105, 2002.

Fernández Rodríguez, José Julio, *Lo público y lo privado en Internet. Intimidad y libertad de expresión en la red*, México, Universidad Nacional Autónoma de México, 2004.

Fernández Segado, Francisco, *La dogmática de los derechos humanos*, Lima, Ediciones Jurídicas, 1994.

Frosini, Vittorio, *Informática y Derecho*, Bogotá, Temis, 1988.

García Corona, Irene Gabriela, "La protección de datos personales en la Comunidad Europea desde la perspectiva alemana y española", en *Derecho de acceso a la información pública*, Ernesto Villanueva e Issa Pla (eds.), México, UNAM, 2004.

García Murillo, José Guillermo, *Derecho a la información. Consideraciones jurídicas para reglamentarlo en México*, Guadalajara, Centro Universitario de Ciencias Sociales y Humanidades de la Universidad de Guadalajara, 2004, p. 95.

Gils Carbó, Alejandra M., *Régimen Legal de las bases de datos y habeas data*, Buenos Aires, Editorial La Ley, 2001.

Gonzáini Osvaldo, Alfredo, *Habeas data. Protección de datos personales*. Buenos Aires, Ribinzal Culzoni, 2001.

Herrán Ortiz, Ana Isabel, *El derecho a la protección de datos personales en la Sociedad de la Información*, Bilbao, Universidad de Deusto, 2003.

Hondius, Fritz W., "A decade of international Protection", en *Netherlands of International Law Review*, vol. 30, núm, 2, 1983.

Jon Bing, "Code, Acces and Control, en Klang Mathias y Murria Andrew, *Human Rights in the Digital Age*, Great Britain, Galss House Press, 2005.

Klang Mathias y Murria Andrew, *Human Rights in the Digital Age*, Great Britain, Galss House Press, 2005.

Martínez Martínez, Ricard, *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas, 2004.

Marván Laborde María, "Mensaje presentado en la XXVII Sesión Ordinaria de la Conferencia Nacional de Gobernadores", Guanajuato, Gto., 6 de marzo de 2006, IFAI/Comunicado 009/06.

Nava Gomar, Salvador, "Información reservada", *Derecho Comparado de la Información*, México, UNAM, Instituto de Investigaciones Jurídicas, Fundación Honrad Adenauer, Comisión Estatal de Acceso a la Información Pública de Sinaloa, núm. 4, enero–junio 2004.

Nogueira Alcalá, Humberto, *El derecho a la libertad de opinión e información y sus límites*, Chile, Lexis Nexis Cono Sur, 2002.

Pérez Luño, Antonio Enrique, *Los derechos humanos en la sociedad tecnológica*, en Lozano Mario et al., *Libertad informática y leyes de protección de datos personales*, Madrid, CEC, 1989.

Pérez Luño, Antonio Enrique, *Manual de Informática y Derecho*, Barcelona, Ariel, 1996.

Pierini, Alicia, et. al., *Habeas Data. Derecho a la intimidad*, Buenos Aires, Editorial Universidad, 2002.

Piñar Mañas, José Luis, et. al., *Protección de Datos de Carácter Personal en Iberoamérica*, Valencia, Tirant Lo Blanch, 2005.

Puente de la Mora, Ximena, "*Habeas data* como mecanismo de protección de los datos personales en Iberoamérica", *De Iure*, Colima, Instituto Universitario de Investigaciones Jurídicas, Universidad de Colima, año 5, segunda época, núm., 3, 2005.

Ruiz Miguel, Carlos, *La configuración constitucional del derecho a la intimidad*, Madrid, Tecnos, 1995.

Tapscot, Don, *The Digital Economy: Promise and Peril in the Age of Network Intelligence*, Nueva York, McGraw-Hill, 1996.

Téllez Aguilera, Abel, *Nuevas tecnologías, intimidad y protección de datos*, Madrid, Edisofer, 2001.

Villanueva Ernesto, *Temas selectos de derecho a la información*, México, Universidad Nacional Autónoma de México, 2004.

Westin, Alan F. *Privacy and Freedom*, New York, Atheneum, 1967.

Wolfed, David A., *Globalization, Information and Communication Technologies and Local and Regional Systems of Innovation*. Toronto, Department of Political Science, University of Toronto, 2004.

Zúñiga Urbina, Francisco, "El derecho a la intimidad y sus paradigmas" *Ius et Praxis*, Chile, Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, año 3, núm. 1.

FUENTES JURISPRUDENCIALES

Semanario Judicial de la Federación y su Gaceta, t. XI, abril de 2000, tesis: P. LXI/2000.

Semanario Judicial de la Federación y su Gaceta, Novena Época, Pleno, XI, abril de 2000.

Semanario Judicial de la Federación y su Gaceta, Novena Época, Tribunales Colegiados de Circuito, XVII, marzo de 2003.

Semanario Judicial de la Federación y su Gaceta, Novena Época, Tribunales Colegiados de Circuito, XIV, septiembre de 2001.

The Florida Star v. B.J.F. 491 U.S. 524 (1989); 109 S.Ct. 2603.

Gertz v. Robert Welch Inc. 418 U.S.323,240

FUENTES ELECTRÓNICAS

Bayley, David H. Democratizing the Police Abroad: What to do and How to do It. National Institute of Justice. NCJ, 188742, June 2001. <http://www.ncjrs.gov/pdffiles1/nij/188742.pdf>

Jornadas de Transparencia y Seguridad Pública, Organizadas por el Instituto de Acceso a la Información Pública del Estado de Guanajuato, 2008, material disponible en:
<http://www.iacip-gto.org/ws/transparencia/material-de-transparencia.htm>

Secretaría de Seguridad Pública y Protección Civil del Estado de Guerrero, disponibles en la página:
<http://seguridadgro.gob.mx/5615>

Idearios de Transparencia No. 7 es una publicación del Instituto de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo, que fue terminado de imprimir en Abril de 2011 en los talleres de Grupo Editorial EstosVías S.A de C.V. con un tiraje de 3,000 Ejemplares

La revisión y corrección de estilo estuvo a cargo de la Mtra. Lili Conde mientras que el diseño editorial fue responsabilidad del Sr. Leonardo David Hernández Palma.
