

LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

JONATHAN GABRIEL GARZÓN GALVÁN*

Resumen

Este artículo tiene como objetivo presentar al lector un panorama general de la normatividad mexicana en materia de intercambio de datos personales, indispensable para que un individuo pueda interactuar en sociedad, cuyo flujo es necesario entre las personas que quieren llevar a cabo actividades conjuntas o entre quienes requieren recibir o prestar algún servicio.

Summary

This article aims to present the reader with an overview of the Mexican regulations for the exchange of personal data, essential for an individual to interact in society, whose flow is necessary among people who want to carry out joint activities or between those required to receive or provide a service.

Palabras clave

Datos personales, privacidad, vida privada, intimidad, Instituto Federal de Acceso a la Información, Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Key words

Personal data, privacy, private life, intimacy, Federal Institute of Access to Information, Federal Law of Transparency and Access to Public Govern-

* Maestro en Comercio Electrónico por el ITESM y Catedrático de la Facultad de Derecho de la Universidad La Salle (México) jgarzon@gmail.com.

ment Information, Federal Law of Protection of Personal Data in Possession by Private Parties.

1. Introducción

El tratamiento de datos personales no es una actividad que se haya comenzado recientemente, y que por tanto la regulación haya tenido que actualizarse para abarcar esta nueva actividad del ser humano. El tratamiento de los datos se ha llevado a cabo desde tiempos remotos, sin embargo, hay una nueva realidad que ha abierto las puertas a vulnerabilidades antes no conocidas.

El uso de la tecnología ha beneficiado al ser humano en muchas de las facetas en las que se desenvuelve, por su enorme capacidad de recopilación, almacenamiento, transferencia, explotación y uso de la información. Siendo este último elemento considerado como la materia prima de las actividades económicas y/o de los servicios gubernamentales.

A pesar de esto, y por la gran concentración, sistematización e instantánea disponibilidad de información concerniente a las personas, se ha dejado a las mismas a merced de un sin número de posibles situaciones que afectan sus derechos y garantías fundamentales: discriminación, molestias, persecución, presión, control social y hasta como víctima potencial de ciertos delitos, como el robo de identidad o el fraude.

Hoy en día a través de la tecnología se puede sin mucho esfuerzo y costo, y en tiempo real, comparar y contrastar datos sobre uno o varios individuos, para señalar aquellos que se desvíen y/o cumplan un perfil establecido. También es posible que a través de una recopilación continua de datos se cree un perfil de la personalidad que contenga información sobre la persona incluso desconocido por ella misma.¹ Es posible localizar a personas sin su conocimiento y/o consentimiento. Actualmente dejamos rastro de todo lo que hacemos o decimos en la red y posiblemente esa información está siendo recabada, sin que lo sepamos.

Todo lo anterior, provoca que los individuos estén en un estado de indefensión e impone una peligrosidad cuantitativa y cualitativamente distinta a la del pasado. Hasta antes de la era digital los datos eran tratados de forma manual, a través de documentos físicos (papel) y procesos mecánicos, la manipulación de la información y su transferencia eran costos y muchas veces complicados, por lo tanto la posibilidad de que se materializaran los riesgos que se han señalado era menor.

¹ Davara, Miguel Ángel, *Manual de Derecho Informático*, Thomson Aranzadi, 10ª. edición, España 2008, p. 48.

Es por tal motivo que la revolución tecnológica requirió que el marco legal contemplará la protección de las personas contra estos riesgos que nacen y crecen paralelamente al desarrollo tecnológico.²

El objetivo del presente trabajo es dar un panorama general de lo que es la protección de datos personales, comenzando por su importancia, conceptos relacionados y sistemas utilizados para su protección; para posteriormente hacer un breve recuento de los antecedentes internacionales que le fueron dando forma a esta figura legal, y como estos se tradujeron en regulación para México. En cuanto a esta última temática se prevé el análisis de antecedentes y el estatus de la regulación al respecto en México, donde encontraremos regulación separada para el ámbito público (gobierno) y el ámbito privado, donde se realizará un mayor énfasis; y concluir con temáticas diversas que se encuentran pendientes por resolver en la regulación mexicana.

No es objetivo del presente trabajo hacer un análisis detallado y/o práctico, sino presentar un panorama general de la normatividad mexicana para que los lectores puedan basar investigaciones futuras sobre la protección de datos personales; y en cuanto a las temáticas que están pendientes, se espera sirva como detonadores para su análisis y desarrollo.

Es innegable que el intercambio de datos personales es necesario para que un individuo pueda interactuar en sociedad, que son un activo intangible de las empresas y del gobierno, y que su flujo es necesario entre personas que quieren llevar a cabo actividades conjuntas o entre quienes requieren recibir o prestar algún servicio. Sin embargo, ello no quiere decir que por tal motivo las personas a quienes pertenecen estos datos deban perder el control sobre los mismos.

Antes de continuar con el presente trabajo es relevante señalar que, si bien el concepto de protección de datos personales pareciera que refiere a la idea de que se busca mantener una seguridad y defensa para salvaguardar datos de, la realidad es que el dato no requiere de protección alguna. El objetivo de este concepto es la protección de las personas, a través del establecimiento de principios y derechos que regulen un tratamiento de datos controlado por sus titulares.³

Muchos conceptos están relacionados con la protección de datos personales, tales como privacidad, intimidad y vida privada, sin que por ello

² En la Exposición de Motivos de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de Datos, ley española hoy abrogada y sustituida por otra más precisa, se podrán encontrar mayores argumentos que respaldan el nacimiento de la regulación de protección de los datos personales. Boletín Oficial Español. Número 262, de 31 de octubre de 1992.

³ Revista IDC en colaboración con Davara Abogados S.C., Edición especial, ¿Y SUS DATOS ESTÁN PROTEGIDOS?, México, enero 2012. p. 2.

sean conceptos equivalentes. Cuando hablamos de intimidad nos referimos a información o a una esfera que buscamos solamente sea conocida por un número muy pequeño de personas y que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente. Este concepto protege la parte más profunda de la personalidad o actitud de una persona, es decir sentimientos o pensamientos que se reserva el individuo para él o para sus más allegados, siendo cada uno quien define lo que es íntimo para él, en función de sus preferencias. De este derecho se desprenden otros derechos como la inviolabilidad de las comunicaciones⁴ o el derecho a la propia imagen.

En lo que respecta al concepto de privacidad es posible señalar que puede ser utilizado desde su definición original como “derecho a ser dejado solo” hasta ya más recientemente como el derecho de mantener control de la propia información y exigir que ésta permanezca en su esfera interna o privada. En contraste con el concepto de intimidad, la privacidad es un concepto más amplio.⁵ No toda la información de una persona puede ser considerada como íntima en el mismo grado.

La privacidad constituye información de la persona que, de forma aislada, puede carecer de importancia real pero que, en conjunto y enlazadas con otra, podrían arrojar un retrato de la personalidad del individuo que debe mantenerse reservado y en control de su titular. La idea del control es el punto crucial de la privacidad.⁶ La privacidad implica el derecho para decidir qué información personal se desea entregar, cuándo y a quién, conservando el control sobre la misma.

Otro concepto relacionado pero no equivalente es el de vida privada, el cual es un concepto medio entre intimidad y privacidad. Dentro de privacidad esta la información personal que debemos compartir para llevar a cabo actividades comerciales, sociales y/o con el gobierno, pero de la cual se debe mantener un control. Vida privada engloba aquello que no se quiere sea de general conocimiento y dentro de esta hay una esfera

⁴ En este aspecto la Constitución mexicana prevé en su artículo 16:

(...)

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacidad de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley. (...)

⁵ Revista IDC, Op. Cit. P. 3.

⁶ Piñar, Jose Luis. *¿Existe Privacidad?*, en *Protección de Datos Personales, Compendio de Lecturas y Legislación*, IFAI, Alonso Editores, 2010, México, p. 17.

más profunda, la intimidad, que se protege con aun más celo, porque se entiende como esencial en la configuración de la persona.⁷

Dentro de la privacidad se encuentra la vida privada y dentro de ésta se encuentra inserta la intimidad; la privacidad, es lo controlado, la vida privada es lo genéricamente reservado y la intimidad lo radicalmente vedado, lo más personal. Por lo tanto si se afecta la intimidad, se afecta la vida privada; si se afectan cualquiera de los dos anteriores se daña la privacidad de la persona; y afectando cualquiera de ellos se estaría afectando el derecho a la protección de datos personales.



Figura No. 1

El derecho a la protección de datos consiste en un poder de disposición y control sobre toda la información concerniente a la persona. La protección de datos personales es un derecho más amplio que la intimidad, la vida privada y la privacidad, abarcan cualquier dato vinculado a la persona, sea o no íntimo privado o público.

Miguel Ángel Davara (2008) define la protección de datos, como el amparo debido a los individuos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamientos, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional.⁸

⁷ La Suprema Corte de Justicia de la Nación ahonda en el tema en la resolución al amparo directo en revisión número 402/2007.

⁸ Davara, Miguel Ángel, 2008, *Op. Cit.* P. 49.

Esta protección se ve materializada en la protección a la privacidad (que abarca vida privada e intimidad) y la autodeterminación informativa.⁹ Es decir, el derecho de las personas a saber quién trata sus datos personales y para qué, y la posibilidad de ejercer ciertos derechos ante dicho tratamiento. Esta autónoma decisión por parte de los titulares de los datos debe protegerse tanto del poder del Estado, como de las funciones de entidades privadas. Debe precisarse que los titulares de los datos son sus legítimos propietarios, quienes los tratan lo hacen en concepto de posesión, no de propiedad.

Ahora bien, un dato personal es toda información que está vinculada a la persona. La regulación mexicana señala que será dato personal cualquier información concerniente a una persona física identificada o identificable.¹⁰ De lo anterior se desprenden que los datos relacionados con personas morales o jurídicas no son datos personales, excepto cuando se vinculan con una persona física, ejemplo: empleados, representantes, apoderados, etc.

Finalmente, podemos señalar que hay dos sistemas de protección que los países que han agregado a su regulación la protección de datos personales aplican: el *"Data Protection"* y el *"Habeas Data"*. El primero de ellos se refiere a que ha sido incorporado en la regulación del país un conjunto de normas, reglas, principios, procedimientos y deberes que rigen el tratamiento de datos personales en todas sus etapas (recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional).¹¹

El *"Habeas Data"* se considera como una acción legal generalmente de rango constitucional que de manera específica trata algunos aspectos de la protección de los datos personales, y tiene un enfoque más reactivo, es decir busca reparar o modificar las actividades que van en contra de la protección de datos personales, pero no previene el tratamiento ilícito de los mismos. La acción de *"Habeas Data"* puede ser definida como el derecho que asiste a toda persona a solicitar judicialmente la exhibición de los registros, en

⁹ La autodeterminación es un concepto acuñado por la doctrina alemana, que debe ser comprendido como aquella facultad que tiene una persona para decidir sobre la recolección, difusión y utilización de sus datos personales, lo cual solo es posible si se impone a terceros deberes para el tratamiento legal de datos personales. Este punto se abordará con mayor amplitud en el presente trabajo en el apartado de Antecedente Internacionales.

¹⁰ El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (RLFPDPPP) en su artículo 2, fracción VIII establece que se entenderá por persona física identificable a *"toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas"*.

¹¹ Ossio, Freddy. *Protección de Datos Personales, ¿Habeas Data o Sistema de Data Protection?*, Escuela de Juristas, Bolivia, 2010. P. 74.

los cuales están incluidos sus datos personales, para tomar conocimiento de su exactitud, requerir su rectificación, o la supresión de datos inexactos u obsoletos o que impliquen discriminación.¹²

2. Antecedentes internacionales

Como se señaló anteriormente para enfrentar estos nuevos retos que la tecnología impuso, el marco regulatorio tuvo que actualizarse para hacerles frente.¹³ Cabe mencionar que algunos conceptos como el derecho y respeto a la intimidad o a la vida privada fueron reconocidos como derechos fundamentales e incorporados en un gran número de instrumentos internacionales desde hace más de medio siglo:

1. Declaración Universal de los Derechos Humanos, 1948, art. 12.¹⁴
2. Pacto Internacional de Derechos Civiles y Políticos, 1966, art. 17.¹⁵
3. Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica), 1969, art. 11.¹⁶
4. Convención Europea de Derechos Humanos, 1950, art. 8.
5. Carta de los Derechos Fundamentales de la Unión Europea, 2000, art. 8.¹⁷

¹² *Ibidem*. PP. 78-80.

¹³ Ornelas, Lina, y Ayllon, Sergio, *La recepción del Derecho a la Protección de Datos Personales: Breve descripción de su origen y estatus legislativo en Protección de Datos Personales, Compendio de Lecturas y Legislación*, IFAI, Alonso Editores, 2010, México. p. 54.

¹⁴ Artículo 12.- *Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*

¹⁵ Artículo 17.- *Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*

Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

¹⁶ Artículo 11. *Protección de la Honra y de la Dignidad*

Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

¹⁷ Artículo 8 *Protección de datos de carácter personal*

Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Sin embargo, solo el último de estos marcos regulatorios supranacionales abarca el derecho de protección de datos personales como tal. Fue la Ley de Protección de Datos del Estado alemán de Hesse en 1970, la primera en regular específicamente la materia de protección de datos, aunque no con aplicación en todo el territorio alemán sino únicamente en el Estado de Hesse.¹⁸

La primera en su tipo con aplicación a nivel nacional fue la “*Datalag*” o Ley de Datos sueca de 1973, y la primera en el continente americano fue la “*Privacy Act*” de Estados Unidos de América (EUA), en 1974,¹⁹ sin embargo, ésta solo hacía referencia al concepto de vida privada. A estas regulaciones le siguieron documentos marco para la protección de datos personales a nivel internacional:

¹⁸ Ossio, Freddy. 2010. *Op. cit.* P. 60.

¹⁹ Tellez, Julio. *Derecho Informático*, 3ra edición, Mac Graw Hill, México, 2004. P. 63.

ANTECEDENTES INTERNACIONALES

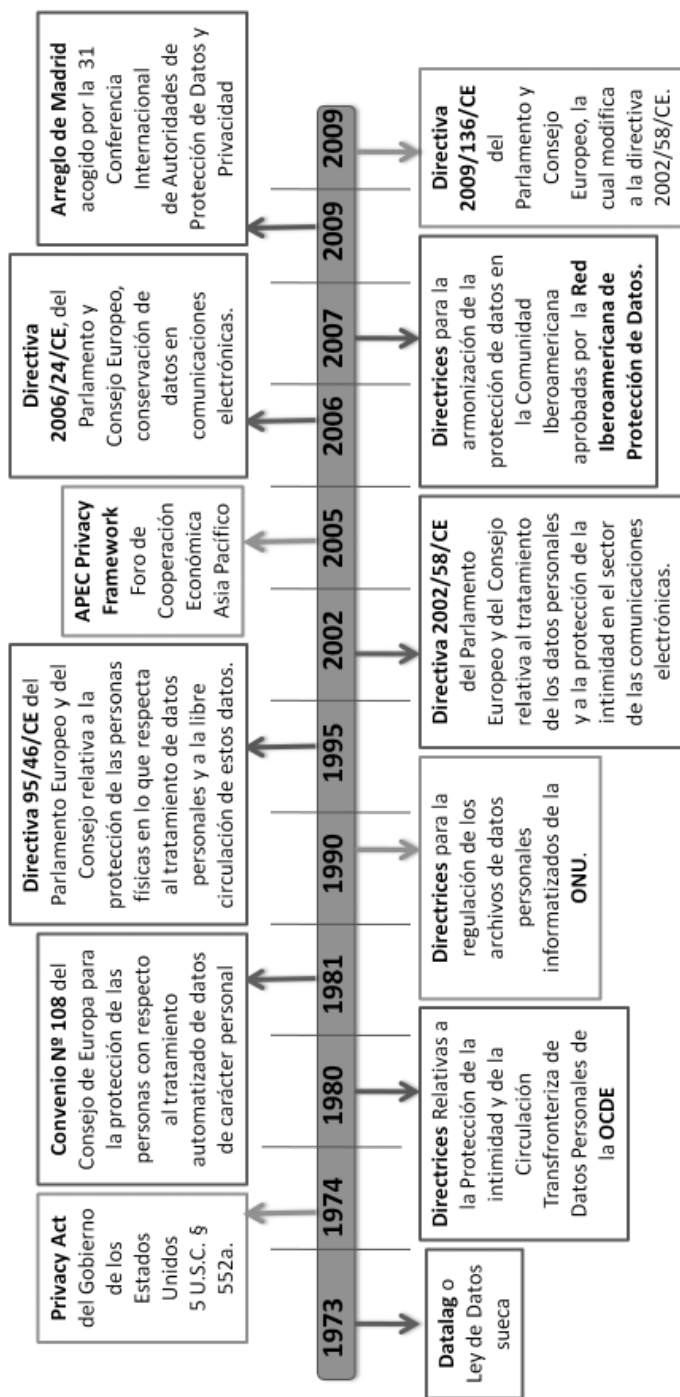


Figura No. 2

Es importante señalar que el ya comentado derecho a la autodeterminación informativa, fue asentado por primera ocasión en la sentencia de 1983 del Tribunal Constitucional Federal Alemán,²⁰ que provocó que se declararan inconstitucionales algunos artículos de la Ley del Censo Alemán.²¹

Como se puede apreciar el derecho a la protección de datos personales encontró mayor desarrollo en Europa, donde, primero, con el Convenio 108 se emitió el primer instrumento internacional de carácter vinculante, en el que se plasman los principios de la protección de los datos de carácter personal; y posteriormente con la Directiva 95/46 CE, se buscó uniformidad en la regulación en esta materia por cada país miembro de la Unión Europea, para evitar obstáculos al flujo de los datos personales entre los mismos. Cabe señalar, que esta directiva prohíbe la transferencia de datos personales a un tercer país que no tenga un adecuado sistema de protección de la privacidad. En adición a lo anterior, es en este continente donde se declara el 28 de enero de cada año como el “Día de la Protección de los Datos Personales”.²²

Por lo que respecta a América muchos de los países latinoamericanos han incorporado esta protección ya sea a través de los sistemas de “*Data Protection*” o, a través del “*Habeas Data*”. En el caso de los EUA como bien se señaló anteriormente, cuenta con la *Privacy Act*, pero su alcance está acotado a la protección de los individuos frente a la afectación de su vida privada por los sistemas electrónicos de recolección, uso y almacenamiento de datos de las agencias federales de dicho gobierno.

En cuanto al ámbito privado, EUA no cuenta legislación amplia al respecto, por lo que se basan principalmente en la autorregulación. En atención a esto y para mantener un flujo de información personal entre divisiones, clientes, proveedores filiales o socios pertenecientes a los EUA y

²⁰ Sentencia sobre el Censo de Población de 1983. Versión traducida al castellano por Manuel Daranas: “Sentencia de 15 de diciembre de 1983: Ley del Censo. Derecho de la Personalidad y Dignidad Humana”, Boletín de Jurisprudencia Constitucional, Madrid, Dirección de Estudios y Documentación del Congreso de los Diputados, vol. IV, núm. 3, enero de 1984. PP. 126-170.

²¹ Al respecto, dicho tribunal definió claramente el derecho a la autodeterminación informativa como aquella facultad del individuo de decidir básicamente por sí solo sobre la difusión y la utilización de sus datos personales, y estableció que sólo serían admisibles limitaciones al referido derecho si existiese un interés superior fundamentado por una normatividad de rango constitucional. La anterior interpretación ha sido adoptada en muchas de las regulaciones en otros países, incluyendo la mexicana.

²² Esto se llevó a cabo en 2006 cuando a través de una resolución del Comité de Ministros del Consejo de Europa con motivo del aniversario de la firma del Convenio N° 108 del Consejo de Europa para la protección de los datos personales con respecto al tratamiento autorizado de datos de carácter personal. A esta celebración se han unido distintas organizaciones y asociaciones públicas, privadas y la sociedad civil en Estados Unidos, Canadá y México a través de la organización de sesiones informativas, debates y presentaciones en distintas ciudades para crear conciencia de este derecho.

a Europa se establecieron los *International Safe Harbor Privacy Principles*, suscritos el 21 de julio de 2000 por el Departamento de Comercio de los Estados Unidos.²³ Con base a estos principios las empresas estadounidenses que voluntariamente se adhieran al programa *Safe-Harbor* contarán con la “presunción” de cumplir con un nivel adecuado de protección de datos personales exigido por la Directiva 95/46 CE, y podrán continuar o comenzar a tratar datos personales provenientes de la UE.²⁴

A grandes rasgos estos son los antecedentes y avances más relevantes en materia de datos personales, muchos de los cuales fueron sustento para el análisis, debate y generación de la regulación mexicana, catalogada como un modelo híbrido de protección de datos personales.

3. Antecedentes nacionales

En México la protección de datos personales inicialmente surgió en contraste con el derecho al acceso la información pública gubernamental. El 11 de julio de 2002, fue publicada en el Diario Oficial de la Federación (DOF) la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), la cual contemplaba el derecho a la protección de datos personales como uno de los límites al derecho de acceso a la información.²⁵ Esta misma regulación estableció como autoridad garante del derecho al acceso a la información pública gubernamental y de velar por sus limitantes a nivel federal, al Instituto Federal de Acceso a la Información (IFAI).²⁶

Al no ser una regulación a nivel nacional, la protección de datos personales en posesión de entidades de gobiernos estatales se regula por lo que los propios estados establezcan en normas locales al respecto y tienen sus propios organismos locales de transparencia y acceso a la información pública.

Retomando la regulación del sector público federal, el IFAI derivado de las atribuciones ha expedido regulación secundaria en la materia como los Lineamientos de Protección de Datos Personales (LPDP), el 30 de

²³ Téllez, Julio, 2004, *Op. Cit.* P. 63.

²⁴ Davara, Isabel. Protección de Datos de carácter personal en México; Problemática Jurídica y Estatus Normativo en *Protección de Datos Personales, Compendio de Lecturas y Legislación*, IFAI, Alonso Editores, 2010, México. P. 94

²⁵ Los límites al derecho de acceso están señalados de manera expresa, en los artículos 12, 14 y 18 de la LFTAIPG.

²⁶ Con la publicación de la LFPDPPP se amplía la esfera de acción del IFAI y se le renombra como Instituto Federal de Acceso a la Información y Protección de Datos.

septiembre de 2005, los cuales tienen por objeto establecer las políticas generales y los procedimientos que deberán observar únicamente las dependencias y entidades de la Administración Pública Federal (APF) para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales.

Posteriormente el 23 de agosto de 2006, publicó en el DOF las Recomendaciones sobre Medidas de Seguridad Aplicables a los Sistemas de Datos Personales (RMSASDP). Adicional a los anteriores, se han emitido otros lineamientos para establecer los procedimientos que deben seguir las dependencias de la APF en la atención a los derechos de acceso y corrección de datos por parte de los ciudadanos.²⁷

Finalmente y en este mismo sentido —sector público federal— el 20 de julio de 2007 fue reformado el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) para establecer como garantía constitucional el acceso a la información pública, señalando las bases para el ejercicio de dicha garantía, e incluyendo en su segunda fracción elementos respecto del ejercicio de derechos relacionados con la protección de datos.²⁸

Posterior a estos avances en el sector público, México enfrentó un intenso debate para adoptar la regulación de protección de datos personales en el ámbito privado, debido a que debió elegir entre una legislación muy proteccionista como la europea o una laxa basada en mayor medida en la autorregulación como la de EUA. Así como, por elegir si esta regulación debía ser a nivel nacional o debía dejarse como facultad de los estados el regular este derecho como sucede en el sector público.

Fue el 30 de abril del 2009 cuando se publica en el DOF la reforma al artículo 73 constitucional donde se adiciona la fracción XXIX-O, que faculta al Congreso de la Unión a legislar en materia de protección de datos personales en posesión de particulares, con lo cual se elige que la regulación en esta materia y sector sea a nivel nacional.²⁹ Complemen-

²⁷ Pueden ser consultados en el sitio Web del IFAI: <http://www.ifai.org.mx/regulacion/regulacion>

²⁸ CPEUM: Artículo 6.- (...) *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 (...)*

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.

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. (...)

²⁹ CPEUM: Artículo 73.- (...) *El Congreso tiene facultad:*

I. a XXIX-M.(...)

XXIX-N. Para legislar en materia de protección datos personales en posesión de particulares. (...)

tando lo anterior, el 1º de junio de 2010, se publica la reforma al artículo 16 constitucional estableciendo la protección de datos personales como derecho fundamental.³⁰

Para dar cumplimiento a dichas reformas el 5 de julio de 2010 fue publicada en el DOF la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual contempla un sistema híbrido entre el modelo americano y el europeo. En este mismo tenor el 21 de diciembre de 2011 fue público el Reglamento de la LFPDPP con el objetivo de reglamentar las disposiciones de la ley de la que se desprende.

4. Regulación en sector público

Como ya se mencionó la protección en este sector se desarrolla partir del derecho al acceso de la información pública gubernamental, el cual tiene como regla general que toda la información en posesión del gobierno puede ser accedida por los ciudadanos de manera gratuita y sin dilación alguna. Sin embargo, esto podría generar un alto riesgo a la privacidad de toda la población pues muchos de sus datos estaban en posesión de autoridades gubernamentales. Para evitar lo anterior, la LFTAIPG estableció que la información personal no puede estar sujeta al principio de publicidad, pues pondría en grave riesgo otros derechos fundamentales, como el de vida privada e inclusive el de intimidad.

La LFTAIPG establece dentro de sus objetivos, la protección de los datos personales en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal,³¹ y establece como sujetos obligados a:

- a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;
- b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;
- c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;

³⁰ CPEUM: Artículo 16.- (...) *Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (...)*

³¹ LFTAIPG: Artículo 4. Son objetivos de esta Ley: (...)

III. Garantizar la protección de los datos personales en posesión de los sujetos obligados; (...)

- d) Los órganos constitucionales autónomos;
- e) Los tribunales administrativos federales y,
- f) Cualquier otro órgano federal.

Sin embargo, también señala que la regulación secundaria de la LF-TAIG emitida por el IFAI solo aplica a la APF. Todos los demás sujetos obligados en el ámbito de sus respectivas competencias, establecerán cada uno de ellos mediante reglamentos o acuerdos de carácter general, los órganos, criterios y procedimientos institucionales para la clasificación y conservación de los datos personales y los procedimientos de acceso y rectificación a los mismos.

Por cuestiones de metodología y espacio, la regulación que aplica a la APF será el único objeto de análisis del presente apartado.

La LFTAIPG clasifica a los datos personales como información confidencial³² y por tanto la exceptúa de su publicidad en el ejercicio del derecho de acceso a la información pública.³³ Así mismo, esta ley reconoce los derechos de acceso y corrección de los datos y establece algunas reglas en torno a los procedimientos para hacerlos efectivos.

También hace referencia a la necesidad del consentimiento de los titulares para difundir, distribuir o comercializar sus datos personales, no así para su recolección y/o uso. Dicho consentimiento debe ser expreso y por escrito o con un medio de autenticación similar. Se encuentran exceptuados de dicho consentimiento:

- a) Los datos necesarios por razones estadísticas, científicas o de interés general, previstas en ley, previo procedimiento de disociación;
- b) Cuando los datos se transmitan entre dependencias y entidades de la APF, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
- c) Cuando exista una orden judicial y,
- d) A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales.

³² LFTAIPG: Artículo 18. Como información confidencial se considerará (...)

II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.

³³ LFTAIPG: Artículo 7.- Con excepción de la información reservada o confidencial prevista en esta Ley, los sujetos obligados deberán poner a disposición del público y actualizar, en los términos del Reglamento y los lineamientos que expida el Instituto o la instancia equivalente a que se refiere el Artículo 61, entre otra, la información siguiente (...)

Obliga de la misma forma a las dependencias y/o entidades de la APF, que en caso de mantener un sistema de datos personales,³⁴ deberán hacerlo del conocimiento del IFAI, quien mantiene un listado actualizado de los mismos. Según esta ley, su reglamento y los LPDP, los principios rectores de la protección de datos son 7, los cuales se describen a continuación:

Licitud	La obtención y uso de los datos personales solo puede realizarse con base en las atribuciones legales o reglamentarias de las dependencias y/o entidades de la APF. Así mismo hace referencia a que solo pueden tratarse los datos para finalidades determinadas y legítimas.
Calidad	Los datos deben ser exactos, adecuados pertinentes y no excesivos en atención a las atribuciones legales y reglamentarias correspondientes.
Acceso y Corrección	En este caso existe correlación entre este principio y los propios derechos de acceso y corrección, los que permiten: a los titulares de los datos, solicitar al responsable del sistema de datos personales información relativa al tratamiento de sus datos personales, así como su modificación si son incorrectos.
Información	Se debe informar de manera escrita al ciudadano, al momento de recabarle sus datos, el fundamento legal para ello, y las finalidades para las cuales serán tratados sus datos. ³⁵
Seguridad	Se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.
Custodia	Los datos personales serán debidamente custodiados y se deberá garantizar el manejo cuidadoso en su tratamiento.

³⁴ El artículo 3 de la LFTAIPG define como sistema de datos personales, al conjunto ordenado de datos personales que estén en posesión de una entidad o dependencia de la APF.

³⁵ En atención a esto los LPDP establecen como obligación el incorporar en sus mecanismos escritos de recolección de datos la siguiente leyenda (aviso de privacidad) textual:

"Los datos personales recabados serán protegidos y serán incorporados y tratados en el Sistema de datos personales (indicar nombre), con fundamento en (indicar) y cuya finalidad es (describirla), el cual fue registrado en el Listado de sistemas de datos personales ante el Instituto Federal de Acceso a la Información Pública, y podrán ser transmitidos a (indicar), con la finalidad de (indicar), además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de datos personales es (indicarlo), y la dirección donde el interesado podrá ejercer los derechos de acceso y corrección ante la misma es (indicarla). Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación (incluir fecha)."

Consentimiento para la transmisión	Toda transmisión de datos personales deberá contar con el consentimiento libre, expreso e informado del titular.
------------------------------------	--

Cabe señalar que esta normativa no hace distinción alguna entre clases de datos de carácter personal que por su especial naturaleza requieren de una mayor protección como: los sensibles y los patrimoniales. Tampoco incluye los derechos de cancelación y oposición los cuales si son contemplados en la regulación del ámbito privado.

Como complemento los LPDP establecen medidas de seguridad para la protección de los datos personales que deben cumplir las entidades y dependencias de la APF como: designar a un Responsable y a un Comité de Información que velen internamente por la protección de datos, entre otras.

Finalmente la LFTAIPG prevé como causa de responsabilidad administrativa el que los servidores públicos, entreguen y/o traten datos personales en contravención con la propia Ley.³⁶

5. Regulación en el sector privado

Como se comentó la regulación de protección de datos personales en el ámbito privado está fundamentada en los artículos 16 y 73 constitucional, de la cual se desprende la LFPDPPP. A diferencia del sector público la regulación en este ámbito es a nivel nacional, ya que dejarla en manos de los estados podría dar lugar a desigualdades de facto y mercados territoriales ilícitos de tratamiento de datos personales.

La LFPDPPP tiene como objetivo la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento³⁷ legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Establece como sujetos regulados a las personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, y exceptúa de su aplicación a: a) las sociedades de información crediticia (buros de crédito) en cuanto al tratamiento que den a los datos personales con esa

³⁶ LFPDPPP Artículo 63. *Serán causas de responsabilidad administrativa de los servidores públicos por incumplimiento de las obligaciones establecidas en esta Ley las siguientes: (...)*

V. Entregar información considerada como reservada o confidencial conforme a lo dispuesto por esta Ley; (...)

³⁷ Por tratamiento la LFPDPPP define: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio (físico y/o electrónico). El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

específica finalidad; y,^{38,39} b) las personas que lleven a cabo la recolección y almacenamiento de datos personales, es decir sin fines de divulgación o utilización comercial.

Para cumplir este objetivo la LFPDPPP distingue a las personas que intervienen en el tratamiento de datos en 4 figuras:

Titular

- ♦ La persona física o moral a quien corresponden los datos personales, y controla su tratamiento.

Responsable

- ♦ Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales. Son las empresas, asociaciones y personas en general, que recaban los datos y los utilizan para cumplir sus objetivos. Es la principal figura obligada a cumplir con los establecido por la LFPDPPP, debiendo respetar todos los principios, atendiendo el ejercicio de los derechos ARCO por el titular, e impuesto a someterse a procedimientos ante el IFAI y consecuentemente susceptible de sanción.
- ♦ En caso de utilizar a un Encargado para el tratamiento de los datos deberá velar y asegurar, que éste cumpla en su nombre la normatividad, para evitar verse sancionado.

³⁸ Es decir, que los tratamientos de datos que estas empresas realicen con finalidades distintas como: emplear personas, ofrecer y/o contratar otros servicios diferentes con personas físicas, solicitud de información a través de sitios Web, etc, si deberán apegarse a lo establecido por la LFPDPPP.

³⁹ Este tipo de sociedades tienen una regulación específica que es la Ley para Regular las Sociedades de información Crediticia y su regulación secundaria. Específicamente el artículo 28 de esta ley señala:

Artículo 28.- Las Sociedades sólo podrán proporcionar información a un Usuario, cuando éste cuente con la autorización expresa del Cliente, mediante su firma autógrafa, en donde conste de manera fehaciente que tiene pleno conocimiento de la naturaleza y alcance de la información que la Sociedad proporcionará al Usuario que así la solicite, del uso que dicho Usuario hará de tal información y del hecho de que éste podrá realizar consultas periódicas de su historial crediticio, durante el tiempo que mantenga relación jurídica con el Cliente.

Las Sociedades podrán proporcionar información a los Usuarios que adquieran o administren cartera de crédito, utilizando para ello la autorización que el Cliente haya dado conforme al presente artículo al Usuario que otorgó el crédito respectivo originalmente. (...)

Las Sociedades, sus empleados y funcionarios tendrán prohibido proporcionar información relativa a datos personales de los Clientes para comercialización de productos o servicios que pretendan ofrecer los Usuarios o cualquier tercero, salvo para la realización de consultas relativas al historial crediticio. Quien proporcione información en contravención a lo establecido en este párrafo, incurrirá en el delito de revelación de secretos a que se refiere el artículo 210 del Código Penal Federal. (...)

Encargado

- ♦ La persona física o moral que sola o conjuntamente con otras trate datos personales por cuenta del responsable. Son aquellas empresas o personas que dan servicios de outsourcing a Responsables, y solo pueden tratar los datos para aquello que le haya encomendado el Responsable.
- ♦ Esta figura trata los datos personales como consecuencia de la existencia de una relación jurídica que le vincula con el Responsable y delimita el tratamiento de los datos.
- ♦ Esta figura no tiene capacidad de decisión sobre el tratamiento de los datos personales. En caso que el encargado utilice los datos para otras finalidades, será considerado Responsable con todas las obligaciones que ello traiga consigo.

Tercero

- ♦ La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

A diferencia de la LFTAIPG, la LFPDPPP hace una diferenciación entre 3 tipos de datos: a) datos personales en general; b) datos patrimoniales; y, c) datos sensibles.⁴⁰ Estas definiciones traen importantes consecuencias para quienes los tratan. En cuanto a los segundos se establece la necesidad de solicitar el consentimiento expreso del titular para su tratamiento. En cuanto a los datos sensibles se prohíbe la creación de bases de datos de este tipo sin que se justifique la creación de las mismas para finalidades lícitas que persiga el responsable,⁴¹ se exige consentimiento expreso y por escrito y se deben realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo

⁴⁰ En este sentido la ley establece una definición abierta para el concepto de datos sensibles, siendo estos aquellos que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. La propia ley incluye los siguientes ejemplos:

1. Origen racial o étnico.
2. Estado de salud presente y futuro.
3. Información genética.
4. Creencias religiosas, filosóficas y morales.
5. Afiliación sindical.
6. Opiniones políticas.
7. Preferencia sexual.

⁴¹ LFPDPPP: Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

indispensable y el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos. Adicionalmente tratándose de este tipo de datos las sanciones administrativas y penales se duplican.

Ahora bien, la estructura general de la normativa está dividida en principios, derechos y procedimientos:



Figura No. 3

Los *principios* son declaraciones programáticas que deberán guiar el tratamiento de los datos personales en este ámbito, son los pilares en los que se basa la protección de datos personales. Es a través de los derechos que se reconoce a los individuos la potestad de exigir a quienes traten sus datos personales el cumplimiento de los principios.

Los procedimientos son la facultad pública para que una autoridad independiente, en este caso el IFAI, proteja a los individuos en caso de incumplimiento a los principios y a los derechos contenidos en la Ley.⁴²

⁴² Davara, Isabel. 2010. *Op. Cit.* p. 77.

5.1 Principios

Licitud

Señala que se deben tratar y recabar los datos de manera acorde con la legislación nacional e internacional. Es decir solo recabar y usar los datos para lo que la ley permite y no tratar datos para actividades ilícitas. Si el responsable obtiene datos de manera desleal, aunque el individuo haya manifestado su consentimiento al tratamiento, el tratamiento sería ilícito.

Consentimiento

Eje central de esta regulación que establece que todo tratamiento de datos personales requiere del consentimiento previo del titular. El consentimiento debe ser libre (sin coerción, error, mala fe, violencia o dolo), inequívoco (no permita equivocación de la existencia del mismo), específico (referido a una o varias finalidades determinadas) e informado (conocimiento a través del aviso de privacidad). La ley establece 3 tipos de consentimiento:

- a) Tácito, como regla general, el cual se da con la puesta a disposición del aviso de privacidad al titular y su no oposición al mismo.
- b) Expreso, para el tratamiento de datos patrimoniales y/o financieros.
- c) Expreso y con firma, para el tratamiento de datos sensibles.

El consentimiento debe poder revocarse en cualquier momento sin que se le atribuyan efectos retroactivos. Se exceptúa del consentimiento y de su revocación —no de los demás principios de la ley— las siguientes situaciones:

- 1. Esté previsto en una ley.
- 2. Los datos figuren en fuentes de acceso público.
- 3. Se sometan a un procedimiento previo de disociación.
- 4. Cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
- 5. Situación de emergencia.
- 6. El titular no esté en condiciones de otorgarlo (solo para casos de atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria).
- 7. Resolución de autoridad competente.

Con base a este principio es posible tratar los datos hasta en tanto el titular no ejerza sus derechos de oposición, cancelación o no revoque su consentimiento.

Información

El Responsable deberá informar, a los titulares, previo a la obtención o tratamiento de los datos, cómo se llevará a cabo el tratamiento, su procedencia, uso, finalidades y los derechos que puede ejercer, así como la identidad del Responsable. Lo anterior se lleva a cabo mediante el Aviso de Privacidad, entendido este último como: el documento físico, electrónico o en cualquier otro formato generado por el Responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales.

El Aviso de Privacidad deberá ser sencillo, claro y comprensible,⁴³ con una estructura y diseño que facilite su entendimiento, y contener al menos:

ART. LFPDPPP	REQUISITO
8	Mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales.
15	Datos personales recabados.
15 y 16	Finalidades del tratamiento de los datos personales.
16	Identidad y domicilio del responsable que recaba los datos personales.
16	Opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de sus datos personales.
16	Medios para ejercer los derechos ARCO.
16	Transferencias de datos que en su caso se efectúen.
36	Cláusula que indique si el titular acepta o no la transferencia de sus datos personales.
16	Procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad.
16	Señalamiento expreso de los datos personales sensibles que en su caso se traten, expresión de consentimiento por escrito.

⁴³ Los avisos de privacidad que solamente buscan cumplir con la LFPDPPP y que por tal motivo son largos, con contenido y vocabulario legalista, inhiben el derecho de los titulares a conocer la información sobre el tratamiento de sus datos- les es difícil dedicar el tiempo suficiente a su lectura, transfiriéndoles a los titulares una carga excesiva en la protección de su privacidad, y por tanto, no consiguen alcanzar el propio objetivo de la ley: garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Revista IDC, *Op. Cit.* p. 36.

Este principio no tiene excepciones, es decir los titulares de los datos tienen que conocer el aviso de privacidad, aun cuando no se necesite su consentimiento para tratar los datos.

Calidad

Los datos deberán ser pertinentes, correctos y actualizados. Se tendrán por correctos los proporcionados por el titular hasta que no se manifieste o se conozca lo contrario.

Finalidad

El Tratamiento debe limitarse al cumplimiento de finalidades determinadas (no genéricas), explícitas (no confusas) y legítimas (acordes con la ley). No se debe tratar los datos de forma no compatible con alguna de las finalidades para las que se hubiese recabado (informado y consentido). La finalidad o finalidades del tratamiento deberán estar previstas en el Aviso de Privacidad.

Proporcionalidad

Este principio está íntimamente vinculado al de finalidad, y refiere que, tanto los datos como el tratamiento deben ser necesarios, adecuados, relevantes y no excesivos en relación con las finalidades. Es decir, el Responsable deberá limitar al mínimo necesario los datos personales tratados, de acuerdo a las finalidades.

No se puede recabar más datos de los que se necesitan, ni de los que se deben recabar, aunque el titular consienta para ello, porque no sería lícito.

Lealtad

Se debe privilegiar la protección de los intereses del titular y la expectativa razonable de privacidad, entendida como la confianza que deposita el Titular en el Responsable, respecto de que los datos personales proporcionados no serán tratados en perjuicio del Titular. Se considerarán desleales aquellos tratamientos que den lugar a una discriminación injusta o arbitraria contra sus titulares. También refiere a que la obtención de los datos nunca será de forma fraudulenta o engañosa.

Responsabilidad

El Responsable vela y responde por el cumplimiento de los principios, adoptando medidas de seguridad para su aplicación inclusive si los trans-

fiere a un tercero. Este principio se materializa en el cumplimiento de los deberes de confidencialidad y de seguridad.

El primero de los deberes requiere que el Responsable mantenga medidas administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

El segundo de los deberes impone la obligación al Responsable y/o Terceros a su cargo, que intervienen en cualquier fase del tratamiento, a guardar confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

5.2 *Derechos*

Los principios analizados requieren del reconocimiento por parte del Estado de ciertos derechos mediante el ejercicio de los cuales las personas pudieran reclamar realmente la protección perseguida. Estos derechos son ejercidos por el Titular ante el Responsable.

Los derechos de protección de datos personales son comúnmente conocidos por la doctrina como los derechos ARCO en atención a la primera letra de cada uno de ellos: Acceso, Rectificación, Cancelación y Oposición.

Acceso

Refiere a que el titular podrá en todo momento solicitar al Responsable que le ponga a su disposición los datos que de él posea, así como, el Aviso de Privacidad, lo cual podrá hacerse por medios electrónicos, ópticos, sonoros, visuales o con la expedición de copias simples.

Rectificación

El titular podrá en todo momento solicitar al Responsable la actualización y/o corrección de sus datos, cuando estos no cumplan con el principio de calidad, es decir, que sean inexactos o incompletos. Para el ejercicio de este derecho el Titular deberá presentar la documentación pertinente que permita acreditar la rectificación.

Cancelación

Establece que cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de pri-

vacidad y/o las disposiciones legales aplicables, estos deberán ser cancelados. Este derecho puede realizarse de oficio por parte del Responsable y/o a petición del Titular.

Este derecho no implica la eliminación o supresión de los datos de forma inmediata, sino el cese en el tratamiento regular de los datos por parte del Responsable. Es decir, solo se podrán almacenar (tratar) durante el plazo de prescripción legal, para efectos de mantener la evidencia necesaria en caso de juicios o procedimientos legales.

A este almacenamiento de datos personales posterior al cumplimiento de finalidades y solo durante el tiempo de prescripción legal, la LFPDPPP lo define como Bloqueo. Pasado el tiempo de bloqueo, se procede a su supresión. De forma general se tienen las siguientes prescripciones legales dependiendo del tratamiento, sin embargo, es posible que la regulación específica de algún sector marque otras:

Comercial 10 años Arts.: 49 y 1047 Código de Comercio	Fiscal 5 años Arts.: 30 Código Fiscal de la Federación	Laboral Hasta 2 años Arts.: 516 a 119 Ley Federal del Trabajo
• Cartas, • Telegramas • Contratos • Convenios compromisos • Cualquier documento que de nacimiento a derechos y obligaciones	• Sistemas y registros contables, • Papeles de trabajo • Libros y registros sociales, • Equipos y sistemas electrónicos de registro fiscal • Comprobantes fiscales	• Contratos o Convenios • Recibos de nómina • Cumplimiento de obligaciones laborales • Acuses de recibo de políticas, herramientas.. • Expediente laboral

El titular puede solicitar ante el Responsable el ejercicio de este derecho cuando no se cumplan los principios de proporcionalidad, finalidad y calidad o quiere revocar su consentimiento, siempre que no haya excepciones para este derecho. En este sentido la LFPDPPP prevé las siguientes excepciones:

- I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
- II. Deban ser tratados por disposición legal;
- III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;

- IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;
- V. Sean necesarios para realizar una acción en función del interés público;
- VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular y,
- VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Oposición

Este derecho establece que el titular podrá en todo momento y por causa legítima oponerse al tratamiento de sus datos, por lo que, si hay oposición no podrán tratarse los datos de dicha persona. Este derecho se ejerce comúnmente cuando se entrega o conoce el Aviso de Privacidad, pero puede ser posterior a ello.

Todos los derechos ARCO tienen las siguientes características:

- a) Son sencillos, gratuitos y de ágil atención.⁴⁴
- b) Son de ejercicio personalísimo, es decir solo pueden ser ejercidos por el titular de los datos, o su representante legal.
- c) Mantienen independencia entre ellos, ninguno es requisito previo o impedimento para el ejercicio de otro.
- d) Son obligaciones del Responsable y siempre deberá darse respuesta a su solicitud. Aun en el caso de no se traten los datos del solicitante, el Responsable deberá responder en ese sentido.

En los casos en los que el Responsable no atienda el ejercicio de los derechos dentro de los plazos establecidos o cuando niegue total o parcialmente su ejercicio, la persona afectada por dicho comportamiento tiene la facultad de interponer el procedimiento de protección de datos contenido en la LFPDPP.

⁴⁴ En todos ellos se tiene un término de 20 días para dar respuesta, contados a partir de la fecha en que se recibió dicha solicitud, y si resulta procedente se tiene un nuevo término de 15 días siguientes a la notificación de la respuesta para hacer efectiva la medida que de atención al derecho correspondiente. Artículo 20 de la LFPDPPP.

5.3 Procedimientos

Los procedimientos concretan la tutela del Estado a la que los titulares pueden recurrir cuando se ven lesionados en el ejercicio de su derecho a la protección de datos personales por el incumplimiento a lo establecido en la LFPDPPP. La ley contempla 3 procedimientos que son substanciados ante el IFAI:

Protección de Datos Personales⁴⁵

Establece el mecanismo para que el Titular que haya ejercido algún derecho ARCO, y no se le haya permitido su ejercicio o estime que dicho ejercicio no fue atendido debidamente —no recibió respuesta alguna, no esté de acuerdo con la respuesta, o continúe el tratamiento contrario a lo solicitado—, solicite la protección del Estado.

Verificación⁴⁶

Este procedimiento puede iniciarse de oficio o a petición de parte, con el objetivo de comprobar el cumplimiento de la LFPDPPP y la regulación que de ella emane.

Para que proceda de oficio deberán darse alguno de los siguientes supuestos:

- I. Se incumplan las resoluciones dictadas por el propio IFAI en materia de procedimientos de protección de derechos.
- II. Se presuma de manera fundada y motivada la violación a algún precepto de la LFPDPPP o demás normatividad aplicable.

Sanción⁴⁷

Procede en caso de que el IFAI conozca de un presunto incumplimiento sancionado por la LFPDPPP, con motivo del desarrollo de cualquiera de

⁴⁵ Este procedimiento puede ser tramitado ante el IFAI a los quince días contados a partir de que el Titular haya recibido la respuesta a su solicitud de ejercicio de derechos ARCO por parte del responsable, o transcurridos 20 días sin recibir respuesta alguna por parte del Responsable. Este procedimiento tiene un plazo máximo de resolución de 50 días, el cual podrá ampliarse por una sola vez por el mismo plazo.

⁴⁶ La duración máxima de este procedimiento es de 180 días, el cual podrá ampliarse una sola vez hasta por el mismo período.

⁴⁷ Al igual que el de protección de datos este procedimiento tiene un plazo máximo para su resolución de 50 días contados a partir de que inició el procedimiento, el cual podrá ampliarse por una sola vez por el mismo plazo.

los otros dos procedimientos: protección de derechos o verificación. Las causales de infracción establecidas por la LFPDPPP son:

Infracción	Sanción (cifras aproximadas) ⁴⁸
I.- No cumplir con alguna solicitud de derecho ARCO.	Apercibimiento
II.- Negligencia o dolo en la atención de derechos ARCO.	
III.- Declaración dolosa de inexistencia de datos.	
IV.- Contravención a los principios.	
V.- Omitir aviso de privacidad o alguno de sus elementos.	
VI.- Datos inexactos o no efectuar rectificaciones.	
VII.- No cumplir apercibimiento.	
VIII.- Incumplimiento al deber de Confidencialidad.	Multa de 100 a 160,000 Salarios Mínimos Vigentes en el Distrito Federal (SMVDF) (\$6,000.00 a \$9,600,000.00)
IX.- Cambiar finalidad y no solicitar consentimiento.	
X.- Transferencia de datos sin consentimiento.	
XI.- Vulnerar la seguridad de base de datos, programas o sistemas.	
XII.- Transferencia o cesión de datos fuera de los casos.	
XIII.- Recabar y transferir datos sin consentimiento.	
XIV.- Obstrucción de actos del IFAI.	
XV.- Recabar datos de forma engañosa y fraudulenta.	
XVI.- Usar datos a pesar de solicitud del IFAI o titulares.	
XVII.- Tratamiento que afecte o impida el ejercicio derechos ARCO.	
XVIII.- Bases de datos de datos sensibles sin causa justificada.	
XIX.- Cualquier otra incumplimiento a la Ley.	No se establece sanción

⁴⁸ En caso de reincidencia el IFAI puede imponer una multa adicional que irá de 100 a 320,000 SMVDF (\$12,000.00 a \$19, 200,000.00) y tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Sin perjuicio de la substanciación de los procedimientos antes señalados, cualquier Titular podrá ejercer las acciones civiles y penales que estime pertinente.⁴⁹ Lo anterior se justifica debido a que la sanción impuesta por el IFAI se destina al erario público, pero el daño causado al particular no queda resarcido con ello.

Cabe señalar, que contra de las resoluciones que emita el IFAI para solventar los procedimientos, se puede interponer el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

5.4 Delitos

La LFPDPP establece dos delitos los cuales se transcriben continuación:

Artículo 67.- *Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.*

Artículo 68.- *Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.*

6. Pendientes

Como se puede apreciar existe regulación sustanciosa en la materia de protección de datos tanto en el ámbito público, como el privado. Sin embargo, hay todavía varios pendientes por atender que se desarrollarán conforme vaya madurando la regulación y la cultura de protección de datos personales.

Como parte de los objetivos de este trabajo se analizarán brevemente aquellos que por su particularidad consideramos que debieran ser atendidos en un mediano plazo por las autoridades nacionales: *regulación sectorial, esquemas de autorregulación y la obtención por parte de la Unión Europea del reconocimiento de la regulación mexicana como “adecuada”*.

⁴⁹ LFPDPPP: Artículo 58.- Los titulares que consideren que han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento a lo dispuesto en la presente Ley por el responsable o el encargado, podrán ejercer los derechos que estimen pertinentes para efectos de la indemnización que proceda, en términos de las disposiciones legales correspondientes.

Artículo 66.- Las sanciones que se señalan en este Capítulo se impondrán sin perjuicio de la responsabilidad civil o penal que resulte.

6.1 Regulación sectorial

Existen sectores que por su propia naturaleza requieren que se desarrollen, en las normativas correspondientes, las garantías en el tratamiento de los datos personales adecuadas de acuerdo con las características de cada sector. Es posible que existan avances en ciertas normativas en atención a lo que se acaba de señalar, pero deberán en lo futuro ser actualizadas para asegurar el cumplimiento y respeto de los principios y derechos recogidos en la LTASIPG y la LFPDPPP y sus regulaciones secundarias.

Sector Bancario

El flujo y tratamiento de datos personales en este sector es vital, tanto entre particulares e instituciones de crédito, como entre estas últimas para las transacciones interbancarias, y hacia algunas autoridades de este ramo para cumplir obligaciones de verificación. La Ley de Instituciones de Crédito (LIC) contempla en su articulado al secreto bancario,⁵⁰ entendido éste como aquel deber jurídico que tienen los bancos, sus directores, personal, empleados y personas que tienen relación directa con ellos, de mantener con carácter de confidencial la información sobre cualquier tipo de operación que se celebre con sus cuentahabientes, y en el entendido que las operaciones activas o pasivas son información con la cual se identifica o puede identificar a una persona, estas son datos personales, por lo tanto son conceptos interrelacionados.

El secreto bancario nace de la necesidad de proteger esta información frente a otros particulares e inclusive frente al Estado. Cabe señalar

⁵⁰ LIC: Artículo 117.- *La información y documentación relativa a las operaciones y servicios a que se refiere el artículo 46 de la presente Ley, tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios que en este artículo se establece, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios, (...), sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio.*

Como excepción a lo dispuesto por el párrafo anterior, las instituciones de crédito estarán obligadas a dar las noticias o información a que se refiere dicho párrafo, cuando lo solicite la autoridad judicial en virtud de providencia dictada en juicio en el que el titular o, en su caso, el fideicomitente, fideicomisario, fiduciario, comitente, comisionista, mandante o mandatario sea parte o acusado. Para los efectos del presente párrafo, la autoridad judicial podrá formular su solicitud directamente a la institución de crédito, o a través de la Comisión Nacional Bancaria y de Valores.

(...)

Las solicitudes a que se refiere el tercer párrafo de este artículo deberán formularse con la debida fundamentación y motivación, por conducto de la Comisión Nacional Bancaria y de Valores. (...)

Los empleados y funcionarios de las instituciones de crédito serán responsables, en los términos de las disposiciones aplicables, por violación del secreto que se establece y las instituciones estarán obligadas en caso de revelación indebida del secreto, a reparar los daños y perjuicios que se causen. (...)

que este secreto tiene excepciones en caso de requerimientos de algunas autoridades judiciales y/o administrativas.

La protección al secreto bancario establece que los empleados y funcionarios de las instituciones de crédito serán y las instituciones estarán obligadas en caso de revelación indebida del secreto, a reparar los daños y perjuicios que se causen. Por su parte la Circular Única de Bancos de la CNBV, regulación que se desprende de la LIC, establece la definición de “Información Sensible del Usuario”,⁵¹ y obliga a las instituciones bancarias a implementar medidas para asegurar la transmisión de este tipo de información en forma segura y/o cifrada.

Como se puede apreciar esta regulación reconoce el secreto bancario y el concepto de información sensible de los usuarios, pero no hace mayor énfasis en complementar la protección de datos derivado de las circunstancias especiales en las que se encuentran sus integrantes como: la necesidades de conocer el perfil socioeconómico de sus actuales y potenciales clientes, intercambiar información personal de los clientes entre las propias instituciones de crédito para la prevención de fraudes o lavado de dinero,⁵² así como la posible creación de bases de datos donde se encuentren personas que presumiblemente hayan intentado abrir cuentas para cometer ilícitos en dicho sector.

Sector Salud

Como se ha señalado en el sector privado los datos de salud están catalogados como datos sensibles, y por tanto requieren una protección reforzada dado que pueden llegar a afectar la esfera más íntima de las personas.

En este tenor la ley que regula de forma general este sector es la Ley General de Salud (LGS), la cual no especifica una protección a los datos personales de los pacientes, e incluso se tiene una problemática mayor ya que las instituciones que podrían compartir esta información son parte tanto del sector público, como del privado.⁵³ Aunado a ello, y relacionado

⁵¹ Información personal del Usuario que contenga nombres, domicilios, teléfonos o direcciones de correo electrónico, en conjunto con números de tarjetas bancarias, números de cuenta, límites de crédito, saldos, Identificadores de Usuarios o información de Autenticación

⁵² La LIC establece en su artículo 52 que las instituciones de crédito podrán intercambiar información con el fin de fortalecer las medidas para prevenir y detectar actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de los delitos en contra de su clientela o de la propia institución. Haciendo la especificación que este intercambio de información implicará trasgresión alguna a lo establecido en el artículo 117 de esta Ley.

⁵³ El Sistema Nacional de Salud está constituido por las dependencias y entidades de la Administración Pública, tanto federal como local, y las personas físicas o morales de los sectores social y privado, que presten servicios de salud, así como por los mecanismos de coordinación de acciones, y tiene por objeto dar cumplimiento al derecho a la protección de la salud. Artículo 5º LGS.

al ejercicio de los derechos de rectificación y cancelación se han planteado conflictos teóricos,⁵⁴ dado que la información dentro de un expediente clínico no debiera modificarse y/o borrarse sino siempre adicionarse información, aunque existan diagnósticos que arrojen resultados diferentes.

Como principal garantía, esta regulación debiera contemplar que no debe tener acceso a los datos de salud ninguna persona que no fuere médico o institución médica para la única finalidad de prestar atención hospitalaria o servicios clínicos en cualquiera de sus modalidades. Si por alguna razón algunos resultados o datos de salud específicos, son necesarios para alguna finalidad diferente a la anterior y debieran ser conocidos por un tercero (empleadores, empresas de seguros, escuelas, gimnasios), las instituciones y/o los profesionales médicos con el consentimiento expreso del Titular pondrá a disposición de dicho tercero los resultados concretos y específicos (positivo o negativo), siempre y cuando el tercero haga del conocimiento del Titular la finalidad justificada para tratarlos.

Lo anterior, cobra mayor relevancia cuando se llegue a adoptar el expediente clínico electrónico en México, a través del cual las instituciones del salud podrán compartir a nivel nacional la información clínica de una persona en tiempo real, agregando información en cada consulta, análisis y/o operación. Para ello, será necesario establecer las medidas de seguridad técnica a que debieran sujetarse los sistemas de información utilizadas para este fin. En este sentido México cuenta con las siguientes normas oficiales que aún no están implementadas al cien por ciento: la Norma Oficial Mexicana NOM-168-SSA1-1998 y la Norma Oficial Mexicana NOM-024-SSA3-2010.

Partidos Políticos

De acuerdo al artículo 41 de la CPEUM los partidos políticos son entidades de interés público y tiene como fin el promover la participación ciudadana, contribuir a la integración de la representación nacional y como organizaciones de ciudadanos, hacer posible el acceso de éstos al ejercicio del poder público. De lo anterior se puede apreciar que no forman parte ni del sector público ni del sector privado, son entes *sui generis* que requieren de regulación particular que le establecen sus facultades y limitantes.

Por su parte el Código Federal de Instituciones y Procedimientos Electorales (COFIPE),⁵⁵ señala que los partidos políticos están autorizados a difundir al electorado en general propaganda de campaña con el propósito de dar a conocer sus propuestas. Lo anterior quiere decir que los

⁵⁴ Rubí Navarrete, Jesús. Protección de datos Clínicos, en Protección de Datos Personales, Compendio de Lecturas y Legislación, IFAI, Alonso Editores, 2010, México, p. 200.

⁵⁵ Artículos 212 y 218 del COFIPE

partidos políticos están autorizados para obtener información del padrón electoral y hacerles llegar sus propuestas a los ciudadanos. Sin embargo, en muchos casos la excesiva y directa difusión de su información o recolección de las preferencias electorales llega a invadir la privacidad de los mismos ciudadanos, generando una evidente molestia y afectando su derecho a la privacidad.

Dado que, ni la LFTAIPG ni la LFPDPPP le son aplicables a los partidos políticos en materia de protección de datos personales actualmente no hay garantías suficientes para afirmar que existe una debida protección de los datos en posesión de los partidos políticos, y tampoco el IFAI cuenta con facultades para ejercer acción alguna en caso de una violación a dicho derecho.

6.2 Esquemas de autorregulación vinculante

Como posible apoyo a la regulación sectorial existen los esquemas de autorregulación, esquemas que son muy relevantes en la actualidad, tanto que el sistema americano de protección de datos se encuentra sustentada en ellos. La autorregulación se configura como una solución complementaria especialmente adecuada al esquema legislativo, y como un modo de hacer y dirigir los negocios, con respecto a la regulación de la materia.⁵⁶

La autorregulación debe ser entendida como el conjunto de normas que se aplican a una pluralidad de responsables del tratamiento que pertenezcan a la misma actividad profesional o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión.⁵⁷ Estos esquemas tienen las siguientes ventajas:

- A) Son un elemento de mayor confianza en la relación Titular-Responsable, ante la insuficiencia de las regulaciones existentes en los diversos sectores, añadiendo garantías necesarias adicionales.
- B) Permiten adaptar la normativa a las características especiales que presenta el tratamiento de datos en un determinado sector o actividad, facilitando su cumplimiento.
- C) Están enfocados a ser preventivos, evitando el tratamiento inadecuado de datos.

⁵⁶ Davara, Isabel. 2010, Op. Cit. P. 95.

⁵⁷ Grupo de Trabajo del Artículo 29. Documento de trabajo DG XV D/5057/97: Evaluación de la autorregulación industrial: ¿En qué casos realiza una contribución significativa al nivel de protección de datos de un país tercero? Adoptado el 14 de enero de 1998.

- D) Ofrecen soluciones rápidas a los titulares, para atender sus derechos ARCO y/o resolver controversias derivadas del tratamiento de sus datos, sin tener que acudir a la autoridad estatal.

La LFPDPPP permite el desarrollo de esquemas de autorregulación vinculante,⁵⁸ y a la fecha de elaboración del presente trabajo están pendientes de emisión los criterios al respecto por parte del IFAI. Sin embargo, el reglamento de la ley antes señalada establece que dichos esquemas deberán:

- ❖ Contener mecanismos para medir su eficacia, consecuencias y medidas correctivas.
- ❖ Traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos.
- ❖ Facilitar el ejercicio de los derechos de los titulares.
- ❖ Ser notificados de manera simultánea a las autoridades sectoriales correspondientes y al IFAI.

Estos esquemas permitirán identificar a aquellas empresas que se han adherido a un código ética o deontológico, sello de confianza a través del cual se ha verificado el cumplimiento de la normativa, siendo un factor que el IFAI debe tomar en cuenta para determinar la atenuación de sanciones, en caso de verificarse algún incumplimiento.

Estos esquemas son vinculantes (es decir obligatorios y en caso de incumplimiento sancionados) para quienes se adhieran a los mismos, no obstante, la adhesión es de carácter voluntario.

Por la falta de normativa secundaria y específica al respecto, no existen esquemas de autorregulación autorizados en México, por lo que será uno de los principales retos en los próximos años, no solo el establecimiento de ellos, sino su madurez e implementación, dado que si llegan a establecerse, y no se cumplen las reglas en ellos contenidos, se puede caer fácilmente en una mera declaración de principios o intenciones que no justifique en realidad la existencia del código vinculante.⁵⁹

⁵⁸ LFPDPPP: Artículo 44.- Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley. Dichos esquemas deberán contener mecanismos para medir su eficacia en la protección de los datos, consecuencias y medidas correctivas eficaces en caso de incumplimiento.

Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares. Dichos esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto.

⁵⁹ Davara, Isabel. 2010, Op. Cit. P. 97.

6.3 Protección adecuada

Como ya se había señalado los artículos 25 y 26 de la Directiva 95/46CE, establecen un régimen específico para los flujos transfronterizos de datos personales hacia países distintos de los estados miembros de la Unión Europea, en los cuales se exige, que el país al que se destinen los datos ofrezca un nivel adecuado de protección. Este reconocimiento se obtiene a través de la Comisión Europea y el análisis para ello comprende dos elementos básicos: el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz.

El concepto de protección adecuada debe ser entendido como la calidad de una regulación de un país que cuenta con un “núcleo” de principios de “contenido” de protección de datos y de requisitos “de procedimiento/de aplicación”, cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección.⁶⁰ Este contenido mínimo es el siguiente:

Requerido por la Unión Europea	Incluido en la LFPDPPP	Incluido en la LFTAIPG
Principio de limitación de objetivos	Principio de Finalidad	Principio de Licitud
Principio de proporcionalidad y de calidad de los datos	Principios de proporcionalidad y calidad	Principio de calidad
Principio de transparencia	Principio de Información	Principio de Información
Principio de seguridad	Principio de Responsabilidad y deber de seguridad	Principio de seguridad y custodia
Derechos de acceso, rectificación y oposición	Derechos de acceso, rectificación, cancelación y oposición.	Principio de Acceso y Corrección
Restricciones respecto a transferencias sucesivas a otros terceros países	Obligación de informar y consentir la transferencia ³	Principio de consentimiento para la transmisión

Adicionales a los anteriores también deberá contemplarse en la normativa a evaluar que: a) haga referencia a las categorías de datos sensibles asignándole protecciones adicionales; b) para el caso de que el objeti-

⁶⁰ Comisión Europea, Dirección General XV, DG XV D/5025/98, WP 12, Grupo de Trabajo del artículo 29, Documento de Trabajo, Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE. Aprobado el 24 de julio de 1998.

vo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho; y, c) cuando el objetivo de la transferencia sea la adopción de una decisión automatizada el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona. Estos puntos son adoptados por la regulación mexicana en el ámbito privado (LFPDPPP y su reglamento), pero no son del todo claros en el ámbito público (LFTAIPG).

Lo anterior, sumado a la evaluación de su aplicación eficaz serán los retos que México tiene pendiente para que la protección de datos personales sea un factor diferenciador y de competitividad del mercado económico del país, atrayendo con ello inversión y negocios de los países europeos.

7. Conclusiones

Como se pudo apreciar a lo largo de esta investigación México cuenta con una regulación acorde con su contexto, que paralelamente protege la autodeterminación informativa y la privacidad de las personas; y busca no ser un obstáculo al libre flujo de datos, tan necesario para el desarrollo de la economía nacional e internacional y para el avance hacia una Sociedad de la información.

Actualmente en México, muchas de las empresas creen haber cumplido con la LFPDPPP dado que cuentan con un aviso de privacidad, han designado a una persona o departamento de datos personales y en el mejor de los casos tienen procesos documentados para atender los derechos ARCO, sin embargo, es importante señalar que lo anterior no garantiza que el tratamiento de datos personales que llevan a cabo sea el correcto y/o este conforme a la ley, estos son solo algunos de los elementos para ello.

Se requiere de un análisis más profundo: conocer que datos personales se manejan en toda la organización (clientes, proveedores, personal, candidatos a empleados, usuarios del sitio Web, etc.), quienes tienen permisos para accederlos, como se protegen contra mal uso, destrucción o modificación, entre otros elementos que fortalecen la protección de los datos y que permiten cumplir cabalmente con la regulación.

Así mismo, para que el derecho a la protección de datos se vuelva una realidad es necesaria la formación de una cultura de protección de datos en la que participe el gobierno, la industria y los propios individuos como titulares del derecho. El primero estableciendo una regulación efi-

caz, clara y flexible, que no genere cargas innecesarias a la industria, así como mantener una autoridad y/o tribunales ante quienes se pueda subsanciar acciones legales en caso de incumplimiento.

Por parte de la industria, cumplir la regulación no solo en busca de evitar sanciones, sino como una mejor práctica y/o ventaja competitiva que será reconocida por sus usuarios. Y finalmente los propios usuarios tomando conciencia sobre el uso y el destino que le dan a su información personal, los riesgos a que están expuestos por revelarlos sin cuidado; debiendo siempre exigir sus derechos ante quienes manejan sus datos y asistir ante las autoridades correspondientes para hacer valer los procedimientos necesarios en caso de algún menoscabo del derecho a la protección de datos personales.

Todo lo anterior, requerirá de trabajos conjuntos de autoridad, industria y sociedad civil, lo cual será el mayor reto. Es por ello que este trabajo concluye exhortando a sus lectores a que en conjunto hagamos en México y en el mundo de la protección de datos personales un derecho efectivo y con un alto grado de cumplimiento y respeto, tanto en el sector público como privado, trabajando siempre en beneficio del ser humano.

Bibliografía

ARAUJO, Ernesto. *Derecho a la Información y la Protección de Datos Personales*, Porrúa, México, 2009.

ARENAS, Mónica. *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, 2005.

BIBANA, Luz Clara. *Manual de Derecho Informático*, Editorial Jurídica Nova Tesis, Argentina, 2001.

CARBONELL, M. *La reforma constitucional en materia de acceso a la información: una aproximación general*, en *Hacia una democracia de contenidos: La reforma constitucional en materia de transparencia*, Instituto de Investigaciones Jurídicas, UNAM, México, 2007.

CORRPIO GIL-DELGADO, María de los Reyes. *Regulación jurídica de los tratamientos personales realizados por el sector privado en Internet*. Agencia de Protección de Datos, Madrid, 2000.

DAVARA, Isabel. *Breve análisis de la reforma al artículo 6° constitucional en lo relativo a protección de datos personales*, en *Hacia una democracia de contenidos: La reforma constitucional en materia de transparencia*, Instituto de Investigaciones Jurídicas, UNAM, diciembre México 2007.

—, Protección de Datos de carácter personal en México; Problemática Jurídica y Estatus Normativo en *Protección de Datos Personales, Compendio de Lecturas y Legislación*, IFAI, Alonso Editores, 2010, México.

Davara, Miguel Angel. *Manual de Derecho Informático*, Thomson Aranzadi, 10ma edición, España 2008.

—, *Guía Práctica de Protección de Datos para abogados*, Editorial DaFe-Ma, Madrid, 2004.

—, *La protección de datos en Europa. Principios, derechos y procedimiento*. Grupo Asnef Equifax, Madrid, 1998.

FERNÁNDEZ, María Luisa. *Nuevas tecnologías, Internet y Derechos Fundamentales*. Mc Graw Hill Interamericana de España, Madrid, 1998.

GALINDO, Fernando. *Derecho e informática*. La Ley-Actualidad, Madrid, 1998.

RZÓN VALDÉS, E. “Lo íntimo, lo privado y lo público”, en cuadernos de transparencia, N° 6, Instituto Federal de Acceso a la Información Pública (IFAI), México, 2005.

KUSCHEWSKY, Monica. Editor General, *Data Protection & Privacy – Jurisdictional Comparisons*, European, Lawyer Reference, Thompson Reuters, 1ra Edición, Reino Unido, 2012.

MURILLO, Pablo Lucas y PIÑAR, José Luis. *El derecho a la autodeterminación informativa*, Madrid, Fundación Coloquio Jurídico Europeo, 2009.

NAVA, Alberto. *Ley Federal de Protección de Datos personales en posesión de los Particulares con Comentarios*, Porrúa, México, 2012.

LÓPEZ, Sergio. *Derecho de la Información*, McGraw-Hill/Interamericana Editores, México, 1997.

LUCAS, Pablo. *Derecho a la autodeterminación informativa*. Editorial Tecnos, Madrid, 1990.

OECD, *Thirty Years After the OECD Privacy Guidelines*, 2011.

ORNELAS, Lina, y Ayllon, Sergio. *La recepción del Derecho a la Protección de Datos Personales: Breve descripción de su origen y estatus legislativo* en *Protección de Datos Personales, Compendio de Lecturas y Legislación*, IFAI, Alonso Editores, 2010, México.

OSSIO, Freddy. *Protección de Datos Personales, ¿Habeas Data o Sistema de Data Protection?*, Escuela de Juristas, Bolivia, 2010.

PÉREZ, Antonio Enrique. *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de N.T. de la información*. FUNDESCO, Madrid, 1987.

PIÑAR, Jose Luis. *¿Existe Privacidad?*, en *Protección de Datos Personales, Compendio de Lecturas y Legislación*, IFAI, Alonso Editores, 2010, México.

ROBLEDO, Alonso y Ornelas, Lina. *Protección de datos personales en México: el caso del Poder ejecutivo Federal*, UNAM, México, 2006.

RUBÍ NAVARRETE, Jesús. *Protección de datos Clínicos*, en *Protección de Datos Personales, Compendio de Lecturas y Legislación*, IFAI, Alonso Editores, 2010, México.

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

SANCHO, Diana. *Transferencia Internacional de Datos*, Arellano, España, 2003

SUÑÉ, Emilio. *Tratado de Derecho Informático*. Volumen 1, Universidad Complutense de Madrid, Madrid, 2000.

TENORIO, Guillermo. *Los Datos Personales en México Perspectivas y Retos* Porrua/Universidad Panamericana, Mexico, 2012.

TELLEZ, Julio. *Derecho Informático*, 3ra edición, Mac Graw Hill, Mexico, 2004.

VELAZQUEZ, Rafael. *Protección Jurídica de datos personales automatizados*. Editorial COLEX, Madrid, 1993.