UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE POSGRADO EN DERECHO

MAESTRÍA EN DERECHO

LOS DESAFÍOS DEL SISTEMA JURÍDICO MEXICANO EN LA PROTECCIÓN DE DATOS PERSONALES

TESIS QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN DERECHO

PRESENTA:
ANAMELI DÁVALOS VÁZQUEZ

TUTOR:
DR. JOSÉ MANUEL VARGAS MENCHACA
ENTIDAD FACULTAD DE DERECHO

MÉXICO, D.F., MARZO 2013

A mis padres, por su gran amor, paciencia y confianza, que forjaron en mí la fuerza y tenacidad necesarias para continuar y concluir con esta importante etapa de mi vida.

A mis hermanos, a quienes amo profundamente y considero parte de este proyecto de vida, por su comprensión y entrega incondicional, pese a las adversidades y la distancia.

A mi abuelito Cande, por ser mi inspiración diaria en la búsqueda de mi superación espiritual, personal y profesional.

A todos y cada uno de mis maestros del Posgrado, especialmente al doctor José Manuel Vargas Menchaca, por ser mi guía y compartir su invaluable tiempo, dedicación y conocimientos que me permitieron culminar con esta meta profesional.

A mis familiares y amigos que estuvieron en todo momento presentes con palabras de aliento para seguir adelante, y por brindarme su confianza y apoyo incondicional.

ÍNDICE

GLOSARIO

APEC	Foro de Cooperación Económica Asia-Pacífico.
ARCO	Acrónimo conformado por las palabras acceso, rectificación, cancelación y oposición.
Autodeterminación informativa	Bien jurídico a proteger en el derecho a la protección de datos personales. Es el derecho que tiene el Titular para controlar la entrega, uso y destino de sus datos personales.
Aviso de privacidad	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 (artículo 3 fracción I de la LFPDPPP).
Base de datos	Conjunto ordenado de datos personales referentes a una persona identificada o identificable (artículo 3 fracción II de la LFPDPPP).
Comités	Los Comités de Información de cada una de las dependencias y entidades (artículo 3 fracción I de la LFTAIPG).
CFPC	Código Federal de Procedimientos Civiles.
CJF	Consejo de la Judicatura Federal.
Datos personales	Cualquier información concerniente a una persona física identificada o identificable (artículo 3 fracción V de la LFPDPPP).
Dependencias y entidades	Las señaladas en la Ley Orgánica de la Administración Pública Federal, incluidas la Presidencia de la República, los órganos administrativos desconcentrados, así como la Procuraduría General de la República (artículo 3 fracción IV de la LFTAIPG).
Derechos ARCO	Son los derechos de acceso, rectificación, cancelación y oposición (artículo 2 fracción II del RLFPDPPP).
DOF	Diario Oficial de la Federación.

Encargado	Persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del Responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio (artículos 3 fracción IX de la LFPDPPP y 49 de su Reglamento).
Ente público	Órgano de gobierno de cualquier nivel federal o local.
Ente privado	Persona física o moral de naturaleza privada.
Habeas data	Garantía constitucional, procedimiento jurisdiccional o recurso para salvaguardar el derecho a la autodeterminación informativa.
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos.
LFPA	Ley Federal de Procedimiento Administrativo.
LFPCA	Ley Federal de Procedimiento Contencioso Administrativo.
LFPDPPP	Ley Federal de Protección de Datos en Posesión de los Particulares.
LFTAIPG	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
Lineamientos	Lineamientos de Protección de Datos Personales, emitidos por el IFAI, publicados en el DOF el 30 de septiembre de 2005.
LOTFJFA	Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa.
OCDE	Organización para la Cooperación y Desarrollo Económicos.
OEA	Organización de los Estados Americanos.
OIT	Organización Internacional del Trabajo.
OMC	Organización Mundial del Comercio.
ONU	Organización de las Naciones Unidas.

Parámetros	Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares
Persona física identificable	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 requieren plazos o actividades desproporcionadas (artículo 2 fracción VIII del RLFPDPPP).
Principios rectores de la protección de datos personales	Licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad (artículo 9 del RLFPDPPP).
Responsable	Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales (artículo 3 fracción XIV de la LFPDPPP).
Respuesta	Atención que el Responsable otorga por medio escrito, electrónico o cualquier otro formato, a la solicitud de ejercicio de derechos ARCO que le presenta el Titular.
RLFPDPPP	Reglamento de la Ley Federal de Protección de Datos en Posesión de los Particulares.
RLFTAIPG	Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
SCJN	Suprema Corte de Justicia de la Nación.
Sistema de datos personales	Conjunto ordenado de datos personales que están en posesión de un sujeto obligado (artículo 3 fracción XIII de la LFTAIPG).
SMGVDF	Salario Mínimo General Vigente en el Distrito Federal.
Solicitud de ejercicio de derechos ARCO	Solicitud que el Titular presenta ante el Responsable, en los términos señalados en su aviso de privacidad, a fin de ejercer alguno de los derechos ARCO.
Solicitud de protección de derechos	Solicitud que el Titular presenta ante el IFAI para la protección de sus datos personales, derivado de la inconformidad con la respuesta emitida por el Responsable o por la falta de respuesta.

Sujeto obligado	Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República; Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; los órganos constitucionales autónomos; los tribunales administrativos federales; y cualquier otro órgano federal (artículo 3 fracción XIV de la LFTAIPG).
Tercero	Persona física o moral, nacional o extranjera, distinta del titular o del Responsable de los datos (artículo 3 fracción XVI de la LFPDPPP).
TFJFA	Tribunal Federal de Justicia Fiscal y Administrativa.
TIC’s	Tecnologías de la Información y Comunicación.
Titular	Persona física a quien corresponden los datos personales (artículo 3 fracción XVII de la LFPDPPP).
Tratamiento	Obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales (artículo 3 fracción XVIII de la LFPDPPP).
Transferencia	Toda comunicación de datos realizada a persona distinta del Responsable o Encargado del tratamiento (artículo 3 fracción XIX de la LFPDPPP).
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

INTRODUCCIÓN

A través del desarrollo del presente trabajo de investigación se pretende llevar a cabo el análisis del marco jurídico tanto nacional como internacional, en materia de protección de datos personales aplicable en el sistema jurídico mexicano, a fin de acreditar como la diversidad e inconsistencia de la normatividad aplicable puede afectar el ejercicio y protección efectiva de este derecho, así como ocasionar la dificultad institucional para su operación.

Al efecto, se parte de una hipótesis explicativa o de causa efecto, al afirmar que en el sistema jurídico mexicano, la protección de datos personales no se garantiza de manera adecuada como lo prevé la Constitución Política de los Estados Unidos Mexicanos y los tratados internacionales suscritos y aprobados por México, al encontrarse su marco jurídico aplicable disperso e inconsistente.

De esta manera, el objeto de estudio del presente trabajo es la protección de datos personales en el sistema jurídico mexicano y los desafíos que enfrenta a partir de su reconocimiento, de manera expresa, en el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, precepto constitucional reformado por Decreto publicado en el Diario Oficial de la Federación el 1 de junio de 2009, para garantizar el derecho de toda persona a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición (derechos mejor conocidos por el acrónimo ARCO), con lo cual se establecen las bases para garantizar, dentro del sistema jurídico mexicano, su observancia en los términos y con las excepciones que la ley establezca.

La inclusión del derecho fundamental a la protección de datos personales en la Carta Magna, representó un enorme avance en la materia, pues hasta antes de la citada reforma, este derecho se encontraba regulado de manera heterogénea y limitada, dentro de ordenamientos jurídicos secundarios relativos al derecho de acceso a la información, tanto federales como locales, de aplicación exclusiva a entes públicos responsables del tratamiento de datos personales en el ejercicio de sus atribuciones, así como en diversas disposiciones regulatorias de otras materias como son la de salud, financiera, telecomunicaciones, de protección al consumidor, entre otras.

Con la reforma al artículo 16 constitucional se pretende garantizar de manera homogénea e integral, el derecho que tiene todo individuo a controlar de manera informada, el uso y divulgación de sus datos personales, conocido como el derecho a la autodeterminación informativa, mediante el establecimiento de instituciones y ordenamientos jurídicos adecuados que salvaguarden el ejercicio efectivo de los derechos ARCO de los titulares frente a cualquier ente, sea público o

privado, que realice el tratamiento de los mismos. Sin embargo, al hacer un análisis del marco jurídico secundario aplicable en la materia de protección de datos personales en el sistema jurídico mexicano, se observa el cumplimiento parcial de dicho objetivo, especialmente ocasionado por la presencia de los siguientes factores:

a) Existe una segmentación en la legislación reguladora del derecho a la protección de datos personales, de acuerdo con la naturaleza jurídica, privada o pública, federal o local, de los sujetos que obtienen, usan, divulgan o almacenan los datos personales. Encontrándose por un lado, las legislaciones federal y locales en materia de transparencia y acceso a la información y, por el otro, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, independientemente de los ordenamientos jurídicos dispersos en otras materias especializadas.
b) La diversidad de disposiciones relacionadas con esta materia, provoca una pluralidad de procedimientos, criterios e instituciones encargadas de su aplicación.
c) Debido a la estrecha relación que existe entre este derecho y diversas materias como lo son la económica, tecnológica, de salud, financiera, entre otras, requiere no sólo de un conocimiento más especializado sino también de su constante actualización, lo cual repercute en la necesaria revisión y adecuación integral del marco jurídico aplicable.
d) Al ser el derecho a la protección de datos personales de reciente reconocimiento constitucional en México, existe aún una escasa cultura en la sociedad mexicana en la protección de datos personales, lo cual se ve reflejado en un inadecuado ejercicio informado y responsable del derecho, así como en la observancia de la ley.
e) El entendimiento y aplicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, como disposiciones más recientes y completas en la materia, pueden resultar complejas para los sujetos involucrados en el tratamiento de datos personales, especialmente por lo que se refiere a los términos técnicos y especializados en la materia, la presencia de lagunas y las limitaciones en las atribuciones de la autoridad garante de este derecho para la aplicación del procedimiento administrativo previsto en la ley.

Ante dicho escenario, cuestionamos si el marco jurídico vigente garantiza adecuadamente la protección de datos personales como derecho fundamental reconocido en la Constitución Política de los Estados Unidos Mexicanos y en los instrumentos internacionales suscritos y aprobados por México, o será necesario, como resultado de la evolución de este derecho, llevar a cabo su adecuación integral para hacerla acorde con el contexto nacional e internacional actual.

Para la comprobación de la hipótesis planteada se aplicarán los métodos:

- Analítico, puesto que se separará en partes la normatividad nacional e internacional en materia de protección de datos personales para realizar un estudio sobre los conceptos jurídicos, principios y directrices aplicables en el funcionamiento e interacción de este derecho.
- Sintético, en razón que a partir del análisis realizado se concatenarán los conceptos fundamentales, principios y directrices que componen el marco jurídico nacional e internacional en materia de protección de datos personales, para verificar si existe compatibilidad y coherencia entre los mismos.
- Comparativo, a través del cual se llevará a cabo un análisis de las diversas formas en que es denominado o relacionado este derecho de la protección de datos personales en otros países, a fin de establecer sus efectos y alcances.
- Histórico, para realizar un estudio de los antecedentes del derecho a la protección de datos personales en los derechos de la personalidad, entre los cuales se encuentran el derecho a la intimidad, vida privada y privacidad; así como para analizar su surgimiento y evolución.
- Jurídico, a fin de analizar los conceptos jurídicos, antecedentes, marco legislativo, fenomenología jurídica y derecho comparado del derecho a la protección de datos personales en México.

El trabajo consta de cuatro capítulos, en el Capítulo Primero realizamos un estudio del derecho a la protección de datos en el contexto nacional e internacional, en donde señalaremos los primeros acontecimientos históricos que fueron definiendo su origen y conformación, especialmente a partir de los derechos de la personalidad de la intimidad y vida privada, y en su acepción moderna como el derecho a ser dejado solo o *right to be alone*, mencionado por primera vez en el siglo XIX. De lo anterior, se desprenden principalmente cinco factores que motivaron el surgimiento y desarrollo de este derecho, entre los cuales destacan, el reconocimiento de la libertad individual de toda persona y la aparición de nuevas tecnologías.

Asimismo, en el Capítulo Primero destacamos dentro de la definición de derecho a la protección de datos personales, lo complejo que puede resultar este término debido a las diversas acepciones utilizadas, las cuales no obstante ello, pueden coincidir en determinar como el bien jurídico a proteger, el derecho de los titulares a la autodeterminación informativa y no de meros datos aislados o los medios físicos o electrónicos donde constan. También abordaremos los principales modelos regulatorios en protección de datos personales, y sus ventajas o desventajas para su operación, así como ubicar el modelo aplicable en México. Finalmente, estudiaremos el contexto internacional, regional y nacional existente en

la materia, a través de los instrumentos jurídicos aplicables, y su impacto en la sociedad, especialmente en cuanto al uso de tecnologías y el desarrollo de la economía.

En el Capítulo Segundo se analizará la evolución que ha tenido este derecho en nuestro sistema jurídico mexicano hasta su reconocimiento como derecho fundamental en el párrafo segundo del artículo 16 constitucional y en los tratados internacionales en los que México es parte, a efecto de determinar los principios y directrices que lo rigen para garantizar su adecuada protección y ejercicio.

Asimismo y en cuanto a la legislación secundaria se analizará de manera detallada, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en lo relativo a la protección de datos personales, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como cada una de las leyes que existen en la materia a nivel estatal, a efecto de establecer si se encuentran acordes o no con los principios, directrices y medidas de protección en la materia, para alcanzar la armonización entre las mismas. Lo anterior permitirá observar las ventajas o desventajas, así como los alcances que tiene para el derecho a la protección de datos personales, su regulación como parte del derecho de acceso a la información, o si es posible su regulación única y de manera independiente, por tratarse de derechos totalmente diferentes, regidos bajo principios igualmente diversos.

Por lo que se refiere al Capítulo Tercero, llevamos a cabo un análisis exhaustivo del procedimiento de protección de datos personales a nivel federal, contemplados en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como sus correspondientes Reglamentos. En este capítulo explicamos el motivo para brindar una especial atención al procedimiento administrativo contemplado en la ley, en razón de ser el principal medio con el que cuenta el titular para defender su derecho ante la inadecuada o falta de atención del Responsable, en el ejercicio de sus derechos de acceso, rectificación, cancelación u oposición. A partir de este estudio se evidenciarán las lagunas e inconsistencias en la ley, a fin de plantear posteriormente, posibles propuestas de modificación o eliminación.

Finalmente y como consecuencia del estudio previo, en el Capítulo Cuarto, definimos la comprobación de la hipótesis planteada, a fin de llegar a la exposición de posibles alternativas de solución de la problemática observada, entre las cuales proponemos reformas constitucionales para la creación de un órgano autónomo especializado y la emisión de una ley general en la materia, todo lo cual permitirá

contar con los instrumentos legales e institucionales adecuados para lograr una protección completa y efectiva del derecho fundamental a la protección de datos personales.

De esta manera, con el presente trabajo de investigación se pretende resaltar el gran desafío que representa para el Derecho, el reciente reconocimiento constitucional del derecho a la protección de datos personales, a fin de alcanzar su consolidación en el sistema jurídico mexicano, a través de una legislación que contemple medios e instancias adecuadas para garantizar efectivamente su tutela y ejercicio responsable por parte de los titulares, así como favorecer en todo momento, como lo contempla el segundo párrafo del artículo 1o. constitucional, la protección más amplia de este derecho, sin dejar a un lado su constante revisión y actualización, a fin de hacerlo acorde con la realidad social y el marco jurídico nacional e internacional vigente en la materia.

CAPÍTULO PRIMERO
EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO NACIONAL E INTERNACIONAL

I. Antecedentes del derecho a la protección de datos personales.

Los acontecimientos históricos que determinaron el surgimiento del derecho a la protección de datos personales, pueden ser analizados a partir de diferentes enfoques, de tal manera que podemos encontrar antecedentes de este derecho en:

1. La evolución de los derechos a la intimidad y a la vida privada, como origen del derecho a la protección de datos personales;
2. La evolución de los derechos fundamentales,
3. [1] desde el reconocimiento en instrumentos internacionales de las libertades individuales y la dignidad humana, hasta el reconocimiento de nuevos derechos como consecuencia de las transformaciones sociales y culturales, en donde se ubica este derecho;
4. Por su estrecha relación con la tecnología, en los orígenes de las computadoras y el internet, como principales sistemas de información y comunicación que prevalecen en la sociedad actual y su influencia en la misma respecto de los datos personales;
5. Desde el punto de vista económico, en los primeros trabajos realizados en foros internacionales, para analizar los efectos de este derecho en detrimento del libre flujo de datos y las relaciones comerciales.

A fin de comprender mejor el surgimiento y desarrollo del derecho a la protección de datos personales, en este apartado del Capítulo Primero expondremos aquellos primeros acontecimientos históricos que consideramos, influyeron directamente, en su conformación y reconocimiento como derecho fundamental a

[1] De acuerdo con Luigi Ferrajoli en su obra *Derechos y garantías. La ley del más débil*, alude a los derechos fundamentales como: "todos aquellos derechos subjetivos que corresponden universalmente a "todos" los seres humanos en cuanto dotados del *status* de personas, de ciudadanos o personas con capacidad de obrar". A partir de estos elementos, el autor distingue cuatro clases de derechos: 1) derechos humanos, derechos primarios que conciernen indistintamente a todos los seres humanos; 2) derechos públicos, derechos primarios reconocidos sólo a los ciudadanos; 3) derechos civiles, derechos secundarios adscritos a todas las personas humanas capaces de obrar; y 4) derechos civiles, derechos secundarios reservados únicamente a los ciudadanos con capacidades de obrar. De esta forma, y al acoger esta definición, el derecho a la protección de datos personales, es un derecho fundamental, clasificado como derecho humano; sin embargo, en el presente trabajo se hará referencia al mismo, en su acepción general, es decir como derecho fundamental, por ser un derecho subjetivo y universal.

través de diversos instrumentos internacionales, así como para su establecimiento en las primeras legislaciones sobre la materia, expedidas principalmente, en países europeos.

Al respecto, resulta de interés para nuestro objetivo, el antecedente de los registros públicos, considerados como las primeras bases de datos personales, cuando en una forma rudimentaria pero bien organizada, se empezaron a utilizar datos personales para propósitos meramente registrales, pero también con alcances probatorios, en este sentido Carlos G. Gregorio señala: "La generalización del registro de datos personales tuvo un impulso significativo a partir del Concilio de Trento (1563), que dictó normas regularizando el modo de llevar los libros parroquiales de bautismos y matrimonios. Luego la práctica impuso las defunciones, y con el tiempo, estos asientos fueron utilizados y admitidos como prueba en los contenciosos civiles".[2]

Posteriormente, refiere el citado autor, que las autoridades civiles crearon los registros civiles (España en 1749, Francia en 1793 y Alemania en 1874), así como los de propiedad. En cuanto a la forma como se llevaban los registros, explica que en libros registraban los datos cronológicamente, y utilizaban el sistema de generación de índices, consistente en organizar los libros mediante índices alfabéticos por apellidos, aunque sus herramientas de búsqueda eran muy rudimentarias. Agrega que su valor era fundamentalmente local, y su uso se limitaba al establecimiento de parentesco, propiedad u otra relación jurídica.

Si bien el uso de los datos era limitado y las técnicas de búsqueda rudimentarias, debido a sus características, los primeros registros se conformaron como verdaderas bases de datos, es decir, como el conjunto ordenado y organizado de datos correspondientes a personas físicas identificadas o identificables. Y en cuanto a sus alcances, no se limitaban a proporcionar sólo datos registrales, sino también a través de ellos era posible vincular o acreditar ciertos derechos para sus titulares.

En este sentido, Carlos G. Gregorio destaca el impacto, tanto positivo como negativo, que pueden tener los registros sobre los derechos, al mencionar: "Los sistemas de registro suelen crearse para proteger algún derecho específico,

---

[2] GREGORIO, Carlos G., "Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina", *Transparentar al Estado: la experiencia mexicana de acceso a la información*, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, número 193, México, 2004, primera reimpresión 2005, ISBN 970-32-1836-9, formato pdf, disponible en http://biblio.juridicas.unam.mx/libros/3/1407/12.pdf, p. 299, consultada el 6 de abril de 2012.

pero también pueden convertirse en obstáculo para otros derechos … Existe una fuerte relación entre registros y derechos".[3]

Para ejemplificar lo anterior, cita el caso del ministro de Hacienda de Brasil, Rui Barbosa, quien en 1890, época de la abolición de la esclavitud, ordenó requisar y quemar todos los papeles, libros y documentos relacionados con los esclavos, a fin de evitar que sus ex-propietarios demandaran al Estado una indemnización.

De esta manera, los registros se convirtieron en un medio idóneo para acreditar derechos ante terceros y ante el propio Estado, pero también en una forma, para quien los administra, de mantener cierto control respecto de los dueños de los datos, o para realizar fines distintos a los que tenían al momento de ser recabados.

Otro caso similar son los censos de población, los cuales a partir de la obtención de cierta información personal disociada, permiten determinar ciertos datos como son el número de habitantes en una población, para fines primordialmente estadísticos, aunque sus usos pueden ser diversos como para evaluar impactos demográficos, implementar políticas de gobierno, detectar fenómenos sociales frecuentes, establecer muestras, entre otros.

En este caso pareciera que no hay relación con el derecho objeto de nuestro estudio, porque si bien a través de los censos se pueden obtener datos personales, no es posible vincularlos con personas físicas identificadas o identificables, cuando sus resultados se reflejan sólo en números y estadísticas. Sin embargo, existieron acontecimientos en la historia que revelan cómo estos datos fueron utilizados para fines diversos a los del censo, para ocasionar incluso, la vulneración de derechos.

Un ejemplo claro sucedió en la Segunda Guerra Mundial cuando los nazis hicieron uso de información contenida en el censo poblacional de 1939 de Alemania, a través de la cual obtuvieron y utilizaron datos personales para la identificación de judíos, que posteriormente serían sujetos de uno de los más terribles holocaustos sufridos en la humanidad.

En dicho censo se registraron datos como la edad, sexo, lugar de residencia, profesión, religión, estado civil de las personas y, por primera vez, se registró la raza de la persona según el origen de sus abuelos. La información del censo fue ingresada en tarjetas codificadas para ser procesada en la máquina

[3] *Ibidem,* p. 300.

Hollerith, inventada en 1884 por Herman Hollerith, considerada como la primera versión de la computadora moderna que ordenaba y contaba tarjetas.[4]

La información del censo de 1939, fue utilizada por el alemán nazi Adolf Eichmann para crear un registro nacional de personas de ascendencia judía, la cual al cabo de tres años de ser completada, sirvió para proporcionar a los nazis la base para elaborar las listas de deportación de judíos y judíos "mischlinge" (judíos de razas mixtas).[5]

Con ello, el binomio de información y tecnología empezó a emerger como un elemento de poder y control para quien lo poseía. Con el surgimiento de las primeras computadoras se facilitó el manejo y administración de la información, pero su acceso y uso era limitado, especialmente para bancos y gobiernos de los Estados más desarrollados, quienes contaban con los recursos necesarios para implementar este tipo de tecnología y posteriormente otras más complejas, como fue más adelante la conformación del Internet.

En relación con los orígenes del Internet, Clara Luz Álvarez alude al proyecto creado en 1958 denominado DARPA, descrito como: "… un centro de investigación y desarrollo del Departamento de Defensa de Estados Unidos de América. Su misión es mantener la superioridad tecnológica del ejército de EUA mediante el patrocinio de investigaciones de vanguardia".[6]

La referida autora agrega que en 1960 con el DARPA se propuso iniciar una investigación para crear una red robusta que permitiera la comunicación durante tiempos de guerra y proyectara conectividad aun cuando la red hubiere sido destruida. Derivado de dicha investigación surge ARPANET, el cual fue utilizado entre redes de universidades y centros de investigación, mediante el intercambio de información y acceso remoto. Del desarrollo del proyecto se obtuvieron grandes

---

4 Información obtenida de la página *United States Holocaust Memorial Museum*, Washington, D.C., disponible en http://www.ushmm.org/outreach/es/article.php?ModuleId=10007703, consultada el 7 de abril de 2012.

5 Información obtenida de la obra denominada *Registrarse, entrar, darse de baja. Proteger tu privacidad y controlar tus datos. Un recurso para el profesorado*, publicado por la Oficina del Comisionado para la Protección de Datos de Irlanda, 2007, redacción, edición adaptada y publicación de la Agencia Española de Protección de Datos y de las Comunidades Autónomas de Madrid, Cataluña y Euskadi, ISBN 978-0-9557 187-0-0, formato pdf, disponible en http://www.avpd.euskadi.net/s04-5273/es/contenidos/informacion/documentos_difusion/es_difusion/adjuntos/guia-educativa.pdf, p. 32, consultada el 7 de abril de 2012.

6 ÁLVAREZ, Clara Luz, *Internet y derechos fundamentales,* Porrúa y Universidad Panamericana, México, 2011, p. 4.

resultados, entre ellos, la posterior conformación de una de las más grandes herramientas de la actualidad, el Internet.

Ante esta situación de vanguardia, las administraciones públicas que manejaban una gran cantidad de datos personales de aquellos individuos a los cuales proporcionaban algún tipo de servicio público, empezaron a hacer uso de la tecnología para facilitar la tarea de recolección y almacenamiento de datos personales para la integración de grandes bases de datos que permitieran incluso ser compartidas.

De acuerdo con Ximena Puente de la Mora: "El primer claro ejemplo de procesamiento de información que se produjo en la Administración Pública fue en 1972, cuando el sistema de gobierno noruego decidió implementar un sistema, donde el ciudadano estaba facultado para solicitar un beneficio social para reducir los costos de compra de vivienda. El solicitante solo debería de 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".[7]

Así, cuando la comunicación de información empezó aumentar a través de medios electrónicos, según Aristeo García González, surgió un proceso de socialización de los archivos, el cual se implementó con el Internet y finalmente se concretó con las aplicaciones basadas en la *World Wide Web*, que junto con la presencia de micoordenadores y terminales telemáticas accesibles, tanto para las administraciones como para los ciudadanos, dieron paso a los llamados *Electronic Government (e-Government)* y la administración electrónica *(e-Administración)*, mediante los cuales se busca la optimización de la provisión de la información, la prestación de los servicios públicos y la modernización de la gestión.[8]

---

[7] PUENTE DE LA MORA, Ximena, "Protección de datos personales en posesión de los particulares en México: Avances y Desafíos"*,* ponencia presentada en la Mesa 10: Protección de Datos Personales del XIV Congreso Iberoamericano de Derecho e Informática, Universidad Autónoma de Nuevo León, Facultad de Derecho y Criminología T, Federación Iberoamericana de Asociaciones de Derecho e Informática, realizado del 25 al 30 de octubre de 2010, formato pdf, disponible en http://biblio.juridicas.unam.mx/libros/6/2941/26.pdf, p. 911, consultada el 6 de abril de 2012.

[8] *Cfr.* GARCÍA GONZÁLEZ, Aristeo, "La protección de datos en la administración electrónica. Aspectos generales"*, Derecho comparado de la información*, número 14, julio-diciembre 2009, obra del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, ISSN 1870-0594, formato pdf, disponible en http://www.juridicas.unam.mx/publica/librev/rev/decoin/cont/14/art/art3.pdf, p. 85, consultada el 5 de abril de 2012.

Con lo anterior, podemos observar cómo los gobiernos empezaron a utilizar la tecnología para facilitar el cumplimiento de sus funciones y la prestación de servicios públicos, y con ello, el manejo de datos personales de manera automatizada; sin embargo esto no fue exclusivo de los entes públicos, pues también tuvieron acceso a los avances tecnológicos, el sector privado a través de investigadores y empresarios, quienes fueron sus principales impulsores. Así, la tecnología empezó a ser accesible para todos y a estar presente en varias actividades económicas y sociales del hombre, en beneficio del libre flujo de información, pero a la vez como amenaza en la vulneración de derechos.

Ante esta situación, la comunidad internacional empezó a manifestar una gran preocupación respecto del impacto que podía tener la tecnología en los derechos fundamentales, así como la posibilidad de regular el flujo transfronterizo de datos personales sin convertirse en un obstáculo para diversos sectores de la economía, reflexiones que más adelante motivaron para la conformación del derecho a la protección de datos personales.

Al respecto, Ximena Puente de la Mora presenta el esquema propuesto por Agustín Puente Escobar en su obra “Breve descripción histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal”, mediante el cual en una manera representativa y completa, expone la evolución de este derecho, sobre todo en Europa, con los primeros trabajos realizados y leyes emitidas en materia de protección de datos personales, para culminar con su reconocimiento como derecho fundamental; evolución que expone a través de las siguientes seis etapas:

> “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.
> 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 limitar el uso desenfrenado de la tecnología.

Así, la primera norma vinculante en esta materia le corresponde al Land de Hesse[9], del 7 de octubre de 1970.

Por su parte la primera Ley Nacional sobre Protección de Datos fue aprobada por el Parlamento Sueco del 11 de mayo de 1973, la cual incorpora la protección de 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 solo incorpora las bases de datos de organismos públicos.[10]

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 (*sic)* [personal].

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

4. 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 OCDE[11] 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

---

9 El *Land* en singular o *Länder* en plural, significa en alemán Estado y *Hesse* es uno de los 16 Estados que integran la República Federal Alemana.

10 El antecedente de la *Privacy Act* del 31 de diciembre de 1974 es la *Fair Credit Reporting Act* del 26 de octubre de 1970, en la cual se reguló el tratamiento genérico de datos personales.

11 OCDE son las siglas en español para referir a la Organización para la Cooperación y Desarrollo Económicos.

(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 la 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 …[12]

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 la (*sic)* 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, celebrada en Niza el 7 de diciembre de 2000. Además del pronunciamiento de sentencias que le otorgan a este derecho un ámbito propio como la STCE 290/2000 y 292/2000 [Sentencias del Tribunal Constitucional de España, emitidas el 30 de noviembre de 2000]". [13]

Como se puede observar con lo antes expuesto, el derecho a la protección de datos personales es de reciente creación y aún se encuentra en proceso de desarrollo y evolución, lo cual implica un gran desafío para aquéllos países que decidan implementarlo dentro de su derecho, toda vez que no basta con reconocerlo en sus disposiciones jurídicas sino también es necesario examinar dentro del contexto de la sociedad donde se desenvuelve, los alcances e impacto que tendrá en la vida y derechos de los individuos, para establecer mecanismos e instituciones especializadas que permitan su adecuada salvaguarda y pleno ejercicio por parte de sus titulares, así como su congruencia con los criterios básicos establecidos a nivel

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

[13] PUENTE DE LA MORA, Ximena, "Protección de datos personales en posesión de los particulares en México: Avances y Desafíos"*, Op. cit.,* pp. 912 y 913.

internacional y regional, a fin de lograr su más amplia y óptima protección, incluso más allá de sus fronteras; ello independientemente del reto para forjar este derecho de manera coherente con los cambios constantes de un mundo globalizado que gira al ritmo del desarrollo y avance acelerados de la tecnología y los intereses económicos.

II. Factores que contribuyeron al surgimiento y desarrollo del derecho a la protección de datos personales.

El derecho a la protección de datos personales puede ser analizado desde diferentes perspectivas: como un derecho derivado de derechos personalísimos; como el derecho que sólo puede desenvolverse en sistemas democráticos; como un derecho fundamental; como un derecho resultado del vertiginoso avance y desarrollo de la tecnología; y como un derecho que debe estar en congruencia y armonía con los intereses económicos y de libre mercado, para favorecer su crecimiento.

Para profundizar respecto del surgimiento y desarrollo del derecho a la protección de datos personales, en este punto analizaremos los diversos factores que a lo largo de la historia del hombre han contribuido a ese fin, como son:

1. El reconocimiento de la libertad individual, entendida como el derecho que tiene todo individuo para elegir y disfrutar una forma de vida digna;
2. El establecimiento de sistemas democráticos;
3. La evolución de los derechos fundamentales y, con ello, la presencia de las llamadas nuevas generaciones de derechos;
4. La aparición de nuevas tecnologías y su impacto en las denominadas sociedades de la información; y
5. La vinculación entre el derecho a la protección de la intimidad y de las libertades individuales y el fomento de la libre circulación de datos personales, derivado de la movilidad internacional de personas, mercancías y actividades comerciales y científicas.

En cuanto al primer factor relativo al reconocimiento de la libertad individual, Fernando Escalante Gonzalbo, al hacer la distinción entre la libertad de los antiguos y la de los modernos, señala: "… La libertad de los modernos es el derecho de cada quien a hacer su propia vida, sin interferencia de la colectividad. Por esa razón vemos en el ámbito privado el espacio más característico de la libertad. Definir

una actividad o una decisión como asunto privado significa decir que es libre … ajeno a toda forma de control público". [14]

Actualmente la libertad particular es reconocida como uno de los derechos más fundamentales de todo ser humano, por el cual el hombre es capaz de establecer los límites y control de su propia vida, en especial dentro de un espacio que considera privado, donde nadie puede interrumpirlo o vulnerarlo, aun y cuando se trate de personas o entes que gocen de cierta autoridad en determinados aspectos como familiar, social, religioso, económico o político, lo que incluye evidentemente al propio Estado, quien frente a este derecho adquiere el papel de garante de las libertades individuales conforme se establece en la ley. No obstante ello, al igual que en otros derechos, éste no es absoluto ya que quedará limitado en tanto no vulnere el derecho de los demás.

A partir de esta libertad individual el hombre goza de diversas libertades fundamentales reconocidas como derechos en todo el mundo, tales como la vida, libertad y seguridad de la persona; libertad de pensamiento, conciencia y religión; de opinión y expresión; de elección de un oficio o profesión; a tener una familia; de reunión y de asociación pacíficas; de voto, entre otros. Lo anterior hace de la libertad individual un concepto muy amplio, que no sólo comprende el aspecto meramente externo, físico o tangible, sino también lo interno, lo intangible, lo relativo a las sensaciones y al intelecto.

Como consecuencia del ejercicio de esa libertad, surge la necesidad de establecer un ámbito privado igualmente protegido por el Derecho, donde el hombre pueda elegir libremente, llevar una vida digna e incluso decidir con quién compartir ese espacio, siempre y cuando en el ejercicio de su derecho, no afecte el de los demás.

En cuanto al segundo factor que ha influido para el surgimiento del derecho a la protección de datos personales, se encuentra el establecimiento de sistemas democráticos, relacionado con el primer factor, toda vez que en este tipo de sistemas es más probable que los individuos realicen un ejercicio responsable de su libertad, sin recibir por parte de la autoridad algún tipo de irrupción en su vida personal, en aspectos como su religión, familia, propiedad, salud, trabajo e incluso su propio pensamiento. Por ello, Fernando Escalante Gonzalbo afirma que la consolidación de un espacio privado se da a partir de la neutralidad del Estado y la libertad individual.

---

[14] ESCALANTE GONZALBO, Fernando. *El Derecho a la privacidad*, 02 Cuadernos de transparencia del Instituto Federal de Acceso a la Información y Protección de Datos, octava reimpresión, México, 2010, pp. 16 y 17.

En estos sistemas democráticos es donde emerge el Estado de Derecho, donde es más factible el reconocimiento de derechos fundamentales en sus disposiciones legales, así como el establecimiento de mecanismos e instituciones adecuadas para su protección y ejercicio efectivo por parte de sus titulares.

Al respecto, Héctor Cuadra afirma: "… la expansión y la observancia del principio del Estado de Derecho constituye la única alternativa racional y razonable frente a la intolerancia, la arbitrariedad, la injusticia y la violencia y por consiguiente la mejor garantía de los derechos humanos … El Estado de Derecho sólo puede concebirse y realizarse donde los derechos del hombre se reconocen y respetan plenamente.[15]

Por ello el citado autor alude al Estado de Derecho como aquél basado en valores fundamentales correspondientes a una sociedad libre, donde se reconoce como valor supremo a la propia persona, y el Estado, así como sus instituciones se encuentran al servicio del individuo. Los requerimientos esenciales de un Estado de Derecho deben coincidir con las condiciones mínimas de un sistema jurídico, en el cual los derechos y la dignidad humanos son respetados, entre las que se encuentran:

- "La garantía de la seguridad personal.
- La prohibición constitucional de reglamentar, por otra vía que no sea la legislativa, las diversas libertades públicas consagradas y por vía administrativa tan sólo el ejercicio efectivo.
- La garantía de la libertad de opinión y de expresión.
- El derecho a la información y por consiguiente la prohibición de la censura.
- La inviolabilidad de la vida privada y el derecho al secreto en la correspondencia.
- La libertad de conciencia o libertad de credo.
- La independencia del poder judicial y la garantía de su imparcialidad son una condición indispensable de un Estado libre y democrático.
- El poder legislativo deberá ser ejercido efectivamente por un organismo apropiado elegido libremente por los ciudadanos.
- Los funcionarios de la administración y de los servicios públicos estatales deberán ejercer sus funciones al servicio de la

[15] CUADRA, Héctor, *La Proyección Internacional de los Derechos Humanos*, Instituto de Investigaciones Jurídicas, Serie B. Estudios comparativos, b) Estudios especiales, número 10, México, 1970, pp. 13 y 14.

comunidad y no de un partido político o de una organización política determinada". [16]

En consecuencia el derecho a la protección de datos personales, dada su condición de derecho fundamental, se ha desarrollado en aquellos países que cuentan con sistemas democráticos, lo cual se vuelve en un requisito necesario para lograr un adecuado ejercicio de este derecho bajo condiciones que mejor lo garanticen. Por lo tanto, dicha exigencia también se dará al momento de la transferencia de datos, puesto que para ello se requiere que el país receptor cuente con similares condiciones y medidas de protección de las otorgadas por el país de origen.

El tercer factor se refiere al reconocimiento de nuevos derechos como resultado de los cambios y necesidades que surgen en determinadas épocas y culturas. En esa tesitura Ferrajoli señala: "… Se puede decir que las diversas generaciones de derechos corresponden a otras tantas generaciones de movimientos revolucionarios…" [17] Los cuales deben ser entendidos no necesariamente como movimientos armados, sino como cualquier cambio violento en instituciones políticas, económicas o sociales, realizado en un país o región.

Aristeo García González[18] señala que en esta evolución ha prevalecido el reconocimiento de tres generaciones de derechos humanos:

En la primera generación se encuentran las libertades individuales, que se reconocen en el Siglo XVIII, las cuales se caracterizan por la autolimitación y la no injerencia de los poderes públicos en la esfera privada de la persona. En esta generación se encuentran el derecho al honor, a la vida, a la integridad personal y a la intimidad.

La segunda generación de derechos surge como consecuencia de las luchas sociales del siglo XIX, en donde se encuentran los derechos económicos, sociales y culturales.

---

16 *Ibidem*, p. 15.

17 FERRAJOLI, Luigi, *Derechos y garantías. La ley del más débil,* Madrid, Trotta, 2004, p. 54.

18 GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado", *Boletín Mexicano de Derecho Comparado*, número 120, septiembre-diciembre 2007, obra del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, ISSN 0041 8633, formato pdf, disponible en: http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/120/art/art3.pdf, pp. 746-748, consultada el 19 de marzo de 2012.

En cuanto a la tercera generación de derechos y libertades, según el mismo autor, se presenta como una respuesta al fenómeno denominado "contaminación de las libertades" (*liberties' pollution)*, término utilizado en la teoría social anglosajona para referir a la erosión y degradación de los derechos fundamentales ante determinados usos de nuevas tecnologías. Es en esta generación donde se ubica el derecho a la libertad informática, autodeterminación informativa, o bien, derecho a la protección de datos personales.

Como cuarto factor se encuentra la aparición y desarrollo de nuevas tecnologías, a través de las cuales el hombre puede tener acceso a un sinnúmero de información de cualquier parte del mundo. Con el surgimiento a finales del siglo XX y principios del XXI de las llamadas Tecnologías de la Información y Comunicación (TIC's), en poco tiempo, el mundo se vio envuelto en una revolución tecnológica que vino a cambiar y continúa haciéndolo, la forma de vida de la sociedad. Su impacto fue tal, que todos los ámbitos como el económico, político, social, jurídico, cultural, entre otros, se vieron influenciados por aquéllas, convirtiéndose para la mayoría, en las herramientas casi indispensables y necesarias de sus actividades.

Para los estudiosos de esta materia, con la revolución tecnológica surge un nuevo orden social conocido como la sociedad informática, que de acuerdo con Raúl Trejo Delarbre es la: "… expresión de las realidades y capacidades de los medios de comunicación más nuevos, o renovados merced a los desarrollos tecnológicos que se consolidaron en la última década del siglo: … La digitalización de la información es el sustento de la nueva revolución informática. Su expresión hasta ahora más compleja, … es la Internet".[19]

Con el uso de las TIC's la información circula rápidamente, entre ella la personal, así como facilita su almacenamiento, gestión, modificación, transmisión o reproducción, pero a la vez el uso excesivo de los datos personales, o una exposición mayor a un uso inadecuado o indebido, poniendo en grave peligro los derechos y libertades individuales de aquellos a quienes pertenecen, pues en la mayoría de los casos, sus dueños desconocen quién tiene sus datos, en dónde se encuentran y para qué fines están siendo utilizados.

Esta desmesurada circulación y exposición de la información hace necesario el establecimiento de mecanismos adecuados de protección para evitar la

[19] TREJO DELARBRE, Raúl, "Vivir en la sociedad de la información. Orden global y dimensiones locales en el universo digital", *La Sociedad de la Información,* Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI), España, Número 1, septiembre-diciembre 2001, ISSN: 1681-5645, disponible en http://www.oei.es/revistactsi/numero1/trejo.htm, consultada el 19 de marzo de 2012.

vulneración de derechos, dado el doble impacto, tanto positivo como negativo, que tiene el uso de las TIC's en la actualidad.

Por ello Marcia Muñoz de Alba Medrano señala: "el papel que juegan las técnicas de comunicación telemáticas frente a los derechos humanos es dual ya que por un lado, la informática se constituye en el instrumento capaz y eficiente para hacer respetar los principios de estos derechos y por el otro, representa el ámbito amenazante en la sociedad contemporánea para poderlos aniquilar".[20]

Ante este dualidad, como se mencionó anteriormente, la comunidad internacional ha manifestado su preocupación y se ha dispuesto a identificar los peligros que pueden derivarse del uso de nuevas tecnologías en perjuicio de los derechos fundamentales, para abatirlos o limitarlos sin menoscabo de la dignidad humana, las garantías y las libertades que tiene todo individuo.

Lo anterior, da lugar al quinto y último factor que se refiere a la vinculación entre el derecho a la protección de la intimidad y a las libertades individuales y el fomento de la libre circulación de datos personales, derivado de la constante movilidad internacional de personas, mercancías y actividades comerciales y científicas, donde la información puede adquirir un valor económico y los datos personales convertirse en objeto del comercio.

En la actualidad la obtención y tratamiento de la información se convierte en uno de los principales motores de diversos sectores de la economía, pues con la libre circulación de datos personales y la elaboración de perfiles cada vez más individualizados, se favorece el incremento de ventas, clientes, ganancias y, en su caso, la eliminación de competidores. Esto ha dado lugar a que no sólo se afirme que la información es poder sino también una fuente de riqueza en este siglo, como lo expresó Stefan Gross-Selbeck, presidente de Xing, una de las redes sociales para profesionales más importantes, en la Conferencia Mundial sobre Internet[21] en Alemania, en la cual señaló: "Los datos personales son el petróleo del siglo XXI".[22]

---

[20] MUÑOZ DE ALBA MEDRANO, Marcia, "Los nuevos derechos humanos en la era tecnológica: ¿El *Habeas Data*… la solución?"*, V Congreso Iberoamericano de Derecho Constitucional*, Instituto de Investigaciones Jurídicas, México, 1998, Serie G: Estudios Jurídicos, número 193, ISBN 968-36-6786-4, formato pdf, disponible en http://biblio.juridicas.unam.mx/libros/1/113/28.pdf, p. 585, consultada el 19 de marzo de 2012.

[21] En la Conferencia Mundial sobre Internet se señaló que en el 2020 se estima que a través de 15 mil millones de objetos de comunicación, se intercambie información personal, pues tan sólo los teléfonos multifunción ya recolectan una gran cantidad de datos personales de su propietarios y de sus contactos, información utilizada por las empresas para dirigir mejor sus publicidades por perfiles bien definidos.

[22] AGENCE FRANCE-PRESSE, "Datos personales, mina de oro para los gigantes de internet"*,* Periódico Organización Editorial Mexicana, Sección Ciencia y Tecnología, 24

Debido a esta nueva visión, en los foros internacionales se planteó la necesidad de proteger los derechos de los individuos del uso y control de sus datos personales por parte de diversos controladores de datos, tanto públicos como privados, a través del establecimiento de estándares mínimos que hicieran congruente el ejercicio de derechos individuales y la libre circulación de datos, sin menoscabo de uno u otro.

Los principales trabajos al respecto fueron llevados a cabo por los miembros de la Organización para la Cooperación y Desarrollo Económicos (OCDE), la cual preocupada por atender los problemas de discrepancia en la regulación existente en protección de este derecho, ordenó en 1978 a un Grupo de Expertos la elaboración de directrices sobre normas básicas para regir la circulación transfronteriza de datos, la protección de datos personales y la intimidad, a fin de facilitar la armonización de la legislación nacional.

Como resultado de los trabajos encomendados al Grupo de Expertos, el 23 de septiembre de 1980, el Consejo de la OCDE emitió la recomendación del Consejo relativa a las Directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales, mediante la cual los países miembros se comprometieron a tomar en cuenta en su legislación nacional, los principios relativos a la protección de la intimidad y de las libertades individuales expuestas en las Directrices; a procurar retirar o evitar la creación de obstáculos injustificados a la circulación transfronteriza de datos personales, en aras de la protección de la intimidad; y cooperar en su implementación.

En razón del valor que se le ha dado a los datos personales, es importante considerar dos elementos para su tratamiento, ya sea por parte del sector público o privado, primero el respeto irrestricto a las libertades y derechos fundamentales de los individuos, y segundo, la contribución al progreso económico y social, al desarrollo de los intercambios, y al bienestar de los individuos; de tal manera que se logre el equilibrio entre ambas, siendo necesario para dicho objetivo, la colaboración internacional entre los Estados y la homologación de estándares mínimos de protección.

---

de enero de 2012, disponible en http://www.oem.com.mx/laprensa/notas/n2398578.htm, consultada el 5 de abril de 2012.

III. Definición del derecho a la protección de datos personales.

Antes de proporcionar una definición del derecho a la protección de datos personales, es importante conocer primero los conceptos que se han relacionado estrechamente con el derecho objeto de nuestro estudio: intimidad, privacidad y vida privada, cuyo análisis permitirá entenderlo y comprenderlo mejor, así como utilizarlo de manera adecuada. Lo anterior resulta relevante al observar que en la práctica es común el uso indistinto de estos conceptos por la delgada línea que los separa, dada su similitud en contenido y su estrecha vinculación.

Para la exposición de este tema, buscaremos apoyo en la doctrina que se ha desarrollado en materia de derechos de la persona o la personalidad, así como en la jurisprudencia que se ha emitido al respecto en el sistema jurídico mexicano, las cuales han explicado con mayor claridad estos conceptos, así como identificado sus diferencias.

La intimidad y la vida privada antes de ser establecidos como derechos humanos, garantizados a través de instrumentos legales nacionales e internacionales, fueron considerados como derechos innatos pertenecientes al individuo por el simple hecho de ser hombre y tener una dignidad humana, con independencia de su reconocimiento o no por parte del Estado o de los demás sujetos, ubicados dentro de los denominados derechos de la personalidad.

Los derechos de la personalidad, se encuentran relacionados en su origen con la dignidad humana, la cual no siempre fue reconocida para todos los seres humanos. Según Eduardo Vázquez Bote, la filosofía estoica representó el primer intento de atribuir dignidad a los seres humanos quienes *iure naturales* nacen libres, pero no fue hasta el cristianismo que se afirmó una dignidad humana referida a todos los hombres. En la Edad Media se aceptó el principio de dignidad sin otorgarle el auge correspondiente; fue a partir del Renacimiento que en la doctrina los derechos de la personalidad se entienden en un doble camino: "… a) de un lado, se pretenderá sostener la dignidad del ser humano frente al Estado y, en general, frente a los sectores que detentan el poder político; b) de otro lado, se pretenderá sostener la dignidad humana por el simple hecho de ser todo hombre persona". [23]

[23] VÁZQUEZ BOTE, Eduardo, "Los denominados derechos de la personalidad", *Boletín Mexicano de Derecho Comparado*, número 18, septiembre – diciembre 1973, Nueva Serie Año VI, ISSN 0041 8633, formato pdf, disponible en http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/18/art/art3.pdf, p. 406, consultada el 3 de abril de 2012.

Vázquez Bote señala que de este doble camino, surgen en la doctrina dos corrientes de los derechos de la personalidad: como concepto esencial de la vida jurídico privada y como concepto en el ámbito jurídico público, siendo en este último concepto donde nacen las corrientes de los denominados derechos civiles o derechos políticos, antecedente de la doctrina de los derechos humanos.

En cuanto a lo que se entienden por estos derechos, Iván Lagunes Pérez explica: "Se ha dado en llamar derechos de la personalidad a diversos privilegios y facultades en general reconocidos legalmente a la persona física, para el ordinario goce de bienes derivados de su propia esencia individual exhibida y desarrollada en el medio social en que vive".[24]

En opinión de Luz del Carmen Martí de Gidi, los derechos de la personalidad son: "… derechos esenciales o fundamentales, innatos, ya que nacen con la persona sin requerir acto jurídico alguno que motive su adquisición, y que atribuyen a su titular un poder de amplia disposición para proteger todo lo que él entiende que concierne a la esencia de su persona y las cualidades que la definen".[25]

Derivado de lo anterior, observamos que el término personalidad no se encuentra en su aceptación meramente jurídica, entendida como la aptitud para ser sujeto de derechos y obligaciones, sino como la personalidad humana referida a las facultades que le permiten a un individuo manifestar de manera libre y consciente su individualidad, con las cualidades físicas y psíquicas que lo distinguen de los demás en el medio donde se desenvuelve.

En este caso se trata de bienes intangibles conformados por el pensamiento, sentimientos y sensaciones, los cuales integran la esencia del ser humano, y de donde se derivan derechos como la libertad personal, el honor, la intimidad, la integridad, entre otros. De esta manera, los derechos de la personalidad poseen las siguientes características:

1. Subjetivos, hay una permisión para su titular de ejercer su derecho y el deber correlativo de los demás para no interferir en su derecho.
2. Personalísimos, sólo pueden ser ejercidos por su titular.
3. Innatos, pertenecen al individuo por el simple hecho de ser humano.
4. Inalienables, no es posible su enajenación o renuncia absoluta.

---

[24] Apuntes de Derecho Civil I impartida por el doctor Iván Lagunes Pérez, el 2 de marzo de 1995 en la Universidad La Salle.

[25] MARTÍ DE GIDI, Luz del Carmen, "Vida privada, honor, intimidad y propia imagen como derechos humanos"*, Letras jurídicas*, Volumen 8, Año 4, julio-diciembre 2003, revista del Centro de Estudios sobre Derecho, Globalización y Seguridad de la Universidad Veracruzana, ISSN 1665 1529, formato pdf, disponible en http://www.letrasjuridicas.com/ Volumenes/8/luz8.pdf, p. 116, consultada el 3 de abril de 2012.

5. Irrenunciables e imprescriptibles, su titular no puede renunciar a ellos de manera total y definitiva.
6. Absolutos, en el sentido que se hacen respetar ante todos los sujetos (porque ningún derecho es absoluto).
7. Variables, cambian de acuerdo con el contexto social donde se desenvuelva el individuo.
8. Extrapatrimoniales, no tienen un valor pecuniario. También son considerados como un patrimonio moral.

Si bien no existe unanimidad en la doctrina respecto de cuáles son estos derechos, si lo existe para incluir dentro de sus diversas clasificaciones a los derechos de la intimidad y el de la vida privada, los cuales resultan de interés para la presente investigación.

a) Intimidad

El derecho a la intimidad se encuentra en el ámbito de lo más privado, está referido a lo individual o subjetivo, tiene el carácter de absoluto, exclusivo y excluyente, se presenta generalmente en secreto o sigilo, en consecuencia se caracteriza por su inaccesibilidad. Intimidad es lo que se guarda en el interior, no se comparte con nadie o con muy pocos, pero siempre de manera voluntaria y consciente.

El concepto de intimidad en su acepción moderna, surgió en 1873 cuando el juez Cooley en su obra *The elements of torts* llegó a la conclusión de que *privacy* constituía el derecho a ser dejado solo, el *right to be alone*. Posteriormente los abogados Warren y Brandeis retoman esa idea y la exponen detalladamente en su artículo denominado *The right to the privacy*, publicado en la Revista de la Facultad de Derecho de Harvard en 1890.

En dicho artículo sus autores refieren que la ley solo protegía las inferencias físicas relacionadas con el derecho a la vida y a la propiedad, pero posteriormente hubo un reconocimiento de la naturaleza espiritual del hombre, de sus sentimientos y de su intelecto. Así, el derecho a la vida sufrió una transformación para convertirse en un derecho a disfrutar de la vida, un derecho a ser dejado en paz, donde los bienes intangibles como pensamientos, emociones y sensaciones también tienen un reconocimiento legal.

La propuesta de un derecho a la intimidad expuesta en ese artículo, ocasiona una diversidad de comentarios, tanto a favor como en contra en el mundo jurídico, pero no es sino hasta 1905 que tiene un impacto contundente en el caso *Pavesick & New England Life Insurance Company*, cuando la Corte Suprema de

Georgia en Estados Unidos de Norteamérica, resolvió reconocer el derecho a la intimidad, cuando en un anuncio publicitario de la referida compañía de seguros, ésta usó el nombre, imagen y testimonio de una persona sin haber manifestado su consentimiento, lo cual se convirtió en precedente jurisprudencial en esta materia.

En la sentencia se estableció que la persona tiene un derecho a disfrutar de la vida en la forma que le sea más agradable y placentera, de acuerdo con su temperamento y naturaleza, siempre que en tal disfrute no invada los derechos de su vecino o viole el derecho público. Asimismo señala que cada uno es titular de una libertad de elegir con respecto a su forma de vida y nadie tiene derecho a robarle esta libertad arbitrariamente.

Según Fernando Escalante Gonzalbo "… lo íntimo cabe dentro de lo privado, pero es más estrecho y personal, más reducido; … es íntimo lo que se hace rigurosamente fuera de la mirada de otros, que sólo se manifiesta voluntariamente, a unos cuantos".[26]

Para la Firma Davara Abogados la intimidad alude a sentimientos, creencias (políticas, religiosas), pensamientos o a información como la clínica o la relativa a la vida sexual cuya difusión puede producir ciertas reservas al individuo.[27]

En la tesis aislada P. LXVII/2009 con número de registro 165821, denominada **DERECHOS A LA INTIMIDAD, PROPIA IMAGEN E IDENTIDAD PERSONAL Y SEXUAL. CONSTITUYEN DERECHOS DE DEFENSA Y GARANTÍA ESENCIAL PARA LA CONDICIÓN HUMANA,** el Pleno de la Suprema Corte de Justicia de la Nación señala que el derecho a la intimidad se encuentra necesariamente dentro de los derechos personalísimos, el cual se entiende como: "… el derecho del individuo a no ser conocido por otros en ciertos aspectos de su vida y, por ende, el poder de decisión sobre la publicidad o información de datos relativos a su persona, familia, pensamientos o sentimientos …"[28]

---

26 ESCALANTE GONZALBO, Fernando. *El derecho a la privacidad*, *Op. cit.*, p. 22.

27 FIRMA DAVARA ABOGADOS, S.C., "¿Y sus datos están protegidos?", *IDC Asesor Jurídico y Fiscal*, Ediciones Especiales IDC 2012, Boletín quincenal, Año 25, cuarta época, Grupo Expansión, México, enero 2012, p. 3.

28 Tesis aislada P. LXVII/2009, Novena Época, Instancia Pleno, Semanario Judicial de la Federación y su Gaceta XXX, Diciembre de 2009, p. 7, materias civil y constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 165821.

Por lo anterior, la intimidad refiere a la esfera privada, lo que se decide dejar fuera de las miradas de los demás, a estar libre de la intromisión ajena en asuntos que sólo pertenecen al individuo y, por tanto, sin ningún impacto social, dando la posibilidad a su titular de excluir y evitar injerencias.

b) Privacidad

Para algunos la palabra privacidad es un anglicismo, que tiene su origen en la palabra inglesa *privacy*, entendida como el estado o condición de estar retirados de la sociedad, de otros o del interés público, aislamiento; otros señalan que el término viene del latín *privatus* que significa separar de lo demás. El Diccionario de la Lengua Española señala por privacidad, "el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".[29]

Según Lucrecio Rebollo Delgado, en el Reino Unido los términos *intimity* o *intimacy*, originarios de intimidad quedaron obsoletos o desposeídos de una concepción de interioridad y fueron sustituidos por el de privacidad, del que surge el *right of privacy,* desarrollado ampliamente en el derecho de los Estado Unidos de Norteamérica, entendido como el derecho a ser dejado en paz.[30]

De acuerdo con la Firma Davara Abogados, "no existe ni una definición de privacidad como tal. El concepto es, en gran medida subjetivo, puesto que varía en relación con la evolución de la sociedad y factores diversos, tales como la cultura, el ambiente político, tecnológico, económico … los datos de salud se encuentran en el centro mismo del significado del *concepto de privacidad."*[31]

De esta manera, se deduce que la privacidad es un término cambiante de acuerdo con el entorno o situación política, social o cultural donde se presente, motivo por el cual su significado dependerá del lugar y contexto donde sea utilizado; como pudiera ser sólo una referencia más a la idea de intimidad, pero bajo otra acepción mayormente utilizada en el derecho americano e inglés; o simplemente un término que refleja la idea contraria a lo público, pero no el derecho como tal.

---

29 Diccionario de la Lengua Española, vigésima segunda edición, Real Academia Española, España, 2001, disponible en http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=privacidad, consultada el 20 de marzo de 2012.

30 *Cfr.* REBOLLO DELGADO, Lucrecio, *El derecho fundamental a la intimidad*, segunda edición actualizada, Dykinson, S.L., Madrid, 2005, disponible en http://books.google.com.mx/books?hl=es&id=S9_loNaIDyUC&q=intimidad#v=snippet&q=intimidad&f=false, ISBN 84-9772-698-7, p. 50, consultada el 5 de abril de 2012.

31 FIRMA DAVARA ABOGADOS, S.C., "¿Y sus datos están protegidos?", *Op. cit.*, p. 3.

c) Vida privada

La vida privada es todo lo que se refiere a lo particular y personal de cada individuo, el ámbito o espacio privado y ajeno de toda intromisión que se encuentra reservado frente a la acción y conocimiento de los demás, y que a través de su ejercicio permite al individuo delimitarlo y separarlo de su ámbito público.

Parafraseando a Cuauhtémoc Manuel de Dienheim Barriguete, todos los seres humanos tenemos una vida privada, conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y por lo mismo, no está destinada a trascender e impactar a la sociedad de manera directa. Pero es muy difícil definir el concepto de vida privada dada las diversas connotaciones que tiene, las cuales dependen de la sociedad de que se trate, sus circunstancias particulares y la época o el periodo que corresponda. No obstante la dificultad para definirlo, es posible establecer su contenido: "… dentro de esta esfera de vida privada podemos considerar a las relaciones personales y familiares, afectivas y de filiación, las creencias y preferencias religiosas, convicciones personales, inclinaciones políticas, condiciones personales de salud, identidad y personalidad psicológica, inclinaciones sexuales, comunicaciones personales privadas por cualquier medio, incluso algunos llegan a incluir la situación financiera personal y familiar".[32]

En cuanto a la probable similitud del derecho a la vida privada con el derecho a la intimidad, la Primera Sala en la tesis aislada 1ª.CXLIX/2007 con número de registro 171883, expone claramente la relación que existe entre estos derechos, así como identifica ciertas características que permiten su distinción, de la siguiente manera:

> "**VIDA PRIVADA E INTIMIDAD. SI BIEN SON DERECHOS DISTINTOS, ÉSTA FORMA PARTE DE AQUÉLLA.** La vida se constituye por el ámbito privado reservado para cada persona y del que quedan excluidos los demás, mientras que la intimidad se integra con los extremos más personales de la vida y del entorno familiar … Así, el concepto de vida privada comprende a la intimidad como el núcleo protegido con mayor celo y fuerza porque se entiende como esencial en la configuración de la persona, esto es, la vida privada es lo genéricamente reservado y la intimidad –como parte de aquélla- lo radicalmente vedado, lo

[32] DE DIENHEIM BARRIGUETE, Cuauhtémoc Manuel, "El Derecho a la intimidad, al honor y a la propia imagen", *Derechos Humanos*, Órgano Informativo de la Comisión de Derechos Humanos del Estado de México, Número 57, septiembre-octubre 2002, ISSN 1405-5627, formato pdf, disponible en http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/57/pr/pr28.pdf, p. 59, consultada el 3 de abril de 2012.

> más personal; de ahí que si bien son derechos distintos, al formar parte uno del otro, cuando se afecta la intimidad, se agravia a la vida privada". [33]

La anterior explicación permite observar claramente ese delgado límite que hay entre el derecho a la vida privada y el derecho a la intimidad, y comprender la razón de su uso indistinto como si se tratara de sinónimos. La vida privada debe ser entendida en un sentido más amplio y la intimidad en un nivel más concreto; la intimidad está contenida en aquélla y al encontrarse en lo más interior de una persona, es más probable que sea más altamente reservada y excluida de la injerencia de los demás.

Y esta diferencia se expondrá en mayor o menor medida, según lo determine el propio individuo, cuando al ejercer su derecho, decida qué parte de su vida privada establecerá como la más íntima y por tanto excluirá con mayor sigilo del conocimiento de los demás; así como decidir qué parte de su vida privada hará pública y qué mantendrá fuera del alcance de los demás.

En este sentido, la Corte Suprema de Georgia, Estados Unidos de América, en la sentencia del caso de *Pavesick & New England Life Insurance Company* antes mencionado, señaló que en ejercicio de la libertad para vivir como cada individuo quiera, uno puede querer llevar una vida de reclusión; otro llevar una vida de publicidad; pero otro quizás llevar una vida con intimidad respecto a ciertos asuntos y con publicidad respecto de otros.

La complejidad del término de vida privada no sólo deriva de la aparente similitud con el de intimidad, sino también de la forma cómo se vincula a su vez con otros derechos, como los enunciados por Cuauhtémoc Manuel de Dienheim Barriguete:

- El derecho a la inviolabilidad de domicilio.
- El derecho a la inviolabilidad de correspondencia.
- El derecho a la inviolabilidad de las comunicaciones privadas.
- El derecho a la propia imagen.
- El derecho al honor.
- El derecho a la privacidad informática.
- El derecho a no participar en la vida colectiva y a aislarse voluntariamente.

---

[33] Tesis aislada 1a.CXLIX/2007, Novena Época, Instancia Primera Sala, Semanario Judicial de la Federación y su Gaceta XXVI, Julio de 2007, p. 272, materia penal, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 171883.

- El derecho a no ser molestado.
- El derecho a la no exteriorización del pensamiento e ideas como parte de la libertad de expresión, la libertad de religión y creencias, la libertad de procreación y de preferencia sexual, la libertad de pensamiento y de preferencia política.
- El derecho a la libertad de expresión, de imprenta y de información, en el sentido que el derecho a la vida privada se establece como límite al ejercicio de estas libertades. [34]

El vínculo que existe entre el derecho a la vida privada y otros derechos, también lo expone la Primera Sala en la tesis aislada 1a.CCXIV/2009 de la siguiente manera:

> "**DERECHO A LA VIDA PRIVADA. SU CONTENIDO GENERAL Y LA IMPORTANCIA DE NO DESCONTEXTUALIZAR LAS REFERENCIAS A LA MISMA**. En un sentido amplio, … la protección constitucional de la vida privada implica poder conducir parte de la vida de uno protegido de la mirada y las injerencias de los demás, y guarda conexiones de variado tipo con pretensiones más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos: el derecho de poder tomar libremente ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular".[35]

En consecuencia, el derecho a la vida privada permite la libre expresión de la identidad de las personas, tanto en sus relaciones con los demás como en lo individual y aunque no siempre lo vamos a encontrar bajo esta acepción en las disposiciones legales, sí podrá estar inmerso en los diversos derechos con los que está relacionado.

---

[34] *Cfr.* DE DIENHEIM BARRIGUETE, Cuauhtémoc Manuel, "El Derecho a la intimidad, al honor y a la propia imagen", *Op. cit.*, pp. 59 y 60.

[35] Tesis aislada 1a.CCXIV/2009, Novena Época, Instancia Primera Sala, Semanario Judicial de la Federación y su Gaceta XXX, Diciembre de 2009, p. 277, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 165823.

Una vez expuestos los términos de intimidad, privacidad y vida privada, trataremos de establecer una definición del derecho a la protección de datos personales como a continuación se menciona.

d) Protección de datos personales

En el contexto social previo a la conformación de este derecho, se observó que con la libre circulación de datos en el mundo, la afectación que podía tener el individuo no sólo se encontraba circunscrito al derecho a la intimidad, y lo que ello implica, como ser dejado en paz e impedir el abuso o revelación de su información íntima. Por ello, fue necesario buscar la ampliación del concepto tradicional de intimidad bajo nuevos matices, a fin de hacerlo más apropiado a las necesidades que iban surgiendo en la materia.

En este sentido, Aristeo García González explica la evolución del derecho a la intimidad, cuando alude al control y almacenamiento de datos personales por parte de los sectores públicos y privados como una práctica habitual de la actualidad, de la siguiente manera: "… el derecho a la intimidad ha tenido que ir redireccionando su ámbito de protección, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, ahora supone el reconocimiento de un derecho de control y acceso de sus informaciones, es decir, de toda aquella información relativa a su persona".[36]

Por su parte, José Luis Piñar Mañas señala en su obra Protección de Datos de Carácter Personal en Iberoamérica: "… este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización y omisión de determinados comportamientos concretados en la ley".[37]

En términos generales el concepto de datos personales se refiere al conjunto de informaciones sobre una persona física, la cual debe ser identificada o identificable, a través del cual se pretende que el individuo goce de un poder para

---

[36] GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado"*, Op. cit,* 745.

[37] GÓMEZ-ROBLEDO, Alonso y Lina, Ornelas Núñez, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal,* Instituto de Investigaciones Jurídicas, Serie Estudios Jurídicos, número 97, México, 2006, ISBN 970-32-3913-7, formato pdf, disponible en http://biblio.juridicas.unam.mx/libros/5/2299/3.pdf, p. 16, consultada el 5 de abril de 2012.

controlar sus datos personales, y establecer límites a los demás para su uso y destino.

Para Gómez Robledo y Ornelas Núñez el derecho a la protección de datos personales, no sólo contempla como único elemento las prerrogativas que tiene el titular, sino también todos aquellos principios y procedimientos que se encuentran relacionados, por lo cual brindan la siguiente definición de manera más amplia:

> "… el derecho a la protección de datos personales se traduce en el reconocimiento y establecimiento de prerrogativas, principios y procedimientos para el tratamiento por parte del Estado o de terceros, de la información concerniente a personas físicas. Las prerrogativas son el derecho a ser informado de la existencia de bases de datos que contengan su información, a otorgar su consentimiento, libre, expreso e informado para la transmisión de dicha información, así como el derecho de oponerse a que sean utilizados y finalmente a solicitar que se corrijan o cancelen (derecho al olvido) cuando así resulte procedente".[38]

En cuanto a los diversos términos utilizados para identificar el derecho a la protección de datos personales, encontramos el derecho a la libertad informática, derecho a la autodeterminación informativa o en la forma de una garantía procesal el *habeas data*. A pesar de ser utilizados como conceptos similares, en los dos últimos términos podemos identificar características especiales que permiten distinguirlos de este derecho.

La autodeterminación informativa, es el bien jurídico a proteger en el derecho a la protección de datos personales, por lo cual va más allá del concepto de intimidad, en su aspecto meramente negativo de no intromisión, pues además permite a su titular una participación activa en el resguardo de su derecho. Al respecto, Marcela I. Basterra indica que "… el derecho a la autodeterminación informativa consiste en la posibilidad que tiene el titular de un dato personal de controlar quiénes serán destinatarios de dicha información y qué uso se dará a la misma. Se ejerce genéricamente a través de los derechos de acceso, rectificación y cancelación".[39]

---

[38] GÓMEZ-ROBLEDO, Alonso y ORNELAS NÚÑEZ, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal, Op. cit*., pp. 17 y 18.

[39] BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados Derecho Constitucional Provincial Iberoamérica y México*, Buenos Aires, Ediar, México, Universidad Nacional Autónoma de México, 2008, p. 11.

De acuerdo con Carlos G. Gregorio el concepto de autodeterminación informativa apareció formalmente en la sentencia del Tribunal Constitucional alemán del 15 de diciembre de 1983 en relación con la Ley del Censo, en la cual se prohibió "… explícitamente al gobierno generar "un inventario de datos personales de los individuos por medio de censos gubernamentales de carácter confidencial". Luego de esta decisión el derecho a la privacidad incluye el derecho a controlar la información sobre sí mismo y la capacidad para determinar si esa información puede ser recogida y cómo puede ser usada".[40]

En cuanto al *habeas data* es la garantía constitucional, el procedimiento jurisdiccional o recurso para salvaguardar el derecho a la autodeterminación informativa. Según Marcela I. Basterra es "una acción de protección de datos personales específicamente ordenada a la defensa de la intimidad de los datos, del derecho a la autodeterminación informativa y a la propia imagen".[41] Para Víctor Bazán el *habeas* data, según las particularidades léxico-jurídicas del país de que se trate, puede conceptuarse "como una acción, una garantía constitucional, un procedimiento jurisdiccional de trámite especial y sumarísimo, un proceso constitucional o un recurso protectorio del derecho de autodeterminación informativa o derecho a la protección de datos personales, frente a los posibles excesos del poder de registración precisamente de la información de carácter personal".[42]

En este último sentido el *habeas data* puede considerarse, de acuerdo al contexto de cada país, como el procedimiento constitucional, jurisdiccional o incluso administrativo, mediante el cual se protege el derecho a la autodeterminación informativa y se brindan los mecanismos legales para su protección.

Ximena Puente de la Mora puntualiza que el derecho a la protección de datos de recién conformación, ha recibido diversas denominaciones utilizadas de manera frecuente en la legislación, doctrina y jurisprudencia de acuerdo con sus diferentes tradiciones jurídicas, pero el término que la doctrina más reciente en este tema, así como los instrumentos jurídicos internacionales han utilizado es el de derecho a la protección de datos, el cual define como la "suma de principios,

---

40 GREGORIO, Carlos G., *Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina, Op. cit.*, p. 310.

41 BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados Derecho Constitucional Provincial Iberoamérica y México*, *Op. cit.*, p. 38.

42 BAZÁN, Víctor, "El habeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado", *Estudios Constitucionales*, Vol. 3, número 002, Centro de Estudios Constitucionales, Santiago, Chile, Red de Revistas Científicas de América Latina y el Caribe, España y Portugal, Universidad Autónoma del Estado de México, 2005, ISSN 0718-0195, formato pdf, disponible en http://redalyc.uaemex.mx/pdf /820/82030204.pdf, p. 90, consultada el 24 de abril de 2012.

derechos y garantías establecidos a favor de las personas que pudieran verse perjudicadas por el tratamiento de datos a ellas referidos".[43]

En cuanto al término de protección de datos personales en su estricto sentido literal, para algunos estudiosos de la materia resulta no ser el más adecuado, por evocar erróneamente a la idea de la protección del dato y no de su titular. Es cierto, la expresión quizás no sea la más propicia, pero es necesario ir más allá de las simples palabras, para comprender que la protección de los meros datos no es el fin que se persigue con este derecho sino de los derechos de la persona a quien corresponden los mismos.

Un dato aislado sólo representa un número, un dato estadístico o un objeto, pero cuando se vincula con su titular adquiere un valor distinto que probablemente se relacionará con un derecho. Así el sujeto es quien le da el valor a la información y no el dato en sí mismo; por ello el individuo es quien puede ser vulnerable en caso del mal uso y destino ilícito de sus datos personales, y quien requerirá por lo tanto de una protección adecuada.

Es importante destacar que este derecho es únicamente para personas físicas que son identificadas, es decir, cuando se puede reconocer o señalar con certeza a una persona determinada como titular de los datos y, por lo tanto, del derecho pretendido; o que sean identificables, entendida como la posibilidad de ser determinado, directa o indirectamente, a través de la información con la que se cuente y sin requerir plazos o actividades desproporcionadas para lograrlo.

Lo anterior implica que este derecho esté limitado a la protección de personas físicas quedando excluidas las personas morales. El motivo de esta exclusión surge principalmente por la derivación de la protección de datos personales del derecho a la intimidad, el cual es inherente sólo a la naturaleza del ser humano.

La Segunda Sala en la tesis aislada 2a. XCIX/2008, con número de registro 169167, explica esta exclusión de la siguiente manera:

> "**TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. LOS ARTÍCULOS 3o., FRACCIÓN II, Y 18, FRACCIÓN II, DE LA LEY FEDERAL RELATIVA, NO VIOLAN LA GARANTÍA DE IGUALDAD, AL TUTELAR EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES SÓLO DE LAS PERSONAS FÍSICAS** … al tutelar sólo el derecho a la protección de datos personales de las personas físicas y no de las morales,

[43] PUENTE DE LA MORA, Ximena, "Protección de datos personales en posesión de los particulares en México: Avances y Desafíos", *Op. cit.,* p. 916.

> colectivas o jurídicas privadas, no violan la indicada garantía contenida en el artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, pues tal distinción se justifica porque el derecho a la protección de datos personales se refiere únicamente a las personas físicas por estar encausado al respeto de un derecho personalísimo, como es el de la intimidad, del cual derivó aquél … del cual únicamente goza el individuo, entendido como la persona humana".[44]

No obstante lo anterior, consideramos que dentro de la evolución de este derecho, en un futuro pueda ser viable el reconocimiento de la protección de información de personas morales, quienes también pueden verse vulnerados ante el uso y destino de sus datos que posean tanto entes públicos como privados. Es evidente que esta afectación no podrá ser en el mismo nivel ni con los mismos alcances que se logran con una persona física, pero igualmente pudiera haber una vulneración por el mal uso de la información, causando daños graves, como su extinción.

Este tema no es nuevo, incluso se ha discutido en foros internacionales como el de la OCDE, donde algunos países miembros han considerado que la protección requerida para los datos relativos a los individuos puede ser de carácter similar a la de las empresas mercantiles, las asociaciones y los grupos que puedan o no tener personalidad jurídica. Además para algunos países resulta difícil definir claramente la línea divisoria entre datos personales y datos no personales, como sucede con los propietarios de pequeñas empresas, en las que incluso se pueden manejar datos sensibles. Sin embargo, todavía no existe una aceptación mayoritaria en esta propuesta, por lo cual la OCDE ha decidido limitar la protección de datos sólo para individuos y dejar a los países miembros que decidan las políticas en relación a las empresas, grupos y entes similares.

El mayor problema al reconocer la protección de datos a personas jurídicas se daría en la manera de tratar a estas personas en el ejercicio del derecho, toda vez que no puede ser con base en la noción de intimidad como sucede con los individuos ni bajo la forma de un derecho humano; por otra parte, sus necesidades de protección serían distintas, así como las políticas a desarrollar para el caso en específico. No obstante ello, más adelante, como resultado del desarrollo y evolución de todo derecho podrían plantearse nuevos escenarios y ante ellos nuevamente esta

---

[44] Tesis aislada 2a. XCIX/2008, Novena Época, Instancia Segunda Sala, Semanario Judicial de la Federación y su Gaceta XXVIII, Julio de 2008, p. 549, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 169167.

propuesta que modificaría tal vez los esquemas establecidos o quizás el surgimiento de un nuevo derecho para personas jurídicas.

Por lo pronto y en el sistema jurídico mexicano, el derecho a la protección de datos personales es un derecho reconocido exclusivamente a favor de individuos, para la salvaguarda de su derecho a la autodeterminación informativa, mediante el establecimiento de prerrogativas, principios y procedimientos específicos que permiten el libre ejercicio de sus derechos de acceso, rectificación, cancelación y oposición, así como su protección por parte de la autoridad, en caso de ser vulnerados por los Responsables, Encargados o Terceros[45] en el tratamiento de sus datos, sean personas físicas o morales, públicas o privadas.

IV. Principios rectores del derecho a la protección de datos personales.

El derecho a la protección de datos personales se ha caracterizado por contar con principios que lo rigen de manera muy particular, los cuales se traducen en la mayoría de los casos en derechos y obligaciones para los Responsables, Encargados o Terceros involucrados directa o indirectamente, en el tratamiento de los datos personales. A nivel internacional se han establecido diversos principios considerados como estándares mínimos para los países que deciden reconocerlos, adoptarlos e incluso ampliarlos en sus legislaciones internas.

Los primeros principios que se establecieron en materia de protección de datos personales a nivel internacional, se encuentran en las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales[46], adoptadas como una recomendación de la OCDE, para establecer guías generales sobre la obtención y gestión de información personal. [47]

---

45 Para efectos del presente trabajo, la referencia de “Responsable” se entenderá como la persona física o moral que obtiene, hace uso y decide sobre el tratamiento de datos personales. “Encargado”, persona física o jurídica que sola o conjuntamente con otras realice el tratamiento de los datos personales por cuenta del Responsable. Y “Tercero”, persona física o moral, nacional o extranjera, distinta del titular o del Responsable de los datos.

46 De conformidad con las Directrices de la OCDE se entienden por flujos transfronterizos de datos personales, los desplazamientos de datos personales más allá de las fronteras nacionales.

47 Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, París, 2002, Resúmenes preparados por la Unidad de Derechos y Traducción de la Dirección de Relaciones Públicas y Comunicaciones de la OCDE, disponibles en http://www.oecd.org/dataoecd/16/51/15590267.pdf, consultada el 6 de abril de 2012.

Las referidas Directrices se encuentran vigentes a partir del 23 de septiembre de 1980 y establecen ocho principios básicos de aplicación nacional y cuatro de aplicación internacional, para ser considerados como estándares mínimos a seguir en la obtención, procesamiento y libre flujo transfronterizo de datos, tanto para el sector público como el privado, y que pueden suponer un peligro para la privacidad y las libertades individuales.

Consideramos relevante mencionar brevemente estos principios por dos motivos, en primer lugar porque México como miembro de la OCDE[48] ha reconocido y adoptado estos principios y, en segundo lugar, por ser este instrumento uno de los principales elementos que sirvieron de base para la elaboración de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), en la cual se acogieron los principios básicos de las Directrices, mediante el establecimiento en la ley de los principios rectores de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Los ocho principios básicos de aplicación nacional de las Directrices y que también relacionamos con los establecidos en la LFPDPPP, son los siguientes:

- Principio de limitación de recogida. Obtención de datos con medios legales y justos, con el conocimiento o consentimiento del sujeto implicado (Licitud, consentimiento y lealtad)
- Principio de calidad de los datos. Datos relevantes para el propósito de su uso y datos exactos, completos y actuales (Calidad y proporcionalidad).
- Principio de especificación del propósito. Se debe especificar el propósito a más tardar al momento de la obtención de los datos y su uso debe estar limitado al cumplimiento de los objetivos establecidos de origen (Información, consentimiento y finalidad).
- Principio de limitación de uso. No divulgar, poner a disposición o usar los datos personales para propósitos distintos, excepto si se tiene el consentimiento del sujeto implicado o por imposición legal o de las autoridades (Finalidad y consentimiento).
- Principio de salvaguardia de la seguridad. Emplear salvaguardias razonables de seguridad para proteger los datos personales contra riesgos de los mismos (Responsabilidad – Medidas de seguridad).
- Principio de transparencia. Debe existir una política general sobre transparencia de evolución, prácticas y políticas relativas a datos personales (Responsabilidad).
- Principio de participación individual. Todo individuo tendrá derecho a: la confirmación de la existencia de datos sobre su persona; le comuniquen

[48] México es miembro de la OCDE desde el 18 de mayo de 1994.

sus datos en un tiempo razonable, a un precio no excesivo, de forma razonable y de manera inteligible; le expliquen las razones por las que su petición ha sido denegada, así como para cuestionar tal denegación; expresar dudas sobre los datos relativos a su persona y si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan (Ejercicio de los derechos ARCO).

- Principio de responsabilidad. Todo controlador de datos debe ser responsable del cumplimiento de las medidas que hagan efectivos los principios antes señalados (Responsabilidad).

En cuanto a los principios básicos de aplicación internacional de las Directrices, como restricciones en el libre flujo y la legitimidad para los países miembros de la OCDE, se encuentran los siguientes:

- Considerar las implicaciones que el procesamiento nacional y la reexportación de datos personales puedan tener para otros países miembros.
- Seguir todos los pasos razonables y apropiados para asegurar que el flujo transfronterizo de datos personales, incluido el tránsito a través de un país miembro, se realice en forma ininterrumpida y segura.
- Abstenerse de restringir el intercambio transfronterizo de datos personales con otros países miembros, excepto cuando el país receptor todavía no observe de forma sustancial estas directrices o cuando la reexportación de tales datos burle la legislación nacional sobre privacidad.
- Evitar la elaboración de leyes, políticas y prácticas destinadas a proteger la privacidad y las libertades individuales que pudieran crear obstáculos al flujo transfronterizo de datos personales excediendo los requisitos para tal protección.

El 29 de octubre de 2004 el Foro de Cooperación Económica Asia-Pacífico (APEC)[49] emitió el Marco de Privacidad, el cual también sirvió de base para que en México, como miembro de dicho organismo internacional,[50] se llevaran las primeras reformas constitucionales en la materia, siendo igualmente importante mencionar sus nueve principios de privacidad de la información:

---

49 El texto original se encuentra disponible en http://www.nacpec.org/docs/APEC_Privacy_Framework.pdf y su traducción en español realizada en el 2005 por el Secretariado del APEC en *www.sellosdeconfianza.org.mx/capturas/lineamientos.doc, consultada el 15 de mayo de 2012.*

50 México se adhirió al APEC en 1993 con el objetivo de expandir y diversificar los vínculos económicos con Asia-Pacífico.

1. Prevención del daño, advertir el mal uso de la información personal, y por consiguiente, el daño de los individuos.
2. Aviso, para dar a conocer a los individuos que se está recopilando información personal; los propósitos; tipos de personas u organizaciones a las que se puede revelar la información; la identidad y ubicación del controlador y la elección de medios que ofrece para limitar el uso, revelación, acceso y corrección de la información.
3. Limitación de recolección, limitada a aquella información que sea relevante a los propósitos de la recolección. Además debe ser obtenida por medios legales y justos.
4. Usos de la información personal, sólo para cumplir con los propósitos de recolección y otros compatibles o relacionados.
5. Elección, proporcionar a los individuos mecanismos claros, prominentes, de fácil entendimiento, accesibles y asequibles para ejercitar su derecho.
6. Integridad de la información personal, la información debe ser exacta, completa y actualizada.
7. Medidas de seguridad, los controladores de la información deben proteger la información personal que guarden con medidas de seguridad apropiadas contra riesgos, sujetas a revisión periódica.
8. Acceso y corrección de información, no es absoluto pues será condicionada a los requerimientos de seguridad que impidan el acceso directo a la información y requerirán de pruebas suficientes de identidad previas al acceso.
9. Responsabilidad del controlador de la información para cumplir con las medidas de seguridad para el acceso y corrección de la información personal. En caso de transferencia deberá obtener el consentimiento del individuo.

Finalmente cabe mencionar que los principios que regulan la protección de datos personales en posesión de entes públicos de la Administración Pública Federal en México, se establecen en los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005 y son: licitud, calidad, acceso y corrección,[51] de información, seguridad, custodia y consentimiento para su transmisión.

[51] Los lineamientos señalan el acceso y corrección de datos como un mismo principio, sin embargo es importante aclarar dos cosas, primero que se trata de derechos y no de un principio y segundo que son dos derechos diferentes que se pueden ejercer por su titular de manera conjunta o independiente.

Aunque los principios pueden ser variados o denominados de distintas formas, lo importante es que cada vez más países reconozcan y apliquen un mínimo de ellos, para lograr a través de criterios homogéneos, una amplia protección de este derecho, especialmente cuando los datos personales sean transferidos a diversos lugares, distintos de aquél donde se encuentre su titular, y garantizar con ello su pleno ejercicio.

V. Modelos de protección de datos personales.

Los modelos de protección de datos personales son los esquemas a seguir para regular el derecho a la protección de datos personales, los cuales varían de acuerdo a los sistemas jurídicos y requerimientos de cada país. Algunos de los modelos regulatorios, como lo veremos más adelante, se van a identificar claramente con determinados países o regiones; sin embargo cada vez más se observa una tendencia a formar un híbrido de las diversas formas de protección establecidas en los modelos existentes, a fin de lograr un equilibrio entre las mismas y garantizar así la protección adecuada de este derecho. Los cuatro modelos principales son los siguientes:

1. Modelo general o de leyes integrales.

Este modelo se identifica por contar con una ley general que regula la protección de datos, tanto en poder de entes públicos como de privados, así como con una autoridad u organismo público autónomo encargado de vigilar el cumplimiento de la ley y, en su caso, sancionar su incumplimiento, pero especialmente fungir como autoridad garante del derecho a la protección de datos personales, reconocido a nivel constitucional como un derecho fundamental. También se le conoce como modelo de regulación y control por centrar la protección de datos en una reglamentación, estableciendo límites y restricciones, especialmente para los operadores de datos, en cuanto al tratamiento de los mismos. Este modelo fue adoptado primordialmente en los Estados miembros de la Unión Europea.

Una de las desventajas de este modelo es el riesgo de caer en la sobrerregulación y excesiva intervención de la autoridad y, en consecuencia, disuadir la participación activa de los operadores de datos, especialmente en la emisión de sus propias reglas y mecanismos de control, con las cuales se permita complementar o ampliar la protección de este derecho, en beneficio de sus titulares; asimismo los excesivos controles por parte de la autoridad pueden convertirse en obstáculos para el libre flujo de datos necesarios para el desarrollo comercial entre países.

2. Modelo sectorial

Se caracteriza por adoptar una variedad de mecanismos de protección a través de diversas reglas emitidas por sector o industria. Este modelo prevalece en los Estados Unidos de América.

Una de las desventajas de este modelo consiste en no contar oportunamente con nueva legislación o debidamente actualizada, que vaya acorde con los requerimientos exigidos por el desarrollo constante de nuevas tecnologías, en menoscabo de la protección eficaz de este derecho; lo anterior resulta de la complejidad para modificar no una, sino diversas leyes relativas a la materia, cuya observancia se encuentra a su vez, a cargo de diferentes autoridades.

Esto último es otra de las desventajas del modelo sectorial, la pluralidad de autoridades que existen en la protección de este derecho, las cuales sólo intervienen en lo relativo al sector que les corresponda, sin que necesariamente exista una coordinación entre las mismas para el establecimiento de criterios homogéneos en la protección eficaz y completa de este derecho.

3. Modelo de autorregulación

Del modelo anterior, se desprende el de autorregulación, el cual consiste en otorgar facultades normativas y de control a las entidades responsables del tratamiento de datos sin la intervención de la autoridad. En consecuencia, se propicia por sector o industria, la emisión de normatividad en esta materia y su instrumentación de manera independiente, a través de la elaboración de códigos de conducta o buenas prácticas profesionales, sellos de confianza, políticas o reglas de privacidad, estándares o modelos específicos, criterios y demás herramientas o mecanismos que fomenten la protección de este derecho y sus alternativas de solución o mejora ante las posibles problemáticas; sin embargo, al ser instrumentos voluntarios carecen de obligatoriedad y exigibilidad para su cumplimiento.

A diferencia del modelo sectorial, aquí no existe una autoridad gubernamental que vigile su cumplimiento, sino un responsable designado de manera interna por los operadores de datos, no siendo posible acreditar la plena observancia de la normatividad, su oportuna adecuación en caso de ser necesario, ni el cumplimiento de las metas propuestas y, en consecuencia, tampoco asegurar la protección real de este derecho.

Estados Unidos de América ha promovido mecanismos de autorregulación, especialmente en materia de comercio electrónico o *marketing* digital, y a pesar de no obtener hasta ahora resultados satisfactorios, la Comisión

Federal de Comercio de ese país confía en que la autorregulación sea la opción para proteger la privacidad de los consumidores en un mercado digital, donde se corre el riesgo del rastreo en línea, la determinación de perfiles y el uso de publicidad virtual debido a la segmentación conductual de consumidores.

Una variación de este modelo es el de Corregulación, el cual consiste igualmente en la emisión de normatividad por sector o industria, pero con la supervisión de una autoridad dotada con facultades para vigilar su cumplimiento. Este modelo fue acogido por Canadá y Australia.

En ambos modelos existe un nivel mínimo de protección de los datos personales establecido en la legislación correspondiente, sin embargo los demás estándares de protección se encuentran a cargo de los Responsables, los cuales variarán según se trate del sector o industria y, al igual que el modelo sectorial no existe homogeneidad de criterios ni certeza en la protección adecuada de este derecho.

4. Modelo de tecnologías de privacidad

Este modelo consiste en la protección de los datos personales por parte del propio titular del derecho, a través de los diversos programas, sistemas de privacidad y seguridad de las comunicaciones que actualmente la misma tecnología proporciona a los usuarios de las TIC´s, como lo es a través de contraseñas, el renvío con remitentes anónimos, uso de funciones de cifrado de la información, creación de certificados digitales y demás herramientas que permitan la confidencialidad de los datos a transferir y la seguridad de los usuarios.

Consideramos que este esquema no es en realidad un modelo de protección de datos, sino tan sólo el uso de diversos medios, con los cuales cuenta el propio titular para proteger y controlar sus datos, como medida de seguridad de su información personal para minimizar los riesgos de alteración o pérdida de la misma, robo de identidad, transmisiones o accesos no autorizados, y sin que ello implique precisamente el ejercicio de su derecho, como lo es para acceder, rectificar, cancelar u oponerse por el uso de sus datos ante quienes los ostenten. Es más bien parte de su derecho a la autodeterminación informativa, entendida como la facultad de toda persona para ejercer control sobre su información, a decidir de manera libre e informada sobre el uso de sus datos personales.

Por otra parte, en cuanto a las desventajas bajo este esquema, los niveles de protección serían desiguales, debido al interés particular que cada individuo tiene en proteger su vida privada y hacer públicos o no sus datos personales, pues lo que puede ser de interés para unos, quizás no lo sea para otros. El consentimiento es el

principal recurso con el que cuenta el individuo para ejercer su derecho; sin embargo, el problema surgirá cuando aún sin otorgarlo, sus datos personales sean manipulados por otros, especialmente para fines ilícitos, con lo cual la persona quedaría totalmente desprotegida en el ejercicio de su derecho.

En México se ha adoptado un modelo de protección híbrido, al considerar el establecimiento de una autoridad encargada de promover y vigilar la debida observancia de la ley de la materia, pero a la vez con la posibilidad de permitir la corregulación por parte de los Responsables, a fin de ampliar y asegurar la protección de este derecho. Asimismo también cuenta con características de un modelo sectorial, al existir leyes en materia específicas y con autoridades particulares, que regulan y protegen en el ámbito de sus facultades, este derecho.

La diversidad de modelos indica que el derecho a la protección de datos personales no es comprendido aún de la misma forma, y por tanto, la regulación para su protección puede llegar a ser tan desigual e incluso contraria, que no se logre la concreción de un modelo de integración para su control y establecimiento de niveles mínimos de protección, aplicables no sólo en ciertos Estados o regiones, sino en todo el mundo. No obstante ello, tampoco se debe caer en los extremos de formar sistemas tan rígidos que incluso limiten el derecho de las personas o tan flexibles que lo dejen totalmente desprotegidos. Por lo cual consideramos relevante, lograr el equilibrio y armonía entre los distintos esquemas de protección existentes en el mundo a favor de los derechos de los titulares.

VI. El contexto internacional del derecho a la protección de datos personales.

En la actualidad la información ha adquirido un valor tan relevante que un Estado moderno no podría funcionar sin ella, debido al estrecho vínculo que existe entre la información y el desarrollo económico y social de los países. De esta manera, el flujo de información se manifiesta en todo el mundo como algo inevitable y necesario, así como la principal actividad a desarrollar en la sociedad actual.

Al respecto, James R. Beniger en su obra *Information Society and Global Science* señala: "… la información es el mayor sector independiente de la economía global. Distintamente de otras sociedades que conocemos, en los casi 50,000 años de la historia humana, ahora hay una docena de naciones, o tal vez más, que dependen de los bienes de la información y de los servicios, antes que de la cacería, la recolección, la agricultura o de la minería, o de manufacturas y comercio ajenos a

la información. Se podría sostener que el proceso de la materia y de la energía ha comenzado a ser desplazado por el proceso de la información".[52]

En este sentido, al otorgarle un valor económico y social a la información, y en cierto modo, poder para quien la posee, se reconoce también la existencia de un mercado de la misma, en el cual fluyen datos de diversos tipos, entre personas o entes, públicos o privados, interesados en su recolección, registro, organización, conservación, modificación, consulta, utilización, transmisión, difusión, o cualquier otro uso que se le pueda dar, para cualquier fin, incluyendo fines ilícitos.

Aunado a lo anterior, con el desarrollo de la tecnología y comunicaciones, se ha logrado acceder de manera rápida y sencilla a todo tipo información, incluso de cualquier parte del mundo, lo que ha dado lugar a una serie de conductas y supuestos no previstos por la ley. En consecuencia, el Derecho como instrumento regulador de las relaciones humanas, tiende a estudiar y regular esta nueva realidad social, para evitar la afectación de derechos, especialmente los fundamentales, en el presente caso, por el inadecuado manejo y control de los datos personales de los individuos, con el cual se vulnera su intimidad y vida privada.

De esta manera, una de las preocupaciones de la comunidad internacional ha sido el regular esta situación ante el uso inadecuado de las nuevas tecnologías informáticas y la forma cómo afectan a los derechos fundamentales, el desarrollo económico de los países e incluso la seguridad nacional e internacional, a fin de lograr una coexistencia entre ellos de manera armónica y equilibrada.

Al efecto, se han llevado a cabo trabajos para analizar esta problemática, los cuales han concluido con la emisión de diversos instrumentos internacionales relativos al tema. En este contexto internacional podemos distinguir dos escenarios: 1. Internacional, con los organismos internacionales; y 2. Regional, con Europa y América como las principales regiones donde se ha desarrollado este derecho.

1. Internacional

Diversos instrumentos internacionales emitidos por la Organización de las Naciones Unidas (ONU) y por la OCDE, refieren en principio, al derecho a la vida privada y a la intimidad, para posteriormente llegar a señalarlo, en sus documentos más recientes, como el derecho a la protección de datos personales. En razón que estos instrumentos serán revisados en el Capítulo Segundo, sólo serán mencionados a fin de ilustrar la evolución de ese derecho en el contexto internacional:

---

[52] LEÓN, Leysser L., *El problema jurídico de la manipulación de información personal*, Colección Derecho PUCP, número 2, Ed. Palestra, Perú, 2007, pp. 54 y 55.

- Declaración Universal de Derechos Humanos adoptada y proclamada por resolución de la Asamblea General de la ONU del 10 de diciembre de 1948, (vida privada).
- Pacto Internacional de Derechos Civiles y Políticos, aprobado por la Asamblea General de la ONU en su resolución del 16 de diciembre de 1966, (vida privada).
- Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad, adoptado por la Asamblea General de la ONU, a través de la Resolución 3384 (XXX) del 10 de noviembre de 1975 (vida privada, protección de la persona humana y su integridad física e intelectual).
- Declaración Universal sobre el genoma humano y los derechos humanos del 11 de noviembre de 1997 (protección de la confidencialidad de los datos genéticos vinculada con el principio general del respeto de la vida privada).
- Principios rectores para la reglamentación de los ficheros computarizados de datos personales, aprobados por la Resolución 45/95 de la Asamblea General de la ONU, el 14 de diciembre de 1990 (ficheros que contienen datos personales).
- Directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, recomendación del Consejo de la OCDE del 23 de septiembre de 1980 (Libre flujo transfronterizo de datos).
- Declaración sobre flujo de datos transfronterizos de la OCDE, adoptada el 11 de abril de 1985 (Flujo de datos personales).
- Directrices sobre política criptográfica, establecidas por recomendación de la OCDE, el 27 de marzo de 1997 (Protección de datos personales).

2. Regional

En lo relativo al ámbito regional encontramos los diversos instrumentos emitidos por el Consejo de Europa, la Unión Europea y la Organización de los Estados Americanos (OEA), entre los que se encuentran los siguientes:

A. Europa

Los avances más significativos en el estudio y regulación del derecho a la protección de datos personales se encuentran en Europa, especialmente los realizados por la Unión Europea, donde como se vio antes, prevalece un modelo general a través de un sistema más estricto en cuanto al control y regulación de los datos personales, tanto en términos generales como también en aquellos sectores con los cuales puede estar involucrado, como lo son las comunicaciones

electrónicas, la genética, la seguridad y el comercio electrónico, por lo que en nuestra opinión tiene también cierta tendencia a aplicar un modelo sectorial.

En materia de protección de datos personales, en la Unión Europea existe una tendencia a lograr una protección uniforme, mediante el establecimiento de normas comunes a las cuales se deben adecuar la regulación interna de cada Estado Miembro, lo cual se refleja en el adecuado funcionamiento de un mercado unificado. Dentro de la normativa que se ha emitido en la Unión Europea con respecto a la protección de datos personales se encuentra la siguiente:

- Convenio del Consejo de Europa para la protección de los derechos humanos y libertades fundamentales del 4 de noviembre de 1950, en su artículo 8.1 se establece el derecho de toda persona para ser respetada en su vida privada y familiar, de su domicilio y de su correspondencia.
- Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del 28 de enero de 1981 y modificado el 15 de junio de 1999, en el cual se establece en su artículo 3 numeral 1, el compromiso de las partes para aplicar el Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado. En el Protocolo adicional del Convenio N° 108 del 8 de noviembre de 2001, se regula de manera específica lo relativo a las autoridades de control y a la transferencia de datos personales a destinatarios no sometidos a la competencia de las partes del Convenio.
- Convenio de Asturias de Bioética del Consejo de Europa, convenio para la protección de los Derechos Humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina. Convenio sobre los Derechos Humanos y la Biomedicina del 4 de abril de 1997, en su artículo 10 señala que toda persona tendrá derecho a que se respete su vida privada cuando se trate de informaciones relativas a su salud, así como para conocer toda la información obtenida de ella o, en su caso, respetar su voluntad para no ser informada.
- Carta de los Derechos Fundamentales de la Unión Europea del 7 de diciembre de 2000, en cuyo artículo 8 se regula expresamente y de manera completa, la protección de datos de carácter personal, al establecer que toda persona tiene derecho a la misma. Menciona que estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afecta o en virtud de otro fundamento legítimo previsto por la ley. Asimismo establece el derecho para acceder y rectificar los datos personales, y señala que el respeto

de estas normas quedará sujeto al control de una autoridad independiente. Con ello la Comunidad Europea reconoce el carácter de fundamental a este derecho.

- Reglamento N° 2725/2000 del Consejo de Europa del 11 de diciembre de 2000 relativo a la creación del sistema "Eurodac" para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín[53], para determinar la identidad del solicitante de asilo y de las personas interceptadas en ocasión de cruce irregular de las fronteras exteriores de la Comunidad. Al respecto los Estados miembros deben establecer un sistema de sanciones por el uso contrario de los datos registrados en la base de datos central a la finalidad de "Eurodac". El 28 de febrero de 2002 el Consejo de Europa emitió el Reglamento N° 407/2002 por el que se establecen determinadas normas de desarrollo del Reglamento antes citado, específicamente para la comunicación y transmisión de los datos relativos a impresiones dactilares.
- Reglamento N° 45/2001 del Parlamento Europeo y del Consejo de la Unión Europea del 18 de diciembre de 2000, publicado en el Diario Oficial de las Comunidades Europeas el 12 de enero de 2001, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Por decisión del Consejo de Europa del 13 de septiembre de 2004 se emitieron las normas de desarrollo del referido Reglamento, mediante las cuales se regulan, entre otros puntos, las funciones y obligaciones de los Responsables de la protección y tratamiento de datos, asimismo se establece el procedimiento para el ejercicio de los derechos de los interesados, consistentes en el acceso, rectificación, bloqueo y supresión de sus datos; y el procedimiento de investigación.
- Convenio del Consejo de Europa sobre la Ciberdelincuencia del 23 de noviembre de 2001, en el cual se regulan delitos como: contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos relacionados con el contenido; y relacionados con infracciones de propiedad intelectual y derechos afines.

[53] Convenio de Dublín relativo a la determinación del Estado responsable del examen de las solicitudes de asilo presentadas en los Estados miembros de las Comunidades Europeas, del 15 de junio de 1990.

El Parlamento Europeo y Consejo de Europa han emitido las siguientes once directivas en diversos sectores relacionados con esta materia, a fin de hacerlas congruentes con la legislación comunitaria referente al tratamiento de datos personales.

- Directiva 95/46/CE del 24 de octubre de 1995, para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Directiva 97/66/CE del 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Directiva 1999/93/CE del 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.
- Directiva 2000/31/CE del 8 de junio de 2000, relacionada a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
- Directiva 2002/19/CE del 7 de marzo de 2002, concerniente al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión (Directiva acceso).
- Directiva 2002/20/Ce del 7 de marzo de 2002, referente a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización).
- Directiva 2002/21/CE del 7 de marzo de 2002, hacia un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco).
- Directiva 2002/22/CE del 7 de marzo de 2002, del servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal). Modificada por la Directiva 2009/136/CE del 25 de noviembre de 2009.
- Directiva 2002/58/CE del 12 de julio de 2002, referente al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Modificada por las Directivas 2006/24/CE del 15 de marzo de 2006 y 2009/136/CE del 25 de noviembre de 2009.
- Directiva 2004/82/CE del 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas.
- Directiva 2006/24/CE del 15 de marzo de 2006 para la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

B. América

Por lo que respecta a los instrumentos emitidos por los organismos internacionales de América, al igual que los internacionales han protegido el derecho a la vida privada y más recientemente han reconocido el derecho a la protección de datos personales, de la siguiente manera:

- Declaración Americana de los derechos y deberes del hombre, adoptada en la IX Conferencia Internacional Americana, celebrada en Bogotá, Colombia, el 2 de mayo de 1948, protege la vida privada.
- Convención Americana sobre Derechos Humanos, también denominada "Pacto de San José Costa Rica" del 22 de noviembre de 1969, también protege la vida privada.
- Relatoría para la libertad de expresión de la Organización de los Estados Americanos, en octubre de 2000 el relator elaboró la Declaración de Principios sobre Libertad de Expresión, en la que se estableció como principio 3, que toda persona tiene derecho a acceder a la información sobre sí misma o a sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registro públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla.

Es de advertirse que en América no todos los países cuentan con legislación o mecanismos de protección de datos personales, por tal motivo es importante señalar los que actualmente si los tienen, a efecto de conocer en términos generales el modelo bajo el cual se encuentra regulado este derecho.

Estados Unidos de América

En materia de protección de datos personales, en Estados Unidos de América se desarrolló el modelo de la privacidad conocido como el *privacy right*, el cual de acuerdo a Carlos G. Gregorio "descansa sobre la fuerza de la ley y en la capacidad de la judicatura para limitar las acciones de un Estado que pudiera resultar invasor y totalitario".[54]

Como se mencionó anteriormente, en dicho país rige el modelo de autorregulación, basado en la idea que el derecho a la privacidad sólo se ejerce contra la intromisión del Estado en los asuntos privados, motivo por el cual su regulación se limita a los datos personales que se encuentran en posesión del gobierno federal. Sin embargo, a partir del 11 de septiembre de 2001, la privacidad

[54] GREGORIO, Carlos G., *Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina, Op. cit.*, p. 306.

del individuo se puso en contraste con la seguridad nacional e internacional, al surgir un mayor manejo y control de todo tipo de información por parte de los gobiernos, en el presente caso el estadounidense, en detrimento incluso de derechos fundamentales tales como la dignidad humana, la vida privada, el honor, la imagen, la libertad de expresión y la protección de datos personales, lo cual se ve reflejado con la emisión de la denominada *USA Patriot Act*, aprobada el 26 de octubre de 2001 y la cual fue motivo de enmienda de otras disposiciones.

Al respecto Francisco Sierra Caballero alude a una nueva cultura mediática que ha propiciado diversos cambios en la doctrina de la seguridad, hacia una guerra digital o ciberguerra, en la cual la información es considerada como "… el centro de toda política bélica, el núcleo de la filosofía y acción militar en la era de las redes comunicacionales, sencillamente porque la revolución informativa introduce cambios significativos no sólo en la infraestructura y el entorno tecnológico, sino también en las condiciones culturales, económicas, políticas y societarias que ponen en el punto de mira servicios básicos para la vida moderna".[55]

A partir de este nuevo escenario geopolítico y la necesidad de un nuevo enfoque operativo, continúa diciendo Sierra Caballero, los Estados Unidos de América modifican sustancialmente su cultura militar y el marco estratégico de la política de expansión de sus intereses económicos, basado en una política informativa de control y manejo de los medios de información y difusión de políticas de propaganda.

En ese sentido, dicha política aplicada, no sólo en ese país sino en otros tantos, vulnera la intimidad y la vida privada de las personas, al suprimir toda barrera formal entre lo público y lo privado, así como provocar una violencia simbólica o psicológica, a base de temor, desestabilidad y miedo en la sociedad a través de las redes de telecomunicación, las cuales pueden convertirse en un problema de seguridad, por su enorme potencial para poner en peligro la paz y el orden mundial.

Lo anterior, dificulta en gran medida el equilibrio y convivencia armónica entre la seguridad y la aplicación de regulación, mecanismos e instituciones adecuadas para garantizar no sólo el derecho a la protección de datos personales, sino también otros derechos fundamentales, siendo este uno de los principales

---

55 SIERRA CABALLERO, Francisco, "La guerra en la era de la información: propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación"*, Sphera Pública*, revista de Ciencias Sociales y de la Comunicación, publicación anual, número 003, Universidad Católica San Antonio de Murcia, España, 2003, ISSN: 1180-9210, Red de revistas científicas de América Latina y El Caribe, España y Portugal, formato pdf, disponible en http://redalyc.uaemex.mx/pdf/297/29700314.pdf, consultada el 27 de abril de 2012.

desafíos a enfrentar actualmente por la comunidad internacional, mediante el desarrollo de estrategias adecuadas que mejor ponderen esta disyuntiva.

Ahora bien, en cuanto a la normativa que regula esta materia en los Estados Unidos de América, se encuentra la *Freedom of Information Act*, mejor conocida por sus siglas en inglés como FOIA, promulgada en 1966 y con vigencia a partir del 5 de julio de 1967. Esta ley regula la revelación de información y el derecho de acceso, rectificación o complementación de los registros informáticos públicos federales.

Otra importante disposición es la *Privacy Act* del 31 de diciembre de 1974, una de las primeras leyes emitidas para la protección del derecho a la privacidad y por el uso inadecuado de información, sin embargo como se señaló antes, sus alcances son limitados al aplicar sólo en la protección de datos personales en posesión del gobierno federal, no encontrándose comprendidos los de gobiernos estatales ni del sector privado.

Carlos G. Gregorio señala que a parte de la protección que se brinda a través de la *Privacy Act*, el modelo americano o sectorial, cuenta a nivel federal con leyes que regulan la privacidad en sectores determinados como son:

> "1. Informes crediticios (*Fair Credit Reportin Act* de 1970, *Public Law* 91-508, modificada varias veces entre 1996 y 2001).
> 2. Archivos de televisión por cable (*Cable Communications Policy Act*, 47 USC 521-611, 1994).
> 3. Comunicaciones electrónicas (*Electronic Communications Privacy Act*, de 1986, 18 USC 2510-2520, 1994 & Supp. 1997).
> 4. Escucha de comunicaciones en una investigación criminal (*Omnibus Safe Streets and Crime Control Act* de 1967, 18 USC 2510-2520, 1968).
> 5. Registros de alquiler de videos (*Video Privacy Protection Act*, 18 USC 2710, 1994).
> 6. Registros telefónicos (*Telephone Consumer Privacy Act*, 47 USC 227, 1994).
> 7. Registros bancarios (*Bank Secrecy Act*, 31 USC 5313, 1994).
> 8. Archivos de permisos de conducir (*Drivers Privacy Protection Act*, 18 USC 2721-25 1994).

9. Control parental de los niños en sus actividades en Internet (*Children´s Online Privacy Protection Act*, 15 USCA 6501-6506, 1998)". [56]

Canadá

Canadá ha tratado de buscar un punto medio entre los modelos antes vistos, a fin de no caer en una sobrerregulación por parte de la autoridad ni en una libre autorregulación por parte de los entes privados. En este sentido Cristos Velasco San Martín señala que a través de este sistema Canadá combina "legislación y políticas de autorregulación eficientes que respondan específicamente a las necesidades individuales de sus nacionales, buscando con ello proteger los derechos de los ciudadanos y consumidores, sin menoscabar los intereses patrimoniales de las medianas y grandes empresas, estableciendo reglas claras y organismos gubernamentales ad-hoc eficientes para su debida vigilancia".[57]

La ley de la materia que rige en Canadá a nivel federal es *The Personal Information Protection and Electronic Documents Act*, conocida como PIPED *Act*, emitida el 13 de abril de 2000, la cual entró en vigor en tres fases, la primera el 1 de enero de 2001 para aplicar a organismos federales, especialmente para datos utilizados en actividades comerciales y los proporcionados por sus empleados; la segunda fase dio inicio el 1 de enero de 2002, para regular la información sobre salud; y finalmente la tercera fase entró en vigor el 1 de enero de 2004 para regular organizaciones bajo la jurisdicción de cada una de las provincias canadienses, excepto en aquéllas donde ya contaran con una legislación similar a la PIPED *Act*.

América Latina

Los modelos regulatorios de protección de datos personales en América Latina son variados, unos países han preferido el modelo europeo y otros el americano, pero algunos con un estilo muy particular, han incluido a estos modelos la figura del *habeas data*.

El *habeas data* en el derecho latinoamericano es generalmente entendido y aplicado más como una garantía procedimental que tiene toda persona para proteger su derecho a acceder y conocer sus datos personales en bancos o

---

[56] GREGORIO, Carlos G., *Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina, Op. cit.,* pp. 306 y 307.

[57] VELASCO SAN MARTÍN, Cristos, *Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México,* Instituto Nacional de Estadística, Geografía e Información, Boletín de Política Informática número 1, 2003, formato pdf, disponible en http://www.inegi.gob.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf, p. 5, consultada el 28 de abril de 2012.

registros, lo cual lo limita a ser ejecutado sólo después que se traten los datos personales, y no para situaciones previas a su vulneración o riesgo, como lo es para establecer acciones preventivas y de control en la protección del derecho.

Víctor Bazán refiere que "… en el ámbito iberoamericano se aprecia una significativa confusión conceptual sobre la naturaleza de la institución del habeas data (se utilice o no literalmente esa denominación), pues mientras en algunas Constituciones se la regula como una suerte de derecho autónomo (*aspecto sustantivo*) consistente en la denominada "autodeterminación informativa" o la protección frente a los posibles excesos del poder informático en bancos de datos, archivos o registros; en otros casos, se lo define como una garantía o proceso constitucional especial (*aspecto instrumental*) destinado a la protección y defensa de los derechos específicos que en las respectivas normas se señalan".[58]

De esta manera, el referido autor señala como países donde aplican el *habeas data* en sus constituciones, en su aspecto instrumental, a Brasil, Paraguay, Perú, Argentina y Bolivia; y en su aspecto sustancial, a Guatemala, Colombia, Nicaragua, Ecuador y Venezuela. Por su parte, Sergio A. Moncayo González alude a Chile, Costa Rica, El Salvador, Nicaragua y Uruguay, como "… los países de América Latina que actualmente no cuentan con una garantía primaria sobre protección de datos personales (es decir, en la constitucional)…"[59] Y a Bolivia, Ecuador, El Salvador y Venezuela, como países que no cuentan con legislación específica.

A continuación se hará una breve reseña de la normativa que regula la protección de datos personales en América Latina, tanto en sus constituciones como en su legislación específica o sectorial, con la cual podremos observar como el derecho a la protección de datos es un derecho reciente que aún se encuentran en proceso de desarrollo en esta región, el cual al no ser comprendido y regulado de la misma forma, dista aún mucho por lograr una normativa común en la materia como sucede en Europa.

---

58 BAZÁN, Víctor, "El habeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado", *Op. cit.,* p. 96.

59 MONCAYO GONZÁLEZ, Sergio A., *Protección de Datos Personales en México. Garantías Primarias y Secundarias / Avances Constitucionales,* ponencia presentada en el Seminario HabeasData2010, celebrado en Buenos Aires, Argentina el 26 y 27 de noviembre de 2010, formato pdf, disponible en http://www.habeasdata2010.com.ar/pdf/ moncayo2.pdf, p. 11, consultada el 29 de abril de 2012.

Argentina considera la acción del *habeas data* en su Constitución,[60] al establecer en su artículo 43, tercer párrafo, que toda persona puede interponer acción expedita y rápida de amparo, para conocer sus datos y su finalidad, que consten en registros o bancos de datos públicos o privados, así como exigir su supresión, rectificación, confidencialidad o actualización. Además cuenta con la Ley Nº 25.326 de Protección de los Datos Personales, sancionada el 4 de octubre de 2000[61] y modificada por la Ley 26.343 sancionada el 12 de diciembre de 2007, para incorporar el artículo 47, relativo al banco de datos de servicios de información crediticia. Esta Ley fue reglamentada por el Decreto Nº 1558/2001 del 29 de noviembre de 2001.[62]

La protección que brinda esta acción en Argentina es integral por abarcar no sólo la información que consta en archivos, registros o bancos de datos públicos sino también privados para proteger el derecho al honor y a la intimidad de las personas, así como el acceso a su información, y por otorgar una legitimación activa al afectado y también a sus tutores o curadores y sucesores, sean en línea directa o colateral hasta el segundo grado, por sí o por medio de apoderado, ya sea porque le afecta un derecho subjetivo o porque tenga un interés legítimo. Asimismo, en el proceso puede intervenir en forma coadyuvante el Defensor del Pueblo.

Bolivia cuenta con la acción de protección de privacidad, en los artículos 130.I y 131.I de su Constitución,[63] para toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar y obtener la eliminación o rectificación de los datos registrados en archivos o bancos de datos públicos o privados, o afecten su derecho fundamental a la intimidad y privacidad personal y familiar, a su imagen, honra y reputación. La acción de protección de privacidad se tramitará conforme al procedimiento establecido para la acción de Amparo Constitucional. En cuanto a las leyes sectoriales en la materia cuenta con la Ley de Telecomunicaciones.

---

60 La parte relativa al artículo 43 de la Constitución de Argentina se encuentra disponible en http://www3.hcdn.gov.ar/folio-cgi-bin/om_isapi.dll?clientID=1185577405&advquery=habeas&hitsperheading=on&infobase=constra.nfo&record={7FF67B87}&softpage=Doc_Frame_Pg42&x=15&y=19&zz=, consultada el 29 de abril de 2012.

61 El texto completo de la Ley de Protección de los Datos Personales de Argentina se encuentra disponible en http://www1.hcdn.gov.ar/BO/boletin00/2000-11/BO02-11-00leg.pdf, consultada el 29 de abril de 2012.

62 El texto completo del Decreto 1558 se encuentra disponible en http://www1.hcdn.gov.ar/BO/boletin01/2001-12/BO03-12-01leg.pdf, consultada el 29 de abril de 2012.

63 El texto completo de la Nueva Constitución del Estado de Bolivia se encuentra disponible en http://www.diputados.bo/images/docs/cpe.pdf, consultada el 29 de abril de 2012.

La Constitución de Brasil fue la primera en incluir el término de *habeas data*, donde es entendido como una acción constitucional o amparo específico para conocer y rectificar los datos que consten en registros o bancos de entidades gubernamentales o de carácter público. Luiz Augusto Paranhos Sampaio, señala: "Sintéticamente, tal remedio jurídico-procesal se destina a garantizar al solicitante el ejercicio de su pretensión, bajo tres aspectos: derecho de acceso a los registros; derecho de rectificación; y derecho de complementación de los registros".[64]

Moncayo González señala que en el artículo 5° fracción LXXII de la Constitución de Brasil, se mencionan los dos supuestos cuando se concede el *habeas data*: "a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiere hacerlo por procedimiento secreto, judicial o administrativo".[65] Además de su norma fundamental existe la Ley Nº 9.507 del 12 de noviembre de 1997, la cual regula el acceso a las informaciones y los aspectos procesales del *habeas data*. También cuenta con algunas normas sectoriales como en materia de consumidores, intercepciones telefónicas y secreto bancario.

En Chile no cuentan con la protección expresa de este derecho en su Constitución[66] sino de derechos personales relacionados con el mismo, como son la vida privada y la honra (Artículo 19, numeral 4°). Asimismo cuentan con la Ley 19628 sobre protección de la vida privada del 28 de agosto de 1999[67], modificada por la Ley 19812 del 13 de junio de 2002, la cual regula el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o particulares. Por otra parte cuenta con algunas normas sectoriales en materia laboral, económica, financiera y de salud.

---

64 BAZÁN, Víctor, "El habeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado", *Op. cit.,* p. 97.

65 MONCAYO GONZÁLEZ, Sergio A., *Protección de Datos Personales en México. Garantías Primarias y Secundarias / Avances Constitucionales, Op. cit.,* p. 7. El texto original de la Constitución de Brasil, en idioma portugués, se encuentra disponible en http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm

66 El texto completo de la Constitución de Chile se encuentra disponible en http://www.leychile.cl/Navegar?idNorma=242302, consultada el 29 de abril de 2012.

67 El texto completo de la Ley N° 19628 de Chile se encuentra disponible en http://www.leychile.cl/Navegar?idNorma=141599&buscar=19628, consultada el 29 de abril de 2012.

En Colombia se regula este derecho en el artículo 15° de su Constitución Política,[68] sin señalar expresamente algún término para identificarlo, al establecer que toda persona tiene derecho a conocer, actualizar y rectificar la información recogida sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. No cuenta con una norma general, pero si con varias sectoriales relativas a la recolección de datos personales como en materia de comercio electrónico y firmas digitales, tributaria, de telecomunicaciones y bancaria.

En Costa Rica sólo se protege el derecho a la intimidad, a la libertad y al secreto de las comunicaciones en el artículo 24 de su Constitución,[69] sin embargo cuenta con la Ley Nº 8968 de Protección de la Persona frente al Tratamiento de sus Datos Personales del 7 de julio de 2011, vigente a partir del 5 de septiembre de 2011,[70] cuyo ámbito de aplicación son los datos personales que consten en bases de datos automatizados o manuales, de organismos públicos o privados. Su objetivo es garantizar el derecho a la autodeterminación informativa de cualquier persona en relación con su vida o actividad privada y demás derechos de la personalidad. A través de dicha ley se crea la Agencia de Protección de Datos de los Habitantes (Prodhab), órgano de desconcentración máxima adscrito al Ministerio de Justicia y Paz, ante quien se pueden presentar denuncia por la violación del derecho o solicitar se inicie el procedimiento sancionatorio.

En Ecuador se reconoce en el artículo 66 numeral 19 de su Constitución[71] dentro de los derechos de libertad, el derecho de toda persona a la protección de datos de carácter personal, el cual incluye el acceso y la decisión sobre información y datos de ese carácter, así como su correspondiente protección. Para la recolección, archivo, procesamiento, distribución o difusión de los mismos, se requerirá de la autorización del titular o el mandato de la ley. En el artículo 92 de su norma fundamental se regula la acción del *habeas data* entendido como el derecho que tiene toda persona para conocer de la existencia y acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma o

---

68 El texto completo de la Constitución de Colombia se encuentra disponible en http://wsp.presidencia.gov.co/Normativa/Documents/ConstitucionPoliticaColombia_20100810.pdf, consultada el 29 de abril de 2012.

69 El texto completo de la Constitución de Costa Rica se encuentra disponible en http://www.pgr.go.cr/SCIJ/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=871&nValor3=74424&strTipM=TC, consultada el 29 de abril de 2012.

70 El texto completo de la Ley N° 8968 de Costa Rica se encuentra disponible en http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC, consultada el 29 de abril de 2012.

71 El texto completo de la Constitución de Ecuador se encuentra disponible en http://www.asambleanacional.gov.ec/documentos/Constitucion-2008.pdf, consultada el 29 de abril de 2012.

sus bienes, consten en entidades públicas o privadas, así como conocer su finalidad, origen, destino y tiempo de vigencia. Por otra parte, tiene derecho a la actualización de sus datos, a su rectificación, eliminación o anulación.

Asimismo cuenta con la Ley de Control Constitucional promulgada el 2 de julio de 1997,[72] la cual regula el recurso del *habeas data* del artículo 34 al 45, al que tienen acceso no sólo las personas naturales sino también las jurídicas. El 18 de marzo de 2010 fue presentada a la Asamblea Nacional de la República del Ecuador, un proyecto de Ley de Protección a la Intimidad y a los Datos Personales, mismo que se encuentra en su segundo debate.[73]

En el artículo 2 párrafo segundo de la Constitución de El Salvador[74] se garantizan los derechos de la personalidad del honor, la intimidad personal y familiar y la propia imagen, y establece la indemnización para los daños de carácter moral. Por su parte, en los artículos del 19 al 22 del Reglamento General de la Ley Penitenciaria del 14 de noviembre de 2000,[75] se regula la privacidad de datos del interno y sus datos personales sensibles o especialmente protegidos, a los cuales se les brindará la garantía de confidencialidad.

En el artículo 31 de la Constitución de Guatemala[76] se regula el derecho de toda persona a conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y su finalidad, así como la corrección, rectificación y actualización de sus datos. La Ley de Acceso a la Información Pública, emitida por Decreto N° 57-2008, publicado el 23 de octubre de 2008,[77] garantiza a toda persona el derecho a solicitar y tener acceso a la información pública en posesión de autoridades, así como garantizar a toda persona individual el derecho a conocer y

---

72 El texto completo de la Ley de Control Constitucional de Ecuador se encuentra disponible en http://docs.ecuador.justia.com/nacionales/leyes/ley-de-control-constitucional.pdf, consultada el 29 de abril de 2012.

73 Dato obtenido en la página de la Asamblea Nacional de la República del Ecuador, disponible en http://asambleanacional.gob.ec/tramite-de-las-leyes.html, consultada el 29 de abril de 2012.

74 El texto completo de la Constitución de El Salvador se encuentra disponible en http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/constitucion-de-la-republica, consultada el 29 de abril de 2012.

75 El texto completo del Reglamento General de la Ley Penitenciaria se encuentra disponible en *http://www.ute.gob.sv/cpp/index.php?option=com_docman&Itemid=102&task=doc_download&gid=53*, consultada el 29 de abril de 2012.

76 El texto completo de la Constitución de Guatemala se encuentra disponible en http://www.congreso.gob.gt/manager/images/1188FE6B-B453-3B8C-0D00-549DA12F72CB.pdf, consultada el 29 de abril de 2012.

77 El texto completo de la Ley de Acceso a la Información Pública de Guatemala se encuentra disponible en http://200.12.63.122/archivos/decretos/2008/gtdcx57-0008.pdf, consultada el 29 de abril de 2012.

proteger sus datos personales que consten en archivos estatales, y actualizar los mismos. También contempla el *habeas data* como garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos o registro públicos y su finalidad, así como solicitar la protección, corrección, rectificación o actualización de sus datos.

Nicaragua establece en su artículo 26 numeral 4 de su Constitución[78] que toda persona tiene derecho a conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho a saber por qué y con qué finalidad la tienen. El 21 de marzo de 2012 fue aprobada por la Asamblea Nacional de la República de Nicaragua y publicada el día 29 de ese mismo mes y año, la Ley N° 787 de Protección de Datos Personales[79], la cual tiene por objeto la protección de la persona natural o jurídica frente al tratamiento, automatizado o no, de sus datos personales en ficheros de datos públicos y privados, a efecto de garantizar el derecho a la privacidad personal y familiar y el derecho a la autodeterminación informativa. Se crea la Dirección de Protección de Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público, para controlar, supervisar y proteger el tratamiento de los datos personales contenidos en ficheros de datos de naturaleza pública y privada, a través de la acción de protección de datos personales, la cual es de naturaleza administrativa; para recurrir la resolución de la referida Dirección, se podrá interponer el Recurso de Amparo, mientras no se desarrolle su protección por la vía jurisdiccional, es decir hasta que se reforme la Ley de Amparo para establecer el recurso del *habeas data*.

La Constitución de Panamá en su artículo 44[80] establece que toda persona puede promover acción de *habeas data* con miras a garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales o particulares, precisando que en este último caso sólo será para empresas que prestan un servicio al público o se dediquen a suministrar información; asimismo mediante esta acción podrán solicitar la corrección, actualización, rectificación, supresión o se mantenga la confidencialidad de la información o datos de carácter personal.

---

78 El texto completo de la Constitución de Nicaragua se encuentra disponible en http://www.bcn.gob.ni/banco/legislacion/constitucion.pdf, consultada el 29 de abril de 2012.

79 El texto completo de la Ley de Protección de Datos Personales de Nicaragua se encuentra disponible en http://www.asamblea.gob.ni/trabajo-legislativo/agenda-legislativa/ultimas-iniciativas-presentadas/, consultada el 29 de abril de 2012.

80 El texto completo de la Constitución de Panamá se encuentra disponible en http://www.asamblea.gob.pa/asamblea/constitucion/index.htm, consultada el 29 de abril de 2012.

En cuanto a la ley de la materia en Panamá existe la Ley Nº 6 del 22 de enero de 2002[81], mediante la cual se dictan normas para la transparencia en la gestión pública y establece la acción de *habeas data*. En su artículo 3 establece que toda persona tiene derecho a obtener su información personal contenida en archivos, registros o expedientes que mantengan las instituciones del Estado, también puede corregir o eliminar información; ante la negativa del acceso se puede promover la acción de *habeas data*, el cual es considerado como un procedimiento sumario, pero que para su sustanciación aplican las normas del Amparo de Garantías Constitucionales.

En Paraguay en el artículo 135 de su Constitución[82] establece el *habeas data* para proteger el acceso y conocimiento de la información y datos que obran en registros oficiales o privados de carácter público, así como para conocer el uso y finalidad, siendo posible solicitar ante el magistrado competente la actualización, rectificación o destrucción de datos erróneos o que afecten ilegítimamente sus derechos. Por su parte, la Ley N° 1682 del 16 de enero de 2001, modificada por la Ley 1969 del 2 de septiembre de 2002,[83] reglamenta la información de carácter privado y establece que toda persona podrá acceder a la información y a los datos que sobre sí misma, sobre su cónyuge o sobre personas bajo su tutela o curatela, o sobre sus bienes, obren en registros oficiales o privados de carácter público o en entidades que suministren información sobre solvencia económica y situación patrimonial; en caso de no ser atendidas las solicitudes se acudirá ante un juez, quien ordenará el cumplimiento de la solicitud y en su caso aplicará las multas correspondientes.

En Perú la acción de *habeas data*, es considerada por su Constitución en el artículo 200[84], como una garantía constitucional que procede contra el hecho u omisión de cualquier autoridad, funcionario o persona, que vulnere o amenaza el Artículo 2°, incisos 5) y 6) de la Constitución, relativos a los derechos de acceso a la

---

81 El texto completo de la Ley Nº 6 se encuentra disponible en http://www.presidencia.gob.pa/ley_n6_2002.pdf, consultada el 29 de abril de 2012.

82 El texto completo de la Constitución de Paraguay se encuentra disponible en http://pdba.georgetown.edu/constitutions/paraguay/para1992.html, consultada el 29 de abril de 2012.

83 El texto completo de las leyes números 1682 y 1969 están disponibles en la página de la red iberoamericana de datos personales en http://www.redipd.org/documentacion/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf y http://www.redipd.org/documentacion/legislacion/common/legislacion/paraguay/Ley_1969_de_2002.pdf, consultadas el 29 de abril de 2012.

84 El texto de este artículo de la Constitución de Perú se encuentra disponible en http://www2.congreso.gob.pe/sicr/relatagenda/constitucion.nsf/constitucion/439F1D9B3CEB1E805256729006BC62C?opendocument, consultada el 29 de abril de 2012.

información y servicios informáticos o computarizados. También cuentan con una diversidad de leyes relativas al tema como la Ley N° 27.489 que rige las centrales privadas de información de riesgos y de protección al titular de la información y la Ley N° 28.237 que aprueba el Código Procesal Constitucional el cual regula el *habeas data* como proceso constitucional. Dentro de sus normas sectoriales se encuentran las materias de firmas y certificados digitales, delitos informáticos y medios electrónicos de comunicación.

En Uruguay existe la Ley N° 17.838 de protección de datos personales para ser utilizados en informes comerciales y acción de *habeas data*, publicada el 1 de octubre de 2004,[85] la cual tiene por objeto regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos públicos o privados, limitándolos a que sean sólo aquellos destinados a brindar informes objetivos de carácter comercial, de lo contrario se requerirá del consentimiento expreso del titular. El órgano de control es el Ministerio de Economía y Finanzas, pero la acción del *habeas data* se ejercerá ante el juez competente, por el titular de los datos o sus representantes, ya sean tutores o curadores, en caso de personas fallecidas, por sus sucesores universales, en línea directa o colateral hasta el segundo grado, por sí o por apoderado; y en caso de personas jurídicas por sus representantes legales o apoderados.

En Venezuela se regula en el artículo 28 de su Constitución[86] el derecho de toda persona para acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados; conocer su uso y finalidad; así como solicitar al tribunal competente la actualización, rectificación o destrucción de los mismos, si fuesen erróneos o afectasen ilegítimamente sus derechos.

Ante la diversidad de regulación, instituciones, niveles de seguridad y mecanismos que aplican en cada uno de los países, es indispensable el establecimiento de principios fundamentales comunes que sirvan de base para garantizar, de manera armonizada la protección de datos personales en todo el mundo, en beneficio de sus titulares.

---

85 El texto completo de la Ley Nº 17.838 de Uruguay se encuentra disponible en http://www0.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17838&Anchor=, consultada el 29 de abril de 2012.

86 El texto completo de la Constitución de Venezuela se encuentra disponible en la página de la Red Iberoamericana de Datos Personales en http://pdba.georgetown.edu/constituti ons/venezuela/ven1999.html, consultada el 29 de abril de 2012.

VII. El contexto nacional del derecho a la protección de datos personales.

Mientras a nivel internacional, en países como los europeos y Estados Unidos de América, el derecho a la protección de datos personales se encontraba en pleno desarrollo y reconocimiento en sus legislaciones desde el siglo XIX, en México no se encontraba reconocido en su Constitución y menos aún existía una ley que regulara la materia, sino que diversas disposiciones, de manera aislada y respecto de una materia en específico, regulaban la protección de datos personales.

Por lo que no fue sino hasta con la emisión de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental del 11 de junio de 2002, que se reguló por primera vez en México la protección de datos personales en posesión de entes públicos federales.

Posteriormente, con la reforma al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, se establecieron ocho bases y principios que debían regir para el ejercicio del derecho de acceso a la información en la Federación, Estados y el Distrito Federal en el ámbito de sus competencias, dentro de los que se encuentran la protección de la información que se refiere a la vida privada y a los datos personales.

Con dicha reforma se reguló por vez primera, a nivel constitucional, la protección de este derecho en posesión de todo ente público, sin embargo aún quedaba fuera de regulación el sector privado. Ante esta ausencia y parcial cumplimiento de los compromisos que nuestro país adquiría en esta materia a nivel internacional, el 30 de abril de 2009 se publicó en el Diario Oficial de la Federación, el Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, por el que se otorgó al Congreso la facultad de legislar en materia de protección de datos personales en posesión de particulares, y se estableció en su artículo Segundo Transitorio, un plazo de doce meses para expedir la ley de la materia.

En el transcurso del proceso legislativo realizado en la Cámara de Diputados para la elaboración de la ley que regularía la protección de datos en posesión de particulares, fue reformado el 1 de junio de 2009, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos para reconocer expresamente en su párrafo segundo, la protección de datos personales como el derecho que tiene todo individuo en el acceso, rectificación, cancelación y oposición de sus datos personales (derechos conocidos con el acrónimo ARCO), para dotar al titular del poder de disposición y control sobre sus datos personales.

Después el 5 de julio de 2010 fue publicada en el Diario Oficial de la Federación (DOF), la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y el 21 de diciembre de 2011 su correspondiente Reglamento. A partir del 6 de enero de 2012 los titulares pueden ejercer sus derechos ARCO ante los Responsables, así como solicitar, en caso de ser vulnerados, el inicio del procedimiento de protección de derechos o de verificación, ante el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), autoridad garante de este derecho. Así con la entrada en vigor de la LFPDPPP, se establecen los principios y mecanismos de protección del derecho a la autodeterminación informativa de los individuos, necesarios para hacer efectiva la garantía establecida en el segundo párrafo del artículo 16 constitucional, la cual hasta antes de la expedición de la ley de la materia, sólo era posible aplicarla para información en poder de entes públicos.

De esta manera, con la integración en el sistema jurídico mexicano del derecho a la protección de datos personales, surge un nuevo desafío para el Derecho, a fin de evaluar si las normas vigentes en la materia, son eficaces en la protección de este derecho, bajo los esquemas y mecanismos en ellas previstos, en congruencia con lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos y los Tratados Internacionales emitidos en esta materia, aprobados por el Senado.

En consecuencia, ante el reconocimiento constitucional del derecho a la protección de datos personales y la emisión de una ley específica en la materia, se hace necesario el análisis de su marco jurídico y las instituciones que lo operan, trabajo que se llevará a cabo en los siguientes capítulos, a fin de determinar si se cumple o no con el objetivo de tutelar y hacer efectivo este derecho fundamental, así como si es acorde o no con la realidad actual de México y el contexto internacional, a efecto de ofrecer un nivel máximo de garantía a los individuos en el ejercicio de este derecho.

CAPÍTULO SEGUNDO
ORDENAMIENTOS MEXICANOS QUE REGULAN EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

I. Constitución Política de los Estados Unidos Mexicanos.

El derecho a la protección de datos personales en posesión de entes públicos fue regulado por vez primera en México a nivel federal, en el Capítulo IV de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en el DOF el 11 de junio de 2002; sin embargo fue hasta la reforma del artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, publicada en el DOF el 20 de julio de 2007[87], que los derechos a la protección, al acceso y a la rectificación de datos personales fueron reconocidos expresamente a nivel constitucional, cuando se establecieron como unos de los principios que rigen el ejercicio del derecho de acceso a la información, en el párrafo segundo, fracciones II y III, de las siete que fueron adicionadas al referido artículo, como se observa a continuación:

> "Artículo 6º. …
> 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. …
> 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.
> IV al VII. …"

De lo antes citado observamos en la fracción II del artículo 6o. constitucional que será en las leyes respectivas donde se regulará la protección a la información relativa a la vida privada y a los datos personales, así como sus excepciones, sin precisar si dicha normativa será la misma que regule el derecho de acceso a la información o una distinta y particular en materia de protección de datos

[87] El Decreto de reforma al artículo 6o. constitucional fue resultado de dos iniciativas presentadas el 16 de noviembre y 19 de diciembre, ambas de 2006 en la Cámara de Diputados. Los Congresos de los 17 Estados de la República Mexicana que emitieron su voto aprobatorio al Decreto fueron: Aguascalientes, Chiapas, Chihuahua, Coahuila, Colima, Guanajuato, Estado de México, Morelos, Nayarit, Nuevo León, Puebla, Querétaro, San Luis Potosí, Sinaloa, Sonora, Tamaulipas y Zacatecas.

personales. Asimismo, observamos en la fracción III del referido precepto constitucional, únicamente la mención de los derechos de acceso y rectificación, sin embargo ello no es impedimento para el ejercicio de los otros derechos de rectificación y oposición, cuando así lo contemplen las leyes de la materia, en razón de ser estándares básicos que pueden ser ampliados, especialmente cuando son en beneficio de los individuos.

Si bien el objetivo principal de esta reforma fue homogenizar en los niveles, federal, estatal y municipal, los criterios aplicables al derecho de acceso a la información, a través del desarrollo de principios y bases mínimas y universales para construir de manera consistente, coherente y no contradictoria este derecho en México; también se observa, con lo señalado en las fracciones antes citadas, la preocupación de los legisladores por garantizar constitucionalmente, el derecho a la protección de datos personales en posesión de entes públicos, sobretodo porque se trata de la principal excepción al principio de publicidad que tanto caracteriza al derecho de acceso a la información.

El documento donde se expresa con mayor claridad los motivos que se tuvieron para incluir en la entonces propuesta de iniciativa, el derecho a la protección de datos personales, es el dictamen emitido el 24 de abril de 2007, por las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, Segunda,[88] de la Cámara de Senadores, en el cual se expusieron dentro de sus considerandos los siguientes objetivos esenciales:

> "… el decreto que propone la Colegisladora tiene los siguientes objetivos esenciales:
> 1. al 6. …
> 7. Establecer que la única gran excepción a la publicidad la constituye el respeto a la vida privada de las personas. Los datos que se refieren a la intimidad de los mexicanos, es la única causal fundamental, permanente y no sujeta a plazo, de reserva de la información que posee el Estado.

[88] El artículo 89 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos establece: "La Comisión de Estudios Legislativos conjuntamente con las otras comisiones ordinarias que correspondan, hará el análisis de las iniciativas de leyes o decretos y concurrirá a la formulación de los dictámenes respectivos. Dicha Comisión se podrá dividir en las secciones o ramas que se estime conveniente", por esta razón y debido principalmente a la cantidad de proyectos de iniciativa de ley o decretos que se presentan a la Cámara de Senadores, esta Comisión se encuentra dividida en tres Comisiones: 1) de Estudios Legislativos; 2) de Estudios Legislativos Primera; y 3) de Estudios Legislativos Segunda. Cada comisión está compuesta por un Presidente y dos Secretarios.

8. **Propiciar la expedición de una legislación en materia de protección de datos personales** que precise los límites entre la información pública y la información que se refiera a las personas físicas, identificadas o identificables, relativa a sus características físicas, morales, emocionales, a su vida afectiva y familiar, creencias o convicciones, estado de salud, preferencias sexuales u otras análogas que atañan a su intimidad.
9. Definir con claridad que éste es un derecho que se dirime con criterios objetivos (la naturaleza de la información) y no mediante consideraciones subjetivas (quién pide la información, para qué solicita la información, etcétera). En esa medida la identificación, la acreditación de interés jurídico, la firma o huella del solicitante resultan totalmente irrelevantes y por ello, prescindible para el ejercicio del derecho de acceso a la información y al acceso de los datos personales.
10. al 17. …"
[Énfasis añadido]

De lo anterior, se desprenden los siguientes comentarios:

- Los derechos a la vida privada y a la intimidad son las principales excepciones al principio de publicidad del derecho de acceso a la información; por lo tanto, los datos que contienen este tipo de información, no podrán ser divulgados, a menos que se cuente con el consentimiento expreso de su titular.
- Es tal la importancia que tiene para el legislador, el garantizar los derechos a la vida privada y a la intimidad sobre cualquier interés público, que no es posible establecer plazos de reserva respecto de ellos, motivo por el cual deberán mantenerse en todo momento con el carácter de confidencial.
- El derecho de acceso a la información es distinto al derecho a la protección de datos personales, pero al estar vinculados, cuando la información está en manos de entes públicos, resulta necesario establecer claramente los alcances y límites de cada uno de ellos en disposiciones específicas y distintas, a fin de evitar su confusión al momento de ejercerlos, o la vulneración de uno en detrimento del otro; porque no toda la información que posean los entes públicos deberá ser considerada bajo el mismo carácter de pública y, por ende, ser divulgada a quien la solicite, pues la información relativa a datos personales quedará exceptuada de ello.

- La finalidad que tienen los órganos del Estado para recolectar y tratar datos personales debe responder a un interés público, el cual se traduzca en el otorgamiento de más y mejores servicios públicos; el establecimiento de políticas en beneficio de la sociedad; en el control de diversos actos jurídicos para brindar mayor certeza a quienes los realizan; así como para llevar a cabo estudios estadísticos que incidan en una mejor planeación.
- El legislador expresa claramente la necesidad de contar con una ley que regule de manera específica el derecho a la protección de datos personales, así esta reforma constitucional sería la base y posible detonador para la emisión de una ley relativa a la materia. Sin embargo, hasta la fecha esto no se ha logrado, pues existe no una, sino varias disposiciones dispersas en todos los niveles de gobierno que regulan la protección de datos personales en posesión de entes públicos, como se verá más adelante, lo cual favorece la presencia de diversos criterios que obstaculizan su ejercicio.
- Finalmente, se señala que la identificación, la acreditación de interés jurídico, la firma o la huella del solicitante son prescindibles para el acceso de los datos personales; sin embargo, es importante aclarar que ello sólo aplica para el titular de los datos personales, y aún en ese caso, consideramos que debe identificarse, no sólo por razones de seguridad, sino también porque sería contrario a la naturaleza del derecho a la protección de datos personales como derecho personalísimo. Tal contradicción se observaría cuando la ley establece, por un lado, que la información concerniente a datos personales se instituye como la única gran excepción a la publicidad, pero por el otro, permite que cualquier persona consiga acceder a datos personales, aun y cuando no se traten de los propios. Esta es una de las interpretaciones que puede darse a la lectura de este objetivo, lo cual es un claro ejemplo de los posibles riesgos que se corre al no tener definidos los límites y alcances de cada uno de estos derechos.

Una de las posibles causas que dan lugar a la confusión de los derechos de acceso a la información y a la protección de datos personales es regularlos en una misma norma sin definir claramente sus diferencias. En este sentido, la autora argentina Basterra señala, al referirse a la confusión conceptual de la institución del *habeas data* o derecho a la protección de datos en el derecho iberoamericano, lo siguiente: “… se advierte en muchos países que, ya sea en la norma constitucional,

como en la propia ley, lo regulan en forma conjunta con el derecho de acceso a la información pública, confundiéndolos, en algunos casos."[89]

Si bien con esta reforma se dio un enorme avance en el surgimiento y desarrollo del derecho a la protección de datos personales en México, aún era necesaria su regulación a través de las normas secundarias para su operación y, aunque a nivel federal ya se encontraba previsto en la LFTAIPG desde el 2002, así como en otras disposiciones, se requería aún su homologación en todos los niveles de gobierno. Por otro lado, era evidente el gran vacío que constitucional y legalmente todavía existía en la protección de datos personales en posesión de entes privados. Es por ello que Sergio Moncayo manifiesta: "Un derecho plasmado en la Constitución, que no disponga de la debida reglamentación, es en la realidad un derecho inválido ..."[90]

Después de casi dos años de haberse emitido la reforma del artículo 6o. constitucional y conscientes de la ausencia de regulación del derecho a la protección de datos en posesión de entes privados, el 30 de abril de 2009 se publicó en el DOF, el Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos,[91] en la cual se otorga al Congreso de la Unión, la facultad de legislar en materia de protección de datos personales en posesión de particulares.

Dentro del proyecto de iniciativa del referido Decreto,[92] se destaca la importancia de contar con una legislación que regule la protección de datos personales en todo el territorio nacional, no sólo por tratarse de un derecho fundamental reconocido en diversos instrumentos internacionales, sino también por

---

89 BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados Derecho Constitucional Provincial Iberoamérica y México*, *Op. cit.*, pp. 195 y 196.

90 MONCAYO GONZÁLEZ, Sergio A., *Protección de Datos Personales en México. Garantías Primarias y Secundarias / Avances Constitucionales, Op. cit.,* pp. 2 y 3.

91 El proyecto que fue presentado a la Cámara de Senadores establecía la adición de la fracción XXIX-Ñ al artículo 73 constitucional, sin embargo al ser aprobada por las Comisiones Unidas de Puntos Constitucionales, de Estudios Legislativos y de Estudios Legislativos, Segunda, de esa Cámara, la Minuta del Proyecto de Decreto por el que se adiciona un párrafo noveno al artículo 4° y se reforma la fracción XXV y adiciona también una fracción XXIX-Ñ al artículo 73 de la Constitución Política, en materia de cultura y derechos de autor; se propuso para no duplicar, cambiar la fracción a la XXIX-O, la cual fue finalmente aprobada.

92 El 27 de marzo de 2007 fue presentada para su revisión en la Cámara de Diputados, la iniciativa de reforma al artículo 73 constitucional y el 25 de septiembre de 2007 en la Cámara de Senadores. Los Congresos de los Estados que emitieron su voto aprobatorio al Decreto fueron: Aguascalientes, Chiapas, Chihuahua, Colima, Durango, Guanajuato, Michoacán, Morelos, Nayarit, Nuevo León, Oaxaca, Puebla, Sinaloa, Tabasco, Tamaulipas, Tlaxcala, Veracruz, Yucatán y Zacatecas.

incidir directamente en el crecimiento económico de un país, tal y como se estableció en las Directrices de la OCDE y el Marco de Privacidad del APEC, organismos internacionales de los que México forma parte. Al respecto, destaca como principal beneficio de esta reforma, la ampliación del derecho a la protección de datos personales en poder de entes privados, así como favorecer el comercio interestatal e internacional.

En dicha iniciativa también se enfatiza la finalidad que tiene para los entes privados el recolectar y tratar los datos personales, la cual responde a un acentuado interés comercial, consistente en la venta de bienes y la prestación de servicios, así como los fines publicitarios. Asimismo, con dicha iniciativa se da cumplimiento a los compromisos internacionales que México tiene en materia de comercio, especialmente los relativos al flujo transfronterizo de datos.

Por su parte, dentro del dictamen emitido por la Cámara de Diputados, se estableció la necesidad de construir un derecho que pudiera ser ejercido en todo el territorio nacional bajo principios uniformes, con lo cual se lograra su efectiva tutela. Asimismo hacen referencia a la recolección de datos personales por parte del Estado, al mencionar que éste actúa constreñido a leyes y diversos ordenamientos sobre la materia, así como bajo fines específicos que son bien conocidos por la sociedad, lo cual no sucede para el caso de entes privados.

Dentro de la Cámara de Senadores la revisión al proyecto se enfoca principalmente en la justificación para legislar esta materia por parte del Congreso de la Unión, para ello argumenta por un lado, el federalismo que rige en México, y por el otro a que el derecho a la protección de datos personales está ligado a dos factores: el desarrollo tecnológico y el comercio, es decir a la materia mercantil y a la de telecomunicaciones, lo cual exige que la legislación que regule este derecho sea federal, para lograr su homogeneidad y el tratamiento uniforme de los datos personales por parte de los particulares.

Cabe destacar que en el dictamen de la Cámara de Senadores aluden a la importancia de respetar la potestad legislativa de las entidades federativas, en relación con los datos personales en poder de entes públicos estatales y municipales, no sólo por la autonomía de la que gozan las legislaturas locales para legislar este derecho, dentro del ámbito de sus competencias, sino también debido a que el Estado no tiene atribuciones para recabar información de particulares con fines de comercio.

En consecuencia, se deja fuera de esta reforma, la protección de datos personales en posesión de entes públicos debido a la autonomía de la que gozan las entidades federativas para legislar este derecho, ello de conformidad con lo

dispuesto por el artículo 124 constitucional, el cual establece que: “Las facultades que no están expresamente concedidas por esta Constitución a los funcionarios federales, se entienden reservadas a los Estados”. Al respecto el artículo 73 constitucional enlista las facultades reservadas al Congreso de la Unión, dentro de las cuales no se contempla la relativa a la protección de datos personales en posesión de entes públicos, por tanto su regulación se reserva a las entidades federativas. Asimismo, el artículo 6o. constitucional establece la facultad de los Estados, para proteger la información relativa a los datos personales, en el ejercicio del derecho de acceso a la información, en los términos y excepciones que fijen sus leyes y dentro del ámbito de sus respectivas competencias.

De acuerdo con lo expuesto en el dictamen emitido por el Senado de la República, otro motivo para excluir de esta reforma a la protección de datos personales en poder de entes públicos, es la finalidad para recolectar y tratar dichos datos, que en el caso de la Federación, Estados y municipios es exclusivamente con fines públicos y no comerciales, materia ésta última que justifica realmente su regulación a nivel federal.

Con lo anterior, observamos que la razón por la cual se decidió regular de manera distinta la protección de datos personales en poder de entes públicos y privados, como si fueran dos derechos distintos, obedeció primordialmente a un aspecto meramente comercial y para favorecer el libre flujo de datos transfronterizos interestatal e internacional. No obstante ello, resaltamos la importancia de tratar este derecho bajo principios y mecanismos básicos, independientemente de quien posea los datos personales, a fin de lograr la adecuada protección de este derecho reconocido como fundamental, y con ello garantizar al individuo el ejercicio pleno de sus libertades fundamentales, lo cual debe ser en definitiva, el principal objetivo de su regulación.

En el artículo Segundo Transitorio del citado decreto, se instruyó al Congreso de la Unión a expedir la ley de la materia en un plazo no mayor de doce meses, contados a partir de la entrada en vigor del decreto, es decir del 1 de mayo de 2009. En cumplimiento de esta disposición transitoria se emitiría más tarde la LFPDPPP, publicada en el DOF el 5 de julio de 2010.

Posteriormente, y como resultado de los trabajos legislativos realizados en esta materia, el 1 de junio de 2009 fue publicado en el DOF el Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos,[93] auténtico sustento

[93] El proyecto de iniciativa que fue presentado a la Cámara de Senadores el 25 de noviembre de 2008 y el 4 de diciembre de 2008 en la Cámara de Diputados, tuvo su

constitucional del derecho a la protección de datos personales, reconocido como derecho fundamental en México, al establecer:

> "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".

En el dictamen de la Cámara de Senadores emitido el 4 de diciembre de 2008, relativo a la iniciativa del proyecto de este decreto, se señala que el objeto de la reforma es desarrollar en el máximo nivel de normatividad, el derecho a la protección de datos personales en poder de cualquier entidad o persona, pública o privada, para asegurar que su aplicación se dé en todos los niveles y sectores; lo cual demuestra a diferencia de las anteriores reformas constitucionales, la intención del legislador para garantizar este derecho de manera integral, así como para analizar con mayor abundamiento la indudable esencia del mismo, es decir el individuo como titular de los datos personales, independientemente de quienes poseen los datos personales o los datos mismos.

Con la incorporación de este nuevo derecho fundamental en la Carta Magna, se reconoce al individuo el poder de disponer y controlar sus datos personales frente a los demás, sin embargo como todo derecho, éste no puede ser absoluto, y por lo tanto tampoco ser superior a los intereses sociales o públicos, motivo por el cual es indispensable establecer sus límites en la ley de la materia, mismos que son enunciados en el propio texto constitucional en términos generales y explicados en el dictamen antes citado de la siguiente manera:

- "Seguridad nacional.- toda vez que es indispensable mantener la integridad, estabilidad y permanencia del Estado mexicano.
- Disposición de orden público.- ya que el orden público tiene un sentido de equidad que rebasa los intereses particulares,

---

antecedente en una iniciativa presentada por el Senador Antonio García Torres, el 5 de abril de 2006, sin embargo fue nuevamente redactada para hacerla más concisa y ordenada. Las Declaratorias del Decreto emitidas por las Cámaras respectivas, obtuvieron los votos aprobatorios de los Congresos de los Estados de: Aguascalientes, Baja California, Coahuila, Colima, Chiapas, Chihuahua, Durango, Guanajuato, Michoacán, Morelos, Nuevo León, Oaxaca, Sinaloa, Tabasco, Tamaulipas, Tlaxcala, Yucatán y Zacatecas.

privados, individuales, porque en realidad el orden público representa el núcleo íntegro de la sociedad.

- Seguridad pública.- por ser una función a cargo de la Federación, las entidades federativas y los municipios, que comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas.
- Salud pública.- en virtud de que ésta también es responsabilidad del Estado, a quien corresponde controlar o erradicar enfermedades, así como prevenir los riesgos que afectan a la salud del conjunto de la población y promocionar hábitos de vida saludables".[94]

Al respecto, cabe mencionar que la LFPDPPP, emitida un año después de esta reforma constitucional, no establece expresamente los supuestos de excepción a los principios que rigen el tratamiento de datos. En los artículos 4 de la LFPDPP y 88 de su Reglamento, denominado "Restricciones al ejercicio de los derechos", se señalan sin mayor abundamiento, las mismas excepciones establecidas en términos generales en la propia Constitución, y sólo en el Reglamento se agrega que las restricciones serán en los casos y con los alcances previstos en las leyes aplicables en la materia o mediante resolución de la autoridad competente.

Dichas excepciones se analizarán en el Capítulo siguiente, por lo que en este apartado sólo queremos hacer evidente el incumplimiento del texto constitucional para señalar de manera clara y concisa las excepciones en la ley de la materia, así como su desacato a dicho precepto constitucional, al establecerlas en instrumentos que no corresponden al rango legislativo, como lo son los reglamentos y las resoluciones. Ante la imprecisión y falta de certeza en la ley de la materia, se deberá acudir a las leyes que regulan cada una de las materias que son objeto de excepción al derecho a la protección de datos personales.

En ese sentido, será necesaria la revisión del ordenamiento legal aplicable en cada supuesto de excepción, tal y como se señala en el dictamen emitido por la Cámara de Diputados el 11 de diciembre de 2008 para presentar este proyecto de reforma constitucional, donde se estableció que previo a instaurar límites al derecho de protección de datos personales frente a otros, deben ser valoradas las circunstancias particulares que prevalezcan en determinada situación.

---

[94] Dictamen del 4 de diciembre de 2008, emitido por las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, para presentar en la Cámara de Senadores el proyecto de decreto que adiciona un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum_crono.htm, p. 5, consultada el 2 de mayo de 2012.

El dictamen arriba citado aclara que las excepciones sólo aplican cuando, por la trascendencia de los casos, este derecho se encuentre en contraposición con otros derechos y amerite una ponderación de la autoridad, teniendo presente el bien común. Asimismo señala que en la ley de la materia será donde se desarrollen dichas situaciones de excepción, así como se establezcan las modalidades del tratamiento y la manera de acreditar la necesidad de conocer dicha información, por lo que no es suficiente el simple señalamiento en la ley, de la excepción a este derecho, sino es necesario contemplar las peculiaridades para su tratamiento.

Por otra parte, si bien es cierto que desde los trabajos de revisión de la Cámara de Senadores para adicionar una fracción al artículo 73 constitucional, se estableció la importancia de respetar la autonomía de los estados y municipios para regular en materia de protección de datos personales en poder de entes públicos, debido a la finalidad de interés social que tienen los órganos estatales para recopilar información personal, también lo es que con la reforma al artículo 16 constitucional se reconoció un derecho integral y uniforme, sin distinción de los sujetos que tratan los datos personales, lo cual amerita una protección de esa misma naturaleza y conforme a las bases mínimas establecidas en dicho precepto constitucional.

Sin embargo, de la revisión al marco jurídico en materia de protección de datos personales aplicable en el sistema jurídico mexicano, se observa que dicha materia se encuentra dividida y no se cumple de manera plena, con lo ordenado en el artículo 16 constitucional. Porque por un lado, existen diversas disposiciones a nivel federal y estatal en materia de acceso a la información, dentro de las cuales se regula como uno de sus apartados, la protección de datos personales en posesión de entes públicos, en congruencia con la fracción II del artículo 6o. constitucional que establece los principios y bases para la protección del derecho de acceso a la información. Y por otro, se encuentra la LFPDPPP, que fue emitida en cumplimiento al Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos y con la cual se garantiza la protección de estos datos en poder del sector privado.

De esta forma, al existir diversos ordenamientos legales, y con ello principios, procedimientos, mecanismos e instituciones federales y estatales que tutelan el derecho a la protección de datos personales en posesión de entes públicos, se puede caer en el riesgo de no lograr la armonización en la normatividad y en los procedimientos aplicables, con su consecuente incompatibilidad o establecimiento de obstáculos en las medidas de protección, dando lugar a una consecuencia aún mayor, como es el no garantizar de manera adecuada este derecho, conforme se establece en el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos y los instrumentos internacionales que México ha suscrito y aprobado en esta materia, los cuales

también forman parte del sistema jurídico mexicano y, por lo tanto, serán objeto de estudio en el siguiente tema de este Capítulo Segundo.

II. Tratados internacionales en materia de protección de datos personales, aprobados por el Senado de la República.

La Convención de Viena sobre el Derecho de los Tratados del 23 de mayo de 1969 establece en su artículo 2, numeral 1, inciso a), lo siguiente:

> "1.- Para los efectos de la presente Convención.
> a) se entiende por "tratado" un acuerdo internacional celebrado por escrito entre Estados y regido por el derecho internacional, ya conste en un instrumento único o en dos o más instrumentos conexos y cualquiera que sea su denominación particular; …"

Por su parte, la Convención de Viena sobre el Derecho de los Tratados entre Estados y Organizaciones Internacionales o entre Organizaciones Internacionales del 21 de marzo de 1986,[95] considerada como complementaria de la arriba citada, contempla como sujetos de Derecho Internacional Público, además de los Estados, a los organismos internacionales, por lo cual pueden celebrar tratados y, por lo tanto, adquirir derechos y obligaciones.

A fin de contemplar la definición de la primera Convención de Viena en esta materia y el reconocimiento de otros sujetos de Derecho Internacional Público, la Ley sobre la Celebración de Tratados, en su artículo 2o., fracción I, brinda la siguiente definición de tratado:

> "**Artículo 2o.-** Para los efectos de la presente Ley se entenderá por:
> **I.- "Tratado":** el convenio regido por el derecho internacional público, celebrado por escrito entre el Gobierno de los Estados Unidos Mexicanos y uno o varios sujetos de Derecho Internacional Público, ya sea que para su aplicación requiera o no la celebración de acuerdos en materias específicas, cualquiera que sea su denominación, mediante el cual los Estados Unidos Mexicanos asumen compromisos.
> De conformidad con la fracción I del artículo 76 de la Constitución Política de los Estados Unidos Mexicanos, los tratados deberán ser aprobados por el Senado y serán Ley Suprema de toda la

[95] Esta Convención aún no entra en vigor general. El Senado de la República la aprobó el 11 de diciembre de 1987 y el Decreto de promulgación se publicó en el DOF el 28 de abril de 1988.

Unión cuando estén de acuerdo con la misma, en los términos del artículo 133 de la propia Constitución."

En ese sentido, independientemente de su denominación, ya sea como tratados, convenciones, declaraciones, acuerdos o protocolos, a través de estos instrumentos, los sujetos de Derecho Internacional Público adquieren compromisos u obligaciones.

Al respecto, el artículo 133 de la Constitución Política de los Estados Unidos Mexicanos establece, en su parte relativa: "… todos los Tratados que estén de acuerdo con la misma, celebrados y que se celebren por el Presidente de la República, con aprobación del Senado, serán la Ley Suprema de toda la Unión…", de lo cual resulta que una vez satisfechos dichos requisitos de fondo y forma,[96] se constituirán como parte integrante del derecho positivo mexicano, y por tanto, serán obligatorios para los Estados Unidos Mexicanos.

En relación con los tratados internacionales concernientes a los derechos humanos, la tesis número XI.1o.A.T.45 K emitida en julio de 2007 por el Primer Tribunal Colegiado en Materias Administrativa y de Trabajo del Décimo Primer Circuito alude lo siguiente: "Los tratados o convenciones suscritos por el Estado mexicano relativos a derechos humanos, deben ubicarse a nivel de la Constitución Política de los Estados Unidos Mexicanos, porque dichos instrumentos internacionales se conciben como una extensión de lo previsto en esa Ley Fundamental respecto a los derechos humanos, en tanto que constituyen la razón y el objeto de las instituciones … "[97]

Posteriormente, y en similar sentido, se redactó el texto del párrafo segundo del artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, con su reciente reforma, efectuada por decreto publicado en el DOF el 10 de junio de 2011, en el cual se indica: "Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados

---

96 De acuerdo con la tesis aislada I.3º.C.79 K, Novena Época, del Tercer Tribunal Colegiado en Materia Civil del Primer Circuito, Semanario Judicial de la Federación y su Gaceta, Tomo XXVI, julio de 2007, p. 2725, materia civil y común, registro IUS 171888, los requisitos formales consisten en que el tratado sea celebrado por el presidente de la República y aprobado por el Senado, y el requisito de fondo se refiere a que la convención internacional esté conforme con el texto de la propia Ley Fundamental.

97 Tesis aislada XI.1o.A.T.45 K, Novena Época, Primer Tribunal Colegiado en Materias Administrativa y de Trabajo del Décimo Primer Circuito, Semanario Judicial de la Federación y su Gaceta, Tomo XXXI, mayo de 2010, p. 2079, materia común, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 164509.

internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia".

De lo anterior, se desprende la relevancia de aplicar las normas relativas a los derechos humanos existentes en el sistema jurídico mexicano, en beneficio de las personas, a través de una exégesis armónica y congruente de los derechos reconocidos en la Carta Magna y los tratados internacionales, independientemente de la preponderancia o aparente jerarquía que pudiera tener una sobre otra, con el único fin de otorgar una salvaguarda mayor en los derechos del individuo. Con ello se concluye, al menos en materia de derechos humanos, con las diversas y contradictorias interpretaciones jurisprudenciales que, hasta ese momento, se habían realizado respecto de la jerarquía de leyes señalada en el artículo 133 constitucional.

Lo antes citado también encuentra sustento en el principio de derecho internacional *pro homine* o *pro personae*, mediante el cual se dispone que deba aplicarse la norma que confiera mayor protección legal, salvaguarde la dignidad y asegure la integridad física, psicológica, emocional y patrimonial de las personas. Al respecto, la tesis 1a. XXVI/2012 emitida por la Primera Sala establece:

> "**PRINCIPIO PRO PERSONAE. EL CONTENIDO Y ALCANCE DE LOS DERECHOS HUMANOS DEBEN ANALIZARSE A PARTIR DE AQUÉL.** El segundo párrafo del artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, exige que las normas relativas a los derechos humanos se interpretarán de conformidad con la propia Constitución y con los tratados internacionales de los que México es parte, de forma que favorezca ampliamente a las personas, lo que se traduce en la obligación de analizar el contenido y alcance de tales derechos a partir del principio *pro personae* que es un criterio hermenéutico que informa todo el Derecho Internacional de los Derechos Humanos, en virtud del cual debe acudirse a la norma más amplia, o a la interpretación más extensiva cuando se trata de reconocer derechos protegidos, e inversamente, a la norma o a la interpretación más restringida cuando se trata de establecer restricciones permanentes al ejercicio de los derechos o de su suspensión extraordinaria, es decir, dicho principio permite, por un lado, definir la plataforma de interpretación de los derechos humanos y, por otro, otorga un sentido protector a favor de la persona humana, pues ante la existencia de varias posibilidades de solución a un mismo problema, obliga a optar por la que protege en términos más amplios. Esto implica acudir a la norma jurídica que consagre el

> derecho más extenso y, por el contrario, al precepto legal más restrictivo si se trata de conocer las limitaciones legítimas que pueden establecerse a su ejercicio. Por tanto, la aplicación del principio *pro personae* en el análisis de los derechos humanos es un componente esencial que debe utilizarse imperiosamente en el establecimiento e interpretación de normas relacionadas con la protección de la persona, a efecto de lograr su adecuada protección y el desarrollo de la jurisprudencia emitida en la materia, de manera que represente el estándar mínimo a partir del cual deben entenderse las obligaciones estatales en este rubro.[98]

Asimismo, y de acuerdo con el principio de convencionalidad, el Pleno de la Suprema Corte de Justicia de la Nación expone que en materia de derechos humanos, el mecanismo de control de convencionalidad debe ser acorde con el de control de constitucionalidad, como se observa en la siguiente tesis aislada P. LXVIII/2011:

> "**PARÁMETRO PARA EL CONTROL DE CONVENCIONALIDAD EX OFFICIO EN MATERIA DE DERECHOS HUMANOS**. El mecanismo para el control de convencionalidad *ex officio* en materia de derechos humanos a cargo del Poder Judicial debe ser acorde con el modelo general de control establecido constitucionalmente. El parámetro de análisis de este tipo de control que deberán ejercer todos los jueces del país, se integra de la manera siguiente: a) todos los derechos humanos contenidos en la Constitución Federal (con fundamento en los artículos 1o. y 133), así como la jurisprudencia emitida por el Poder Judicial de la Federación; b) todos los derechos humanos contenidos en tratados internacionales en los que el Estado Mexicano sea parte; c) los criterios vinculantes de la Corte Interamericana de Derechos Humanos derivados de las sentencias en las que el Estado Mexicano haya sido parte, y d) los criterios orientadores de la jurisprudencia y precedentes de la citada Corte, cuando el Estado Mexicano no haya sido parte.[99]

---

98 Tesis Aislada 1a. XXVI/2012, Décima Época, Primera Sala, Semanario Judicial de la Federación y su Gaceta, Libro V, Febrero de 2012, Tomo 1, página 659, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 200 0263.

99 Tesis Aislada P. LXVIII/2011, Décima Época, Pleno, Semanario Judicial de la Federación y su Gaceta, Libro III, Diciembre de 2011, Tomo 1, página 551, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 160526.

Lo anterior resulta de gran interés para la materia objeto de nuestro estudio, toda vez que el derecho a la protección de datos personales se encuentra también reconocido como derecho fundamental, incluso previo a su establecimiento en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales suscritos y aprobados por el gobierno de México, los cuales bajo la disposición constitucional antes señalada, resultan aplicables en cualquier circunstancia para extender sus beneficios en favor de los individuos; por tanto, la autoridad garante de este derecho, en un afán de brindar una mayor protección, deberá interpretar la leyes de la materia con base en la Ley Suprema de la Unión.

En este orden de ideas, es trascendente establecer el marco jurídico internacional, mediante la distinción de los tratados internacionales aplicables en el sistema jurídico mexicano, que han reconocido como derecho fundamental, el derecho a la protección de datos personales, así como de sus precedentes, como son el derecho a la intimidad y a la vida privada, por los motivos explicados en el Capítulo Primero del presente trabajo.

Cabe aclarar que dentro de esta mención de tratados internacionales, también incluiremos a aquéllos que por sus postulados universales son reconocidos ampliamente por la comunidad internacional como vigentes y obligatorios, no propiamente de manera jurídica, sino por una fuerza moral aceptada por los Estados miembros, sustentada en el reconocimiento de la dignidad intrínseca del ser humano mediante el respeto, sin distinción alguna, de sus libertades y derechos fundamentales.

Dentro de los instrumentos internacionales que cumplieron con los requisitos de fondo y formales establecidos en el artículo 133 de la Constitución Política de los Estados Unidos Mexicanos y que por tanto gozan de una obligación jurídica, se encuentran los siguientes:

I. El Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de la ONU en su Resolución 2200 A (XXI) del 16 de diciembre de 1966, mismo que entró en vigor el 23 de marzo de 1976,[100] reitera al igual que otros instrumentos internacionales, lo ya dispuesto en el artículo 12 de la Declaración Universal de los Derechos Humanos, con la única adición de las injerencias ilegales, para quedar como sigue en su artículo 17:

[100] El Pacto Internacional de Derechos Civiles y Políticos fue aprobado por el Senado el 18 de diciembre de 1980, según Decreto publicado en el DOF el 9 de enero de 1981, y promulgado por Decreto publicado en el DOF el 20 de mayo de ese mismo año. El 23 de junio de 1981 entró en vigor para México.

> "1. 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.
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

II. En ese mismo tenor, pero en el ámbito regional se encuentra la Convención Americana sobre Derechos Humanos,[101] adoptada en San José, Costa Rica, el 22 de noviembre de 1969 y entró en vigor el 18 de julio de 1978, la cual en su artículo 11 relativo a la protección de la honra y de la dignidad, expresa en sus numerales 2 y 3, lo siguiente:

> "2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

III. Por su parte, la Convención sobre los Derechos del Niño, adoptada el 20 de noviembre de 1989,[102] también reconoce el derecho a la vida privada a favor de los niños, al indicar en su artículo 16 que:

> "1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.
> 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

IV. En la Convención sobre los derechos de las personas con discapacidad, adoptada por la Asamblea General de la ONU, el 13 de diciembre de 2006, [103] se menciona textualmente, en sus artículos 22 y 31 el respeto a la privacidad y la recopilación de datos, de la siguiente manera:

---

101 La Convención Americana sobre Derechos Humanos, también conocida como Pacto de San José de Costa Rica, fue aprobada por el Senado el 18 de diciembre de 1980, según Decreto publicado en el DOF el 9 de enero de 1981, y promulgada mediante Decreto publicado en el DOF el 7 de mayo de 1981. Para México entró en vigor a partir del 24 de marzo de 1981.

102 La Convención sobre los derechos del niño fue aprobada por el Senado el 19 de junio de 1990, según Decreto publicado en el DOF el 31 de julio de 1990, ratificada el 21 de septiembre de ese mismo año y promulgada mediante Decreto publicado en el DOF el 25 de enero de 1991. Para México entró en vigor el 21 de octubre de 1990.

103 La Convención sobre los derechos de las personas con discapacidad fue aprobada por el Senado el 27 de septiembre de 2007, según Decreto publicado en el DOF el 24 de

> “Artículo 22
> Respeto de la privacidad
> 1. Ninguna persona con discapacidad, independientemente de cuál sea su lugar de residencia o su modalidad de convivencia, será objeto de injerencias arbitrarias o ilegales en su vida privada, familia, hogar, correspondencia o cualquier otro tipo de comunicación, o de agresiones ilícitas contra su honor y su reputación. Las personas con discapacidad tendrán derecho a ser protegidas por la ley frente a dichas injerencias o agresiones.
> 2. Los Estados Partes protegerán la privacidad de la información personal y relativa a la salud y a la rehabilitación de las personas con discapacidad en igualdad de condiciones con las demás”.

> “Articulo 31
> Recopilación de datos y estadísticas
> 1. Los Estados Partes recopilarán información adecuada, incluidos datos estadísticos y de investigación, que les permita formular y aplicar políticas, a fin de dar efecto a la presente Convención. En el proceso de recopilación y mantenimiento de esta información se deberá:
> a) Respetar las garantías legales establecidas, incluida la legislación sobre protección de datos, a fin de asegurar la confidencialidad y el respeto de la privacidad de las personas con discapacidad;
> b) Cumplir las normas aceptadas internacionalmente para proteger los derechos humanos y las libertades fundamentales, así como los principios éticos en la recopilación y el uso de estadísticas …”.

Ahora bien, dentro de los instrumentos internacionales no obligatorios jurídicamente se encuentran:

I. A nivel regional está la Declaración Americana de los derechos y deberes del hombre, adoptada en la IX Conferencia Internacional Americana, celebrada en Bogotá, Colombia, el 2 de mayo de 1948,[104] en donde en su artículo V

---

octubre de 2007, y promulgada mediante Decreto publicado en el DOF el 2 de mayo de 2008. Para México entró en vigor a partir del 3 de mayo de 2008.

[104] En esa misma Conferencia se constituyó la OEA mediante la adopción de su Carta, en ella México participó como miembro fundador. La Carta de la OEA fue aprobada por Decreto publicado en el DOF el 22 de noviembre de 1948 y promulgada por Decreto publicado en ese mismo medio oficial, el 13 de enero de 1949 y entró en vigor en México, el 13 de diciembre de 1951.

señala: “Toda persona tiene derecho a la protección de la Ley contra ataques abusivos a su honra, a su reputación y a su vida privada y familiar”.

II. Por su parte a nivel internacional y después de siete meses de la declaración emitida por los Estados Americanos, se emitió la Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Asamblea General de la ONU[105] mediante resolución 217 A (III) del 10 de diciembre de 1948, en cuyo artículo 12 se establece: “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”.

III. Posteriormente, ante la inquietud de que los logros científicos y tecnológicos puedan entrañar peligro para los derechos civiles y políticos de la persona o del grupo y para la dignidad humana, pero a la vez mediante un buen uso, puedan ser los medios principales para acelerar el desarrollo económico de los países, se emite la Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad, adoptada por la Asamblea General de la ONU, en su Resolución 3384 (XXX) del 10 de noviembre de 1975. Al respecto, proclama en su numeral 6 lo siguiente:

> “Todos los Estados adoptarán medidas tendientes a extender a todos los estrados de la población los beneficios de la ciencia y la tecnología y a protegerlos, tanto en lo social como en lo material, de las posibles consecuencias negativas del uso indebido del progreso científico y tecnológico, incluso su utilización indebida para infringir los derechos del individuo o del grupo, en particular en relación con el respeto de la vida privada y la protección de la persona humana y su integridad física e intelectual”.

IV. En la Declaración Universal sobre el genoma humano y los derechos humanos, adoptada por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), el 11 de noviembre de 1997, se reconoce en su artículo 1 que: “El genoma humano es la base de la unidad fundamental de todos los miembros de la familia humana y del reconocimiento de la dignidad intrínseca y su diversidad. En sentido simbólico, el genoma humano es el patrimonio de la humanidad”. En relación con los datos genéticos dicha declaración establece en sus artículos 5, incisos b y c, 7 y 9, lo siguiente:

---

[105] México fue admitido como Estado miembro de la ONU, el 7 de noviembre de 1945, misma fecha en la que entró en vigor para México, la Carta de la ONU, publicada en el DOF, el 17 de octubre de ese mismo año.

> “ARTÍCULO 5.
> a) …
> b) En todos los casos, se recabará el consentimiento previo, libre e informado de la persona interesada. Si esta no está en condiciones de manifestarlo, el consentimiento o autorización habrán de obtenerse de conformidad con lo que estipule la ley, teniendo en cuenta el interés superior del interesado.
> c) Se debe respetar el derecho de toda persona a decidir que se le informe o no de los resultados de un examen genético y de sus consecuencias”.
>
> “ARTÍCULO 7.
> Se deberá proteger en las condiciones estipuladas por la ley la confidencialidad de los datos genéticos asociados con una persona identificable, conservados o tratados con fines de investigación o cualquier otra finalidad”.
>
> “ARTÍCULO 9.
> Para proteger los derechos humanos y las libertades fundamentales, sólo la legislación podrá limitar los principios de consentimiento y confidencialidad, de haber razones imperiosas para ello, y a reserva del estricto respeto del derecho internacional público y del derecho internacional relativo a los derechos humanos”.

V. En otros documentos internacionales relativos a esta materia, se encuentran los “Principios rectores para la reglamentación de los ficheros computarizados de datos personales, adoptados el 14 de diciembre de 1990, por la Asamblea General de la ONU”, en la Resolución 45/95, los cuales sirven de guía para los Estados miembros en la elaboración de su reglamentación correspondiente. Los principios se dividen en dos grupos: a) los relativos a las garantías mínimas que deberían preverse en la legislación nacional, los cuales son aplicables a ficheros computarizados públicos y privados; y b) los ficheros de las organizaciones internacionales gubernamentales que contienen datos personales. Dentro de los principios rectores se encuentran los de: licitud y lealtad; exactitud; finalidad; de acceso de la persona interesada; de no discriminación; facultad de establecer excepciones; y de seguridad. También regula el control y sanciones por la vulneración de los principios, así como el flujo de datos a través de las fronteras.

A continuación se enuncian los instrumentos internacionales adoptados por organismos internacionales especializados en ciertas materias, que reconocen la protección de datos personales, y que igualmente formaron parte del marco jurídico internacional de México, al momento de ser admitido como uno de sus miembros:

I. El 18 de mayo de 1994, México fue admitido como miembro de la OCDE, fecha en que ratifica y entra en vigor la Convención de la OCDE del 14 de diciembre de 1960 y la Declaración del Gobierno de los Estados Unidos Mexicanos sobre la aceptación de sus obligaciones como miembro de la misma, documentos firmados el 14 de abril de 1994 y aprobados por la Cámara de Senadores, el 10 de mayo de 1994 por Decreto publicado en el DOF el día 13 de ese mismo mes y año. El Decreto de promulgación fue publicado en el DOF el 5 de julio de 1994.

En la "Declaración del Gobierno de los Estados Unidos Mexicanos sobre la aceptación de sus obligaciones como miembro de la OCDE", se establece que México aceptará los propósitos y objetivos del Informe del Comité Preparatorio de la Organización de diciembre de 1960, así como las Actas de la Organización en vigor al momento del depósito del instrumento, con las excepciones que se señalan en la declaración.

En el Anexo V denominado "Declaraciones a las que México se asocia" de la citada Declaración, se encuentra una relativa al tema de "Política de Información, Computación y Comunicaciones" que es la "Declaración sobre Flujo Transfronterizo de Información" del 11 de abril de 1985, en la cual se aborda el tema de los flujos de datos e información más allá de las fronteras nacionales, sobre actividades comerciales, flujos entre empresas, servicios de información informatizada e intercambios científicos y tecnológicos.

Si bien en dicha declaración el gobierno de México no hizo manifestación expresa para acoger las "Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales" del 23 de septiembre de 1980, en donde se establecen principios básicos para la recopilación y transferencia de datos personales, como se analizó en el Capítulo Primero, se debe entender como reconocida, en razón que en su Anexo VI, México expresa en términos generales las actividades de la OCDE y órganos de interés en los cuales desea participar, entre los que señala los concernientes a ciencia, tecnología e industria, temas estrechamente relacionados con la protección de datos personales.

Aunado a lo anterior, las citadas Directrices de la OCDE fueron el antecedente y el sustento para la emisión de la Declaración sobre Flujo Transfronterizo de Información, así como la Declaración sobre la protección de la privacidad de las redes globales, adoptada en la conferencia ministerial de la OCDE denominada "Un mundo sin fronteras: determinación del potencial del comercio electrónico", celebrada en 1998 en Ottawa, Canadá, en donde sus miembros reafirman el compromiso sobre la protección de la privacidad de las redes globales a fin de garantizar el respeto de derechos fundamentales, generar confianza en las

redes globales y evitar restricciones innecesarias en los flujos transfronterizos de datos personales.

En relación con la falta de fuerza obligatoria que tienen para los Estados miembros, las directrices, o también denominados lineamientos generales de las OCDE, Rocío Ovilla Bueno señala:

> "… Aún, si esta recomendación no tiene un valor obligatorio, exhorta a los Estados a vigilar el equilibrio en esta materia. En resumen, los Estados tienen dos tipos de obligaciones:
> - la obligación de protección de la vida privada y de las libertades individuales;
> - la obligación de garantizar la libre circulación de datos …".[106]

Por otra parte se encuentran las Directrices sobre política criptográfica, establecidas por recomendación de la OCDE, el 27 de marzo de 1997, en cuyo principio 5 establece que en las políticas nacionales de criptografía, así como en la aplicación y uso de métodos criptográficos, deben respetarse los derechos fundamentales de las personas a la intimidad, incluyendo el secreto de las comunicaciones y la protección de datos personales.

Otro documento emitido en la materia es la "Recomendación del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico", aprobada el 9 de diciembre de 1999, en la cual en relación con el tema de datos personales señala en el numeral "VII. Privacidad" que el comercio electrónico entre empresarios y consumidores debe estar de acuerdo con los principios de privacidad reconocidos y establecidos en las Directrices de la OCDE de 1980, que regulan la protección de la privacidad y el flujo transfronterizo de datos personales, así como con la Declaración de ese mismo organismo sobre protección de la privacidad en redes globales de 1998, a fin de proporcionar una apropiada y efectiva protección a los consumidores.

II. El 1 de enero de 1995 México formó parte de la Organización Mundial del Comercio (OMC), fecha en la que entró en vigor en el país, el Acta Final de la Ronda de Uruguay de Negociaciones Económicas Multilaterales y, por lo tanto, el Acuerdo por el que se establece la OMC, firmado el 15 de abril de 1994. El documento fue aprobado por el Senado el 13 de julio de 1994 y publicado el Decreto correspondiente en el DOF, el 4 de agosto de ese mismo año. El 31 de agosto de 1994 fue ratificado y el 30 de diciembre de ese año fue publicado en el DOF el Decreto de promulgación.

---

[106] OVILLA Bueno, Rocío, *La protección de los datos personales en México*, Porrúa, México, 2005, pp. 3 y 4.

El Acta Final de la Ronda de Uruguay de Negociaciones Económicas Multilaterales está integrada por los siguientes documentos que contienen los resultados de las negociaciones: el Acuerdo por el que se establece la OMC, las Declaraciones y Decisiones Ministeriales y el Entendimiento relativo a los Compromisos en Materia de Servicios Financieros, además de cuatro anexos.

En el Anexo 1B denominado “Acuerdo General sobre el Comercio de Servicios” del Acuerdo por el que se establece la OMC, se señala lo siguiente en su “Artículo XIV Excepciones generales”:

> “A reserva de que las medidas enumeradas a continuación no se apliquen en forma que constituya un medio de discriminación arbitrario o injustificable entre países en que prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios, ninguna disposición del presente Acuerdo se interpretará en el sentido de impedir que un Miembro adopte o aplique medidas:
> a) …
> b) …
> c) necesarias para lograr la observancia de las leyes y los reglamentos que no sean incompatibles con las disposiciones del presente Acuerdo, con inclusión de los relativos a:
> i) …
> ii) la protección de la intimidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales;
> iii) …
> d) …”

Por su parte, el “Entendimiento relativo a los Compromisos en Materia de Servicios Financieros” establece dentro de sus compromisos específicos, la posibilidad de que puedan ser compatibles las transferencias de información financiera y la protección de datos personales, de la siguiente manera:

> “B. *Acceso a los mercados*
> Transferencias de información y procesamiento de la información
> 1 al 7 …
> 8. Ningún Miembro adoptará medidas que impidan las transferencias de información o el procesamiento de información financiera, incluidas las transferencias de datos por medios electrónicos, o que impidan, a reserva de las normas de

importación conformes a los acuerdos internacionales, las transferencias de equipo, cuando tales transferencias de información, procesamiento de información financiera o transferencias de equipo sean necesarios para realizar las actividades ordinarias de un proveedor de servicios financieros. Ninguna disposición del presente párrafo restringe el derecho de un Miembro a proteger los datos personales, la intimidad personal y el carácter confidencial de registros y cuentas individuales, siempre que tal derecho no se utilice para eludir las disposiciones del Acuerdo.
9 al 11 …"

III. El 12 de septiembre de 1931, México ingresa en la Organización Internacional del Trabajo (OIT). El 14 de septiembre de ese año, el Senado aprobó la Constitución de la Organización Internacional del Trabajo, "Parte XIII del Tratado de Paz entre las Potencias Aliadas y Asociadas y Alemania", por Decreto publicado en el DOF, el 2 de octubre de 1931; sin embargo, no fue publicado el Decreto de promulgación correspondiente.

En la Reunión de Expertos de la OIT sobre la vida privada de los trabajadores, realizada en Ginebra el 7 de octubre de 1996, se emitió el "Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores", aplicable tanto para el sector público como el privado. Este documento contiene recomendaciones sin el carácter de obligatorio, no obstante ello, puede servir como una importante orientación y guía para empleadores y trabajadores en la recopilación, tratamiento y protección de datos personales de éstos últimos.

Actualmente ante la falta de estabilidad laboral, empleos bien remunerados y mejores oportunidades de vida, es cada vez más común que las personas padezcan de una movilidad laboral en periodos relativamente cortos, lo cual los obliga a buscar más de un empleo o nuevas fuentes de trabajo, y con ello a proporcionar sin reserva alguna, sus datos personales a diversas personas físicas y empresas, ya sea directamente o a través de la subcontratación o de la también conocida *outsourcing*, sin la garantía de que sean debidamente tratados, resguardados y cancelados sus datos, y con el riesgo de ser utilizados en forma adversa a su objetivo, o incluso para provocar la discriminación, porque dentro de los datos proporcionados se recaban en las pruebas de selección, incluso datos considerados como sensibles, principalmente obtenidos en los exámenes médicos, como el psicológico y el toxicológico.

De ahí la relevancia de contar con instrumentos como éste, en los cuales sin sustituir a la legislación nacional, puedan servir como guías para ampliar la

protección derechos fundamentales, especialmente cuando abarcan puntos trascendentes no previstos de manera específica, en la legislación de la materia, tales como: principios generales; formas de recopilación de datos; restricciones en el tratamiento de datos personales en pruebas de selección; vigilancia de trabajadores; conservación y utilización de datos; casos que requieren la obtención del consentimiento del trabajador; transferencias de datos; medidas de seguridad; derecho del trabajador a estar informado, a tener acceso y rectificar sus datos; y la sujeción a estas recomendaciones por parte de las agencias de colocación.

IV. En noviembre de 1993, México ingresó al APEC como uno de sus miembros. El APEC es un foro multilateral establecido en 1989 con el fin de mejorar el crecimiento económico en la región y para fortalecer a la comunidad de Asia-Pacífico, el cual se caracteriza por establecer compromisos voluntarios no vinculantes. A pesar de ello, es de resaltar el documento denominado Marco de Privacidad del APEC, que establece principios básicos para el flujo de información personal entre las “Economías Miembros”, especialmente llevado a cabo en el comercio electrónico, los cuales ya fueron señalados en el Capítulo Primero del presente trabajo.

Con el Marco de Privacidad, el APEC establece bases mínimas para regular los flujos de información, que al considerarlos como vitales en la realización de negocios dentro de una economía global, hacen necesaria la constitución de mecanismos flexibles que tiendan a la protección de la privacidad, pero al mismo tiempo, eviten la creación de barreras innecesarias para los flujos.

III. Leyes, Reglamentos y disposiciones en materia de protección de datos personales.

1. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Como se mencionó al inicio del presente Capítulo Segundo, la LFTAIPG publicada en el DOF el 11 de junio de 2002, reguló por vez primera a nivel federal, la protección de datos personales en posesión de entes públicos, incluso antes de ser reconocida, siete años más tarde, como derecho fundamental, por el artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos.

La LFTAIPG tuvo su origen en tres iniciativas presentadas para su revisión en primera instancia, por la Cámara de Diputados el 11 de julio, 30 de noviembre y 6 de diciembre, todas de 2001.[107]

De las tres iniciativas, la última se refiere exclusivamente al derecho al acceso a la información, sin hacer mención alguna a la protección de datos personales, razón por la cual no será objeto de análisis en el presente trabajo, a diferencia de las dos primeras que aluden expresamente a la protección de datos personales para incluirlo en la LFTAIPG, como una limitante y a la vez complemento del derecho de acceso a la información, y de las cuales ahondaremos a continuación.

En la exposición de motivos de la iniciativa de ley presentada el 11 de julio de 2001, por el Diputado Luis Miguel Jerónimo Barbosa Huerta, su autor señala al explicar las excepciones al ejercicio del derecho a la información, lo siguiente: "… Este derecho de información también comprende el derecho a acceder a las informaciones contenidas en actas y expedientes de la administración pública, así como a estar informado periódicamente, cuando lo requiera, de las actividades que desarrollan entidades y personas que cumplen funciones públicas, siempre y cuando este acceso no lesione un interés público preponderante o el derecho a la privacidad e intimidad de un tercero".[108]

Asimismo dentro del capítulo de faltas y sanciones administrativas y los delitos relacionados con la materia de la Ley, incluye dentro de las primeras, el entregar datos personales protegidos, y como sanciones penales a servidores públicos, la conducta consistente en alterar datos personales sin consentimiento.

Por su parte la segunda iniciativa presentada por el Ejecutivo Federal el 30 de noviembre de 2001, explica claramente el motivo para incluir la protección de datos personales en la LFTAIPG, la cual considera como uno de los principios que componen el acceso a la información, al exponer lo siguiente:

> "Como último principio, y como parte del objeto de la Ley, se señala la protección de datos personales. Existe una clara

[107] Cabe precisar que la LFTAIPG también fue producto de la activa participación de la sociedad civil, a través del denominado "Grupo Oaxaca" (grupo compuesto por académicos, empresarios, de los medios impresos de comunicación y organizaciones de la sociedad civil), el cual también presentó en el 2001, su propuesta de ley en la materia, ante la Cámara de Diputados.

[108] Exposición de motivos presentada en la Cámara de Diputados el 11 de julio de 2001, por el Diputado Luis Miguel Barbosa Huerta, disponible en http://www2.scjn.gob.mx/leyes/UnProcLeg.asp?nIdLey=24956&nIdRef=1&nIdPL=1&cTitulo=LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA GUBERNAMENTAL&cFechaPub=11/06/2002&cCateg=LEY&cDescPL=EXPOSICION DE MOTIVOS, consultada el 26 de abril de 2012.

> relación entre el derecho de acceso a la información y la protección de datos personales, no porque se trata forzosamente de dos realidades contrapuestas, sino porque la regulación de ambas debe ser complementaria. En efecto, la publicidad de la información debe respetar el derecho de privacidad que corresponde a los datos personales de cualquier individuo. Para lograr la correcta armonía entre uno y otro derecho, deben especificarse lo más posible sus alcances.
> Existe la conciencia de que cada uno de estos derechos es de tal magnitud, que requeriría de una ley especial que regule su objeto y establezca su diseño institucional, por esta razón y mientras no se expida una ley en materia de datos personales, la iniciativa que se presenta incluye un capítulo específico relativo a este tema, en el que se recogen los principios fundamentales al respecto y que puede servir de base para la legislación futura".[109]

Este último párrafo transcrito de la exposición de motivos del Ejecutivo Federal, resulta de gran valor para el presente trabajo de investigación, en el cual se intenta demostrar como la dispersa y múltiple normativa, en materia de protección de datos personales, puede convertirse en el principal obstáculo para facilitar su ejercicio mediante procedimientos y requisitos análogos que permitan a los titulares del derecho, identificar de manera ágil y sencilla los alcances y límites de su ejercicio, así como los medios con los que cuenta para la protección de sus datos personales de manera plena y eficaz.

Con lo antes señalado, es evidente que la intención principal para incluir un capítulo de protección de datos personales en la ley que regula el derecho de acceso a la información pública a nivel federal, era para reconocerlo como excepción o limitante a ese derecho, pero de igual forma, como resultado de su trascendencia en la actualidad, para incluirlo sólo bajo principios mínimos y de manera provisional en la LFTAIPG, en tanto se emitiera la ley de la materia y no dejarlo así fuera de toda regulación; sin embargo, esto no se llevó a cabo con la emisión de la LFPDPPP toda vez que la información personal en poder de entes públicos quedó exceptuada de dicha legislación, manteniéndose su regulación en definitiva, en la LFTAIPG y leyes estatales emitidas en materia de transparencia y acceso a la información.

---

[109] Iniciativa de ley presentada en la Cámara de Diputados el 30 de noviembre de 2001, por el Ejecutivo Federal, disponible en http://www.ifai.org.mx/pdf/pot/marco_normativo/iniciativa_LFTAIPG.pdf, consultada el 26 de abril de 2012.

Como consecuencia de la regulación del derecho a la protección de datos personales dentro de la ley que regula el derecho de acceso a la información, se puede caer en el riesgo de considerar a ambos derechos (derecho a la protección de datos personales y derecho de acceso a la información) como uno solo; de ahí la importancia de distinguir claramente la existencia de dos derechos autónomos, que si bien pueden estar estrechamente vinculados, no pueden ni deben confundirse, pues cuentan con fines, alcances y principios particulares, que justifican la existencia de su propia regulación para lograr su adecuada salvaguarda.

El Capítulo IV de la LFTAIPG regula la protección de datos personales y consta de siete artículos, en los cuales se establecen disposiciones mínimas que deberán acoger sus sujetos obligados.[110] Al respecto se emiten los siguientes comentarios:

- Los sujetos obligados puede establecer sus propios procedimientos para la atención de solicitudes de datos, dando lugar a una multiplicidad de requisitos y procedimientos.
- Los únicos derechos que el titular puede hacer valer ante los entes públicos son el de acceso y rectificación de datos, sin hacer mención expresa, a manera de excepción, de los derechos de cancelación y oposición reconocidos en la Carta Magna.
- Regula los principios de proporcionalidad, finalidad, calidad y consentimiento.
- Los sujetos obligados deberán contar con medidas de seguridad para garantizar los datos personales.
- Prohíbe a los sujetos obligados difundir, distribuir o comercializar datos personales, sin el consentimiento expreso de los individuos a que haga referencia, de lo cual se destaca a *contrario sensu* que en caso de contar con dicho consentimiento, entonces los sujetos obligados sí podrán difundir, distribuir y "comercializar" los datos personales, esta última conducta contraria a los fines que debe tener todo ente público, según los argumentos expuestos en los dictámenes para aprobar las reformas constitucionales, antes analizados, motivo por el cual se cuestiona el sustento de dichos dictámenes, para separar la regulación en la protección de datos personales, según quien la posea (entes públicos o privados), basado en la materia de comercio.

[110] De conformidad con el artículo 3, fracción XIV de la LFTAIPG, los sujetos obligados son: 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; d) Los órganos constitucionales autónomos; e) Los tribunales administrativos federales; y f) Cualquier otro órgano federal.

- Las bases de datos son denominadas “Sistemas de datos personales”, cuya existencia deberá hacerse del conocimiento de las autoridades competentes en la materia.
- Es importante mencionar que la LFTAIPG no se refiere a titulares de derechos sino a “interesados”, es decir como si se tratara de cualquier persona que acredita tener un interés en el asunto sin importar si es o no el titular del derecho, lo cual es contrario a la naturaleza del derecho a la protección de datos como derecho personal.
- Se reconoce el ejercicio del acceso y rectificación de datos personales a los interesados o sus representantes, previamente acreditados.
- Señala plazos para atender o dar respuesta a las solicitudes: a) para el acceso otorga 10 días hábiles y b) para la rectificación, 30 días hábiles.
- Los sujetos obligados deben establecer unidades de enlace o equivalentes donde reciban las solicitudes de los interesados.
- Establece el recurso de revisión como medio legal para impugnar la negativa de entregar o corregir datos, así como, en contra de la falta de respuesta, no considerando dentro de los supuestos, el de la inconformidad con la respuesta emitida por el ente público.

Como analizaremos más adelante, estos principios mínimos se complementarán con el Reglamento de la LFTAIPG, publicado en el DOF el 11 de junio de 2003, así como con los Lineamientos de Protección de Datos Personales, publicados en ese mismo periódico oficial, el 30 de septiembre de 2005.

Por otra parte, es de observarse que el Capítulo IV de la LFTAIPG no establece que los sujetos obligados deban emitir su propia normatividad respecto de la protección de datos personales, distinta a la ya establecida en dicha ley y su reglamento; sin embargo, cuando la LFTAIPG hace una distinción entre el acceso a la información en el Poder Ejecutivo Federal (Título Segundo) y el acceso a la información en los demás sujetos obligados (Título Tercero), permite que estos últimos, en el ámbito de sus respectivas competencias, emitan reglamentos o acuerdos generales, para establecer criterios y procedimientos institucionales en esta materia; lo cual se ha interpretado, en el mismo sentido, para la protección de datos personales.

De esta manera, encontramos disposiciones en materia de protección de datos personales, emitidas por el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) obligatoria para dependencias y entidades de la Administración Pública Federal, así como para la Procuraduría General de la República, y disposiciones emitidas por los denominados “demás sujetos obligados” de la LFTAIPG, como son el Poder Legislativo Federal; el Poder Judicial de la Federación y el Consejo de la Judicatura Federal; los órganos constitucionales

autónomos; los tribunales administrativos federales; y cualquier otro órgano federal. Aunado a ello, se suma toda la normativa emitida por los entes públicos estatales; lo cual reiteramos, induce a la complejidad del ejercicio del derecho y a la pluralidad de criterios y procedimientos.

Por lo anterior, resulta conveniente analizar como parte de la evolución del derecho a la protección de datos personales, la posibilidad de establecer en una sola ley, disposiciones aplicables tanto para entes privados como públicos; en este último caso, y sólo para los entes públicos estatales, serían lineamientos generales, a fin de respetar su autonomía para legislar sobre la materia.

2. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Como se mencionó en el análisis del Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, en su Artículo Segundo Transitorio se ordenó al Congreso de la Unión expedir en un plazo no mayor de doce meses, contados a partir de la entrada en vigor del referido Decreto, la ley en materia de protección de datos personales en posesión de los particulares, plazo que venció el 1 de mayo de 2010.

En cumplimiento a dicho artículo transitorio, el 27 de abril de 2010 fue aprobado por la Cámara de Senadores, el "Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3 y 33, así como la denominación del Capítulo II, del Título Segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental"; Decreto que fue promulgado por el Ejecutivo Federal el 28 de junio de 2010 y publicado en el DOF el 5 de julio de 2010, para entrar en vigor el día 6 de ese mismo mes y año.

Es importante destacar que los trabajos para la elaboración y emisión de la LFPDPPP no iniciaron después de la publicación del citado Decreto de reforma al artículo 73 de la Carta Magna, sino que éstos comenzaron a realizarse antes, incluso previo a la elaboración y aprobación de las reformas constitucionales en esta materia.

La LFPDPPP tuvo su origen en seis iniciativas presentadas, en primera instancia, a la Cámara de Diputados para su revisión; la primera de ellas se presentó el 6 de septiembre de 2001,[111] fecha considerada como el punto de partida de un

[111] Las otras cinco iniciativas fueron presentadas en la Cámara de Diputados, el 1 de diciembre de 2005, el 23 de febrero y 22 de marzo, ambas de 2006 y el 7 de octubre y

arduo y largo camino por recorrer durante ocho años y diez meses, para concluir finalmente, con la publicación e inicio de vigencia de la LFPDPPP, en julio de 2010.

Así las cosas, el proceso legislativo para la emisión de la LFPDPPP fue complejo al estar implicado de adversidades, tales como, la ausencia o escasez de información de una materia que no se conocía en México, o por lo menos, no se comprendía con la misma fuerza y dimensión que en otros países. Por ello, fue necesario para iniciar con los trabajos de investigación, allegarse de información emitida en el tema, a nivel internacional y en el derecho comparado, a fin de hallar el modelo de protección de datos personales que mejor se adecuara a la realidad y necesidades del país.

Asimismo, debía realizarse por parte de los postulantes de las iniciativas de ley, una labor previa de convencimiento, tanto al interior de las Cámaras de Diputados y Senadores, como al exterior, específicamente con los diversos sujetos involucrados en esta materia, y en general, con la sociedad mexicana para crear consciencia respecto de la relevancia y trascendencia que tiene este derecho en la vida actual y cotidiana. Al respecto, consideramos que la labor informativa y de convencimiento no debe concluir con la sola emisión de la LFPDPPP y su Reglamento, sino que es preciso continuar con la misma hasta obtener su amplio conocimiento, especialmente en cuanto a sus alcances y efectos, para consolidar en la sociedad mexicana, una cultura en la prevención y salvaguarda de este derecho.

Otra de las dificultades halladas durante la elaboración de la LFPDPPP, consistió en establecer las condiciones óptimas para el funcionamiento y desarrollo del derecho a la protección de datos personales, previo a la emisión de la ley, lo cual requirió en primer término, de la creación del sustento constitucional de este derecho mediante su reconocimiento como derecho fundamental. Así se explica que en el transcurso del proceso de revisión de la LFPDPPP, se hubiere emitido la reforma al artículo 16 constitucional, para adicionarle un segundo párrafo, base irrefutable de cualquier disposición normativa en materia de protección de datos personales, y congruente con los compromisos adquiridos por México a nivel internacional.

Para la preparación de las condiciones antes referidas, se debía definir la autoridad garante del derecho a la protección datos personales, encontrándose dentro de las propuestas, la creación de un órgano autónomo federal y especializado en la materia; un órgano de alguna de las dependencias involucradas en la materia, como la Secretaría de Economía; o un órgano autónomo federal ya existente, como el entonces denominado Instituto Federal de Acceso a la Información Pública

11 de diciembre, ambas de 2008, respectivamente, las cuales serán comentadas más adelante.

Gubernamental. Esta última fue la propuesta aprobada, puesto que a través de dicho Instituto, organismo descentralizado ya constituido, se evitarían erogar mayores gastos. Asimismo al estar presidido por un órgano colegiado autónomo, permitiría en igual forma, asegurar la autonomía de sus decisiones, las cuales, desde luego, irían respaldadas con una desarrollada experiencia en la protección de datos personales en poder de entes públicos federales y bajo la aplicación de criterios ya establecidos en esa materia.

Las seis iniciativas que se analizaron para la emisión de la LFPDPPP, en términos generales presentan ciertas semejanzas en cuanto a su estructura y contenido; sin embargo al observar en cada una de ellas ciertas particularidades y una notable evolución, consideramos valioso su señalamiento, por tratarse del origen y sustento de la ley vigente.

❖ **Proyecto de Ley de Protección de Datos Personales, presentada por el Diputado Miguel Barbosa Huerta, del Grupo Parlamentario del Partido de la Revolución Democrática, en la Sesión del jueves 6 de septiembre de 2001**.[112] En la exposición de motivos de esta iniciativa se señala que el proyecto tuvo como propósito esencial, el hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos, a través de "ficheros de datos", por lo cual éstos se convierten en el elemento básico y preponderante de la iniciativa, al considerar que su existencia y utilización justifica la necesidad de una nueva protección al derecho a la intimidad, el cual se ve seriamente amenazado por las nuevas técnicas de la comunicación e informática.

En ese sentido, con esta iniciativa se pretende que los ficheros no sean sólo vistos como meros depósitos de datos, sino también, en una perspectiva más dinámica, como aquellos procesos o aplicaciones informáticas que se llevan a cabo con los datos almacenados; los cuales una vez vinculados entre sí, permiten lograr la configuración de perfiles personales bien definidos. De esta forma, la simple acumulación de datos aislados puede no ser representativa, pero al vincularse entre sí, de manera sistematizada, clasificada u organizada, puede adquirir un sentido distinto y un valor especial, con carácter incluso, comercial o económico. Del contenido del proyecto de ley se destacan los siguientes puntos:

- Excluye de la aplicación de la ley, a los datos estadísticos, a la información pública como la contenida en el registro civil, los ficheros especiales como los electorales y la información en la que prevalece el interés público o por

[112] El proyecto de Ley de Protección de Datos Personales, presentado por el Diputado Miguel Barbosa Huerta, el 6 de septiembre de 2001, se encuentra disponible en http://gaceta.diputados.gob.mx/Gaceta/58/2001/sep/20010907.html#Ini20010907Barbosa.

seguridad nacional o pública. Cabe mencionar que el proyecto no establece expresamente si su aplicación será en todo el territorio nacional, por lo que es omisa en regular la coordinación, en la materia, con entidades federativas y municipios.

- Contempla la posibilidad de aplicar la ley a los datos relativos a personas morales, sin ser precisa en qué sentido. Así como el derecho de acceso de titulares fallecidos a través de sus sucesores legítimos.
- Establece principios generales, entendidos como pautas que regirán la recolección de datos personales, tales como la congruencia, racionalidad, finalidad y, en forma especial, el principio del consentimiento o de autodeterminación, por tratarse del nivel de protección que cada individuo otorga a sus datos personales a través de la manifestación de su consentimiento.
- Propone el establecimiento de un sistema cautelar, mediante el reconocimiento de los derechos de impugnación de valoraciones, de consulta, de acceso, de rectificación, de cancelación, de oposición y de indemnización. En todos los casos, a excepción del último, el titular deberá ejercer primero el derecho ante el Responsable, y derivado de su incumplimiento, entonces podrá ejercer la acción de protección de datos personales ante el juez civil de orden común.
- Crea el Registro Nacional de Protección de Datos como ente integrado al Instituto Nacional de Estadística, Geografía e Informática, encargado de coadyuvar en el cumplimiento de la ley.
- Distingue dos tipos de ficheros, según sea su titularidad, pública o privada, los cuales deben inscribirse en el Registro Nacional de Protección de Datos.
- Contempla la cesión o transmisión de datos, nacional o internacional, a fin de lograr el libre flujo de los mismos.
- Establece como garantía para el acceso, rectificación o destrucción de datos, la acción de protección de datos personales o *habeas data*, promovida respecto de los ficheros de los Responsables, usuarios o encargados, a través de un juicio ordinario civil.
- Considera las conductas delictivas en esta materia y sus correspondientes sanciones privativas de la libertad.

❖ **Proyecto de Ley Federal de Protección de Datos Personales, a cargo del Diputado Jesús Martínez Álvarez, del Grupo Parlamentario de Convergencia**.[113] El elemento principal de este proyecto ya no va a ser el fichero de

[113] El proyecto de Ley Federal de Protección de Datos Personales presentado por el Diputado Jesús Martínez Álvarez, el 1 de diciembre de 2005, se encuentra disponible en http://gaceta.diputados.gob.mx/Gaceta/59/2005/dic/20051201-I.html#Ini20051201JMA.

datos, sino el individuo mismo quien posee derechos fundamentales reconocidos. En la exposición de motivos de la iniciativa, se señala que la protección de datos implica la salvaguarda de los derechos fundamentales de las personas, por lo que es inaceptable la idea de considerarla como una variación de los derechos de la propiedad y, por tanto, atribuible de un valor económico con el cual se puede comercializar. Por eso, resulta necesario garantizar la capacidad de las personas en la protección de sus datos a través de un ordenamiento jurídico relativo a esta materia. Como puntos relevantes de esta iniciativa se encuentran los siguientes:

- Exceptúa de la aplicación de la ley, los datos de carácter personal; los exclusivamente privados y personales; la información científica, tecnológica o comercial publicada en medios de comunicación oficial; las resoluciones judiciales publicadas en esos mismos medios; y la administrada por sindicatos, iglesias y asociaciones religiosas, siempre y cuando sean exclusivas de sus miembros y relacionadas con su objeto.
- Considera la aplicación de las disposiciones de la ley, en lo conducente, a los datos de personas jurídicas; así como el acceso a datos de personas fallecidas, a través de sus sucesores universales.
- Establece principios generales para el tratamiento de datos personales, entre los cuales se encuentran, el de finalidad, calidad, información y consentimiento.
- Considera las transferencias entre entes públicos o privados, nacionales o extranjeros, siempre y cuando proporcionen los niveles adecuados de protección.
- Reconoce como derecho de los titulares el acceso, rectificación o eliminación de sus datos personales ante los Responsables o usuarios de bancos de datos y, ante su incumplimiento, la posibilidad de promover la acción de protección de datos personales ante juez de orden común para archivos privados y ante el juez federal para archivos de datos públicos.
- Contempla el registro de archivos de datos, en donde debe inscribirse todo archivo, registro, base o banco de datos público y privado.
- Señala disposiciones específicas para el tratamiento de datos personales con fines de defensa nacional, seguridad nacional o seguridad pública y los registrados con fines policiales.
- Establece la creación de un Instituto encargado de vigilar la protección de datos personales, conformado por tres comisionados nombrados por el Ejecutivo Federal, el cual se establecería en la Ley Federal de Transparencia y Acceso a la Información Pública.
- Ante el incumplimiento de la ley, se contempla el apercibimiento y la aplicación de sanciones graves y administrativas, como facultad del Instituto, las cuales serían establecidas en su reglamento.

❖ **Proyecto de Ley Federal de Protección de Datos Personales, a cargo del Diputado David Hernández Pérez, del Grupo Parlamentario del PRI**.[114] En este proyecto ya no se busca vincular la protección de datos personales con los derechos fundamentales existentes, sino establecerla como un derecho fundamental autónomo reconocido a nivel internacional, cuya premisa básica es la libertad de los individuos para controlar su información personal. Por ello, su propósito es regular las conductas de terceros en relación con los datos personales de los individuos, quienes tienen el derecho inalienable de decidir sobre el manejo de sus datos; por lo que la característica primordial de esta iniciativa es el respeto de la libertad de decisión del individuo. De acuerdo con la exposición de motivos, este proyecto se caracteriza por:

- Buscar la compatibilidad de la ley con las prácticas empresariales, a fin de no entorpecer el crecimiento y desarrollo del país.
- Exceptúa de la aplicación de la ley, a diferencia de los otros dos proyectos, a los entes públicos, sindicatos o asociaciones profesionales y sociedades de información crediticia.
- Ya no contempla como obligación de los Responsables, el registrar sus bases de datos, por considerar ésta, una tarea imposible de llevar a cabo, debido al dinamismo de las bases, impulsando a cambio el autocontrol.
- Establece una nueva obligación para el Responsable, la de hacer del conocimiento del titular el aviso de privacidad, considerado como el eje central de la propuesta, por ser el pilar en el tratamiento de bases de datos, donde se establecerán los fines primarios y secundarios de su tratamiento y, por lo tanto, los límites de su uso, así como por ser el medio de control con el que cuenta el titular para la divulgación o no de sus datos.
- El aviso de privacidad debe atender a nueve principios básicos: Información, elección, transferencia, seguridad, integridad, acceso, cumplimiento, conocimiento y consentimiento.
- Deja a cargo del entonces denominado Instituto Federal de Acceso a la Información Pública Gubernamental, las funciones de vigilancia e interpretación de la ley, entre las que se encuentran la aplicación del procedimiento administrativo de protección de datos personales; en consecuencia la primera instancia ya no será una autoridad jurisdiccional sino una administrativa, y sus resoluciones serán impugnables ante el Poder Judicial de la Federación.

---

[114] El proyecto de Ley Federal de Protección de Datos Personales, presentado por el Diputado David Hernández Pérez, del Grupo Parlamentario del PRI, el 23 de febrero de 2006, se encuentra disponible en http://gaceta.diputados.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Ini20060223DatosPersonales.

- Establece disposiciones relativas al consentimiento, uso y divulgación de los datos personales.
- Contempla la figura del encargado o departamento de datos personales, designado o establecido por el Responsable, quien recibirá y tramitará las solicitudes de los titulares para el acceso, modificación o cancelación de sus datos. Para el derecho de acceso se establece un procedimiento específico.
- Se precisan las infracciones a la ley, las cuales podrán ser sancionadas con apercibimientos o multas, de acuerdo con las circunstancias del caso, el daño causado y las condiciones del infractor.

A partir de este proyecto de ley empieza a haber una mayor semejanza con la LFPDPPP vigente, en cuanto a que excluye definitivamente de su aplicación a los entes públicos, otorga relevancia a la autodeterminación informativa del titular y al autocontrol de los sujetos obligados, así como concede un papel preponderante a la elaboración y emisión de un aviso de privacidad, como base y sustento para el ejercicio de este derecho.

❖ **Proyecto de la Ley Federal de Protección de Datos Personales, a cargo de la Diputada Sheyla Fabiola Aragón Cortés, del Grupo Parlamentario del PAN**.[115] En la exposición de motivos de esta iniciativa se destaca la importancia de contemplar los trabajos realizados en materia de protección de datos a nivel internacional, ya citados anteriormente, como son los Lineamientos de la OCDE y el Marco de Privacidad de la APEC, en los cuales se establecieron compromisos internacionales, que con esta propuesta se pretenden cumplir; así la emisión de una ley sobre la materia se vuelve una responsabilidad del gobierno mexicano, no sólo por tratarse de un tema de derechos fundamentales, sino por tener su origen y efectos esenciales en la economía nacional y el aseguramiento del comercio interestatal e internacional, por lo que esta iniciativa circunscrita a la materia de comercio, encuentra su sustento en las facultades del Congreso de la Unión en esta materia federal (Artículo 73, fracción X de la Constitución Política de los Estados Unidos Mexicanos). En cuanto a su estructura y contenido, esta iniciativa es muy parecida a la antes citada, como se observa a continuación:

- Exceptúa de la aplicación de la ley a las materias: financiera, de seguros y fianzas, electoral, de seguridad nacional y pública; así como entes públicos, sindicatos o asociaciones profesionales y sociedades de

[115] El Proyecto de la Ley Federal de Protección de Datos Personales, presentado por la Diputada Sheyla Fabiola Aragón Cortés, el 22 de marzo de 2006, se encuentra disponible en http://gaceta.diputados.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Ini20060322Sheyla.

información crediticia. Y excluye del concepto de datos personales, los de registros públicos y los derivados de relaciones laborales.

- Propone como órgano encargado del cumplimiento de la ley al entonces denominado Instituto Federal de Acceso a la Información Pública, únicamente por razones presupuestarias y por la conveniencia de aprovechar instituciones existentes.
- Establece grados de responsabilidad, tanto para quien aprovecha la información (Responsable) como para quien funge como operador directo de su obtención y tratamiento (tercero).
- Introduce el concepto del sistema de datos personales, a fin de no limitarlo sólo a bases o bancos de datos, sino a cualquier actividad automatizada o no de datos clasificados o susceptibles de clasificación. El sistema deberá inscribirse en un registro, propuesta ya presentada con las primeras iniciativas.
- Contempla el aviso de privacidad, el cual al igual que la iniciativa anterior, considera como la principal institución legal de garantía respecto de la privacidad de la que goza el titular.
- Reconoce en todos los casos, la prerrogativa de los individuos de manifestar su voluntad ante el uso contrario de su información.
- La divulgación de información a terceros debe incluir las mismas restricciones de origen.
- Contempla las infracciones a la ley sin enunciar las conductas, las cuales serán sancionadas, de acuerdo con los daños causados, el carácter intencional, la gravedad o la reincidencia, con amonestación o multa.

❖ **Proyecto de la Ley de Protección de Datos Personales en Posesión de Particulares, a cargo del Diputado Luis Gustavo Parra Noriega, del Grupo Parlamentario del PAN**.[116] Como se observa esta iniciativa es la primera que incluye dentro de su denominación, la expresión de datos personales "en posesión de particulares", ello debido quizás, a que para la fecha en que fue presentado este proyecto (7 octubre de 2008), ya se encontraba contemplada la protección de datos personales en posesión de entes públicos, en el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, reformado el 20 de julio de 2007, aunado a que también, para ese entonces, se encontraba para dictamen de la Cámara de Senadores, la reforma al artículo 73 de la Carta Magna, a fin de dotar de facultades al Congreso de la Unión, en materia de protección de datos en posesión de particulares.

---

[116] El Proyecto de la Ley de Protección de Datos Personales en Posesión de Particulares, presentado por el Diputado Luis Gustavo Parra Noriega, el 7 de octubre de 2008, se encuentra disponible en http://gaceta.diputados.gob.mx/Gaceta/60/2008/oct/20081007-III.html#Ini20081007-21.

Por lo anterior, en esta iniciativa ya no se considera necesario regular o hacer mención alguna a la protección de datos personales en posesión de entes públicos, toda vez que ésta ya se encuentra regulada en los diversos ordenamientos legales existentes a nivel federal y estatal. Y es por ello que dentro de sus excepciones a la ley, únicamente se referirán a entes privados, como son las sociedades de información crediticia y la recolección de datos para uso personal, excepciones que se conservaron en la ley vigente. Dentro de los puntos característicos de esta iniciativa se encuentran:

- Incluye el concepto de disociación, entendido como el procedimiento a través del cual los datos personales no podrán asociarse al titular ni permitir la identificación del mismo.
- Establece siete principios: de licitud, consentimiento, información, calidad, confidencialidad, derecho al olvido y seguridad.
- Contempla el procedimiento ante el Responsable para que el titular ejerza sus derechos de acceso, rectificación, cancelación y oposición.
- Ante la inconformidad del titular se incluye un procedimiento denominado declaración administrativa de infracción, llevado ante la autoridad competente, para determinar la procedencia de la solicitud.
- Considera la conciliación en cualquier etapa del procedimiento.
- Crea la Comisión Nacional de Protección de Datos Personales, con la naturaleza jurídica de un organismo centralizado de la Administración Pública Federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio; el cual cuenta con plena autonomía técnica y de gestión.
- Señala las infracciones a la ley y sus correspondientes sanciones, consistentes en apercibimientos y multas.

❖ **Proyecto que expide la Ley Federal de Protección de Datos Personales, a cargo del Diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI**.[117] Esta iniciativa al igual que la anterior, parte de la idea que la protección de datos personales en posesión de entes públicos ya se encuentra resuelta por lo dispuesto en el artículo 6o. constitucional, por tanto, sólo es necesario regular la protección de datos en posesión de los particulares. En su exposición de motivos se señala la importancia de alcanzar un balance entre la protección efectiva de los datos y la necesidad de contar con los mismos, para la generación de productos y servicios que produzcan un valor económico, empleo y desarrollo.

---

[117] El Proyecto de la Ley Federal de Protección de Datos Personales, presentado por el Diputado Adolfo Mota Hernández, del Grupo Parlamentario del PRI, el 11 de diciembre de 2008, se encuentra disponible en http://gaceta.diputados.gob.mx/Gaceta/60/2008/dic/20081211-VII.html#Ini20081211-1.

Esta iniciativa se basa en el modelo regulatorio de protección de datos personales denominado “híbrido”, caracterizado por contemplar la intervención de una autoridad centralizada encargada principalmente de supervisar la aplicación de la ley, y permitir, al mismo tiempo, la autorregulación por parte de los particulares, apoyada en las mejores prácticas a nivel internacional, sin descuidar la protección de los datos de los titulares; modelo que sigue la LFPDPPP vigente. Como características principales de esta iniciativa se encuentran:

- Considera el aviso de privacidad como el principal mecanismo para limitar la recolección de información, mediante el consentimiento de su titular.
- La regulación se centra en las conductas y actividades relacionadas con la recolección y manejo de datos, y no en estos últimos.
- Establece la existencia de una autoridad central dependiente de alguna secretaría de Estado como la Secretaría de Economía. A este ente especializado lo denomina Instituto de Protección de Datos Personales, dotado de facultades para vigilar el cumplimiento de la ley.
- Reconoce la necesidad de las transferencias para operaciones comerciales, pero éstas sólo se harán en los términos establecidos en el aviso de privacidad, a fin de garantizar niveles efectivos de protección de los datos personales.
- Contempla dos procedimientos, el del ejercicio de los derechos de acceso, rectificación, cancelación y oposición del titular ante el Responsable, y el procedimiento administrativo de protección de datos personales, el cual es muy similar al actual procedimiento de protección de derechos contemplado en la LFPDPPP.
- Señala las infracciones a la ley y sus sanciones consistentes en multas.

Estas seis propuestas fueron ampliamente analizadas en la Cámara de Diputados el 25 de marzo de 2010 y en la Cámara de Senadores el 22 de abril de 2010, en donde cabe destacar lo siguiente:

La Comisión de Gobernación de la Cámara de Diputados fue la encargada de concentrar en un solo proyecto las seis iniciativas presentadas y entregar el proyecto final para su discusión y aprobación, en donde entre otros puntos, se señaló:

- La necesidad de contar con una ley de aplicación nacional, para unificar la tutela del derecho a la protección de datos personales, reconocido ya en ese momento como derecho fundamental en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en cuanto a derechos, principios y procedimientos de protección, lo cual repercutirá no sólo en las relaciones a nivel nacional sino también en las internacionales.

- Destaca la importancia de contar con un ordenamiento jurídico de esta naturaleza, para hacer más competitivo al país en su aspecto económico.
- Designa al Instituto Federal de Acceso a la Información Pública, como la autoridad encargada de vigilar el cumplimiento de la ley, especialmente por razones de: ahorro de costos, unicidad de criterios, experiencia, autonomía y su buen posicionamiento en el entorno político y social. Al efecto propone modificar la denominación del Instituto para incluir su nueva función de protección de datos.
- Resalta la función de la ley para desincentivar conductas contrarias a la misma, por lo que al ser vulnerado este derecho fundamental, el Responsable debe ser sancionado por su negligencia o dolo en el tratamiento de datos personales, especialmente cuando se trate de datos sensibles.
- De conformidad con las facultades del Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares, el decreto por el cual se expide la ley, tendría la fuerza legal para imponer la abrogación de las leyes estatales en esta materia.

En la Cámara de Senadores se expusieron diversos puntos, entre los que sobresalen los siguientes:

- Señalan al igual que en la Cámara de Diputados, la necesidad de contar con un sólo régimen de protección en todo el país, para favorecer la inversión nacional y extranjera, así como otorgar ventajas competitivas frente a otras naciones, al brindar certeza jurídica en los intercambios comerciales transfronterizos.
- La ley representa un modelo híbrido de protección de datos, para lograr el justo equilibrio de los principios internacionalmente reconocidos, el libre flujo de datos y las garantías necesarias para el titular, a través del tratamiento lícito e informado de sus datos personales.
- El proyecto satisface los elementos básicos que garantizan la protección de datos personales, establecidos en el artículo 16 constitucional, al establecer principios, derechos, procedimientos, definición de autoridad reguladora y garante, así como un catálogo de infracciones y sanciones.
- Aprueban que el Instituto Federal de Acceso a la Información Pública sea la autoridad reguladora en esta materia, con lo cual México se suma a la nueva tendencia en Europa de incluir en una misma autoridad la materia de acceso a la información y la de protección de datos, como ocurre en Reino Unido, Suiza, Hungría y Eslovenia.
- La propuesta otorga una preeminencia a las decisiones del titular y a la vez evita la imposición de cargas excesivas e innecesarias de cumplimiento a los sujetos obligados.

- Garantiza la coherencia normativa en la materia, al regular la coadyuvancia de las autoridades sectoriales con el Instituto Federal de Acceso a la Información Pública.
- Prevé mecanismos de autorregulación para la observancia de la ley.
- Establece un régimen transitorio que permite a los sujetos obligados adecuar sus prácticas actuales y a las autoridades emitir la regulación mínima indispensable para la correcta observancia de la ley.

Los puntos antes referidos, que fueron revisados y discutidos en primera instancia en la Cámara de Diputados y, posteriormente, en la Cámara de Senadores, se incluyeron en el proyecto final que conformó la LFPDPPP vigente; proyecto en el que ya no se contemplaron algunas propuestas de las seis iniciativas de origen, y que por su contenido relevante consideramos debieron incluirse en la ley de la materia, como son las siguientes:

- En la primera y segunda iniciativas (6 de septiembre de 2001 y 1 de diciembre de 2005)[118], la ley es aplicable tanto para entes públicos como privados, toda vez que ambos pueden poseer y tratar datos personales, y por lo tanto adquieren responsabilidades frente a los titulares de derechos, en el manejo y uso de sus datos personales.
- Asimismo, en dichas iniciativas se regula el caso de las personas fallecidas y el ejercicio de ciertos derechos a través de sus herederos, situación no prevista en la actual ley, pues no obstante, de ser un derecho personalísimo que finaliza con la muerte de su titular, es necesario regular la forma como se cancelarán ciertos datos personales correspondientes al sujeto fallecido.
- La existencia de una autoridad responsable de la protección de datos personales que se propone en las iniciativas quinta y sexta (7 de octubre y 11 de diciembre, ambas de 2008), [119] es relevante en el sentido de establecer una institución especializada en la materia y dotada de las facultades necesarias para garantizar ampliamente este derecho, aunque para ello es indispensable la autonomía en la toma de sus decisiones como se establece en la segunda iniciativa (1 de diciembre de 2005).
- Es importante incluir como lo señala la iniciativa segunda, algunas disposiciones específicas relacionadas con las excepciones a la ley, como lo son en materia de seguridad nacional, seguridad pública y defensa nacional, pues no obstante de encontrarse ello regulado en las leyes de cada materia, con esto se daría cumplimiento al precepto constitucional para establecer claramente las excepciones a la ley.

---

[118] *Cfr.* el análisis de la primera y segunda iniciativa de la ley en materia de protección de datos personales, en las páginas 91 y 92 del presente trabajo.

[119] *Cfr.* el análisis de la quinta y sexta iniciativa de la ley en materia de protección de datos personales, en las páginas 96 y 97 del presente trabajo.

3. Leyes Estatales en materia de transparencia y acceso a la información pública gubernamental.

El artículo Segundo Transitorio del Decreto por el que se adicionó un segundo párrafo con siete fracciones al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, publicado en el DOF el 20 de julio de 2007, señaló lo siguiente:

> "… La Federación, los Estados y el Distrito Federal, en sus respectivos ámbitos de competencia, deberán expedir las leyes en materia de acceso a la información pública y transparencia, o en su caso, realizar las modificaciones necesarias, a más tardar un año después de la entrada en vigor de este Decreto".

De acuerdo con el referido artículo transitorio, todas las entidades federativas y el Distrito Federal tenían hasta el 21 de julio de 2008, para emitir sus leyes en materia de acceso a la información pública y transparencia o, en su caso, llevar a cabo las adecuaciones correspondientes en las mismas, a fin de contemplar los principios y bases aludidos en dicho precepto constitucional, dentro de los cuales se encuentra la protección de datos personales.

Al respecto, como se observa en el cuadro siguiente, todas las entidades federativas ya contaban con una ley de acceso a la información y transparencia, incluso antes de la reforma constitucional, a excepción de Baja California Sur que emitió su ley hasta el 10 de marzo de 2010. De esta forma los demás Estados y el Distrito Federal realizaron únicamente modificaciones a sus legislaciones vigentes o emitieron unas nuevas para hacerlas acordes a lo dictado por el artículo 6o. constitucional.

N°	Estado	Ley	Fecha de emisión y/o publicación	Órgano encargado	Disposición que regula la protección de datos personales
1	Aguascalientes	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 26 de agosto de 2002)	Emisión: 19 mayo 2006 Publicación: 22 mayo 2006	Instituto de Transparencia	Capítulo IV Artículos 23 al 28
2	Baja California	Ley de Transparencia y Acceso a la Información Pública	Emisión: 28 julio 2005 Publicación: 12 agosto 2005	Instituto de Transparencia y Acceso a la Información Pública	Artículos 31 al 36 y 70 al 76
3	Baja California Sur	Ley de Transparencia y Acceso a la Información Pública	Emisión: 10 de marzo 2010 Publicación: 12 de marzo 2010	Instituto de Transparencia y Acceso a la Información Pública	Artículos 25 al 28
4	Campeche	Ley de Transparencia y Acceso a la	Emisión: 1 de julio 2005	Comisión de Transparencia y	Capítulo Séptimo Artículos 31 al 38

		Información Pública	Publicación: 21 julio 2005	Acceso a la Información Pública	(Capítulo derogado por la emisión de la Ley de Protección de Datos Personales del Estado de Campeche y sus Municipios)
5	Chiapas	Ley que Garantiza la Transparencia y el Derecho a la Información Pública	Emisión: 12 octubre 2006 Publicación: 12 octubre 2006	Instituto de Acceso a la Información Pública de la Administración Pública Estatal	Capítulo II Artículos 42 al 45
6	Chihuahua	Ley de Transparencia y Acceso a la Información Pública	Emisión: 14 octubre 2005 Publicación: 15 octubre 2005	Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública	Capítulo III Artículos 36 al 42 *Habeas Data*
7	Coahuila	Ley de Acceso a la Información Pública y Protección de Datos Personales (Abroga Ley del 4 de noviembre de 2003)	Emisión: 17 junio 2008 Publicación: 2 septiembre 2008	Instituto Coahuilense de Acceso a la Información Pública	Capítulo Sexto Artículos 47 al 84
8	Colima	Ley de Transparencia y Acceso a la Información Pública	Emisión: 28 febrero 2003	Comisión Estatal para el Acceso a la Información Pública	Artículos 8 y 26, fracción I *Habeas Data* Cuenta con una ley de protección de datos personales
9	Distrito Federal	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 8 de mayo de 2003)	Emisión: 7 marzo 2008 Publicación: 28 marzo 2008	Instituto de Acceso a la Información Pública y Protección de Datos Personales	Artículos 8 y 38, fracción I Cuenta con una ley de protección de datos personales
10	Durango	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 25 de febrero de 2003)	Emisión: 11 julio 2008 Publicación: 13 julio 2008	Comisión Estatal para la Transparencia y el Acceso a la Información Pública	Artículos 39 al 42 y Capítulo VII Artículos 43 al 51
11	Estado de México	Ley de Transparencia y Acceso a la Información Pública	Emisión: 18 marzo 2004 Publicación: 30 abril 2004	Instituto de Transparencia y Acceso a la Información Pública	Artículos 25Bis, 26 y 27 Capítulo V Artículos 50 al 55
12	Guanajuato	Ley de Acceso a la Información Pública	Publicación: 29 julio 2003	Instituto de Acceso a la Información Pública	Artículos 5, fracción III, 12 y 18, fracción I Cuenta con una ley de protección de datos personales
13	Guerrero	Ley Número 374 de Transparencia y Acceso a la Información Pública (Abroga Ley del 10 de octubre de 2005)	Emisión: 21 mayo 2010 Publicación: 15 junio 2010	Instituto de Transparencia y Acceso a la Información Pública	Capítulo VI Artículos 50 al 55 Capítulo VIII Artículo 56 al 62 Capítulo X Artículos 65 al 70
14	Hidalgo	Ley de Transparencia y Acceso a la Información Pública Gubernamental	Emisión: 29 diciembre 2006 Publicación: 18 diciembre 2006	Comité de Información Pública Gubernamental	Título Cuarto Capítulos I y II Artículos 39 al 51
15	Jalisco	Ley de Información Pública (Abroga Ley del 6 de enero de 2005)	Emisión: 9 diciembre 2011 Publicación: 22 diciembre 2011	Instituto de Transparencia e Información Pública	Artículos 2, fracción II y 44numeral 1, fracción I La protección de datos está regulada sólo como información confidencial
16	Michoacán	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 28 de agosto de 2002)	Emisión: 21 octubre 2008 Publicación: 7 noviembre 2008	Instituto de Transparencia y Acceso a la Información Pública	Capítulo Quinto Artículos 53 al 64 Capítulo Sexto Artículos 65 al 71 Capítulo Séptimo Artículos 72 al 79

17	Morelos	Ley de Información Pública, Estadística y Protección de Datos Personales	Emisión: 25 agosto 2003 Publicación: 27 agosto 2003	Instituto Morelense de Información Pública y Estadística	Título IV Capítulo Primero Artículos 54 al 58 Capítulo Segundo Artículos 59 al 67 *Habeas Data*
18	Nayarit	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 16 de junio de 2004)	Emisión: 19 diciembre 2007 Publicación: 22 diciembre 2007	Instituto para la Transparencia y Acceso a la Información Pública	Artículos 20 al 25
19	Nuevo León	Ley de Transparencia y Acceso a la Información (Abroga Ley del 21 de febrero de 2003)	Emisión: 3 julio 2008 Publicación: 19 julio 2008	Comisión de Transparencia y Acceso a la Información	Título Segundo Capítulo Primero Artículos 43 al 54 Capítulo Segundo Artículos 55 al 62 Capítulo Tercero Artículos 63 al 69 Capítulo Cuarto Artículos 70 al 79
20	Oaxaca	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 16 de septiembre de 2006)	Emisión: 28 febrero 2008 Publicación: 15 marzo 2008	Instituto Estatal de Acceso a la Información Pública	Título Segundo Capítulo Único Artículos 35 al 42 (Título derogado por la emisión de la Ley de Protección de Datos Personales –*Habeas Data*)
21	Puebla	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 16 de agosto de 2004)	Emisión: 19 diciembre 2011 Publicación: 31 diciembre 2011	Comisión para el Acceso a la Información Pública y Protección de Datos Personales	Artículos 38, fracción I y 39 La protección de datos está regulada sólo como información confidencial
22	Querétaro	Ley Estatal de Acceso a la Información Gubernamental	Emisión: 26 septiembre 2002 Publicación: 27 septiembre 2002	Comisión Estatal de Información Gubernamental	Artículos 3, fracciones II, VII y XVI último párrafo La protección de datos está regulada sólo como información confidencial
23	Quintana Roo	Ley de Transparencia y Acceso a la Información Pública	Emisión: 13 mayo 2004	Instituto de Transparencia y Acceso a la Información Pública	Capítulo Sexto Artículos 31 al 35 Capítulo Séptimo Artículo 36
24	San Luis Potosí	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 20 de marzo de 2003)	Emisión: 11 octubre 2007 Publicación: 18 octubre 2007	Comisión Estatal de Acceso a la Información Pública	Título Tercero Capítulo I Artículos 11 al 13 Título Quinto Capítulo II Artículos 44 al 47 Capítulo III Artículos 48 al 57
25	Sinaloa	Ley de Acceso a la Información Pública	Emisión: 25 abril 2002 Publicación: 26 abril 2002	Comisión Estatal para el Acceso a la Información Pública	Capítulo Sexto Artículos 33 al 36 *Habeas data*
26	Sonora	Ley de Acceso a la Información Pública	Publicación: 25 febrero 2005	Instituto de Transparencia Informativa	Sección IV Artículos 30 al 34BisB Sección V Artículos 34BisC-H y 35
27	Tabasco	Ley de Transparencia y Acceso a la Información Pública	Emisión: 17 enero 2007 Publicación: 10 febrero 2007	Instituto Tabasqueño de Transparencia y Acceso a la Información Pública	Capítulo Octavo Artículos 55 al 58

28	Tamaulipas	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley de Información Pública)	Emisión: 4 julio 2007 Publicación: 5 julio 2007	Instituto de Transparencia y Acceso a la Información	Capítulo Tercero Artículos 36 al 39 *Habeas data*
29	Tlaxcala	Ley de Acceso a la Información Pública (Abroga la Ley del 12 de enero de 2007)	Emisión: 10 mayo 2012 Publicación: 22 mayo 2012	Comisión de Acceso a la Información Pública y Protección de Datos Personales	Artículos 25, fracción I y 8, fracciones X y XXII, último párrafo Cuenta con una ley de protección de datos personales
30	Veracruz	Ley de Transparencia y Acceso a la Información Pública (Abroga Ley del 8 de junio de 2004)	Emisión: 16 febrero 2007 Publicación: 27 febrero 2007	Instituto Veracruzano de Acceso a la Información	Capítulo Quinto Artículos 19 al 25
31	Yucatán	Ley de Acceso a la Información Pública	Emisión: 15 mayo 2004 Publicación: 31 mayo 2004	Instituto Estatal de Acceso a la Información Pública	Capítulo V Artículos 20 al 26
32	Zacatecas	Ley de Transparencia y Acceso a la Información Pública (Abroga la Ley del 14 de julio de 2004)	Emisión: 24 mayo 2011 Publicación: 29 junio 2011	Comisión Estatal para el Acceso a la Información Pública	Capítulo Quinto Sección Primera Artículos 45 al 54 Sección Segunda Artículos 55 al 64

Fuente: El cuadro fue elaborado con la información obtenida en http://www.diputados.gob.mx/LeyesBiblio/gobiernos.htm, a través de la cual se tuvo acceso a cada una de las páginas de Internet de los congresos estatales y de la Asamblea Legislativa del Distrito Federal, mismas que fueron consultadas del 8 al 17 de junio de 2012. Y actualizado el 7 de octubre de 2012.

Del cuadro anterior, es de resaltar que Sinaloa fue el pionero en la materia de acceso a la información y también en protección de datos, en razón de ser el primer Estado en contar con una ley de esta naturaleza, desde el 26 de abril de 2002, fecha anterior incluso a la LFTAIPG, aprobada el 30 de abril de 2002 y publicada en el DOF el 11 de junio de ese mismo año.

En ese sentido, consideramos relevante hacer mención especial a la Ley de Acceso a la Información Pública del Estado de Sinaloa, la cual regula el derecho a la protección de datos personales, a través de la figura jurídica del *habeas data*, definida en su artículo 5, fracción VII, como: “La garantía de tutela de la privacidad de datos personales en poder de las entidades públicas”. Dentro de su Capítulo Sexto “Del ejercicio de Derecho de Habeas Data”, incluye los principios de finalidad e información, asimismo considera los derechos de acceso, rectificación y cancelación de datos personales, para toda persona que demuestre su identidad. Asimismo señala las excepciones al registro de datos personales para proteger la seguridad pública o la vida de las personas, y hace especial mención a evitar situaciones de discriminación con la obtención de datos sensibles. Sin embargo, en esta ley no se mencionan cuáles serán los criterios y procedimientos a seguir para el ejercicio del derecho, por lo cual se considera incompleta.

Al igual que Sinaloa, otros Estados como Chihuahua, Colima, Morelos, Oaxaca y Tamaulipas también regulan en sus leyes la protección de datos personales a través de la figura jurídica del *habeas data*, sin contemplar en ninguna

de ellas un alcance mayor al meramente administrativo, toda vez que esta acción no es interpuesta ante autoridad jurisdiccional, sino ante los propios sujetos obligados y, en una segunda instancia, impugnada su resolución, a través de recursos administrativos presentados ante el órgano encargado del acceso a la información y transparencia en la entidad.

Por otra parte, de la revisión de las legislaciones estatales, observamos como los Estados de la Federación regulan de manera distinta dentro de sus leyes de acceso a la información pública y transparencia, la protección de datos personales en poder de entes públicos, porque mientras unos lo hacen de manera amplia y propositiva, otros tan sólo lo hacen en los mismos términos que en la LFTAIPG y unos más, como Jalisco y Puebla, sólo de manera somera y enunciativa dentro de la información confidencial, sin hacer mayor abundamiento. Por otra parte, algunos Estados cuentan también con disposiciones secundarias relativas a la materia, en cuyo caso se encuentran Aguascalientes, Chiapas, Guanajuato, Guerrero, Tlaxcala y el Distrito Federal, los cuales ha emitido lineamientos sobre protección de datos personales.

Algunos Estados han ido todavía más allá, como son Campeche, Colima, Guanajuato, Oaxaca, Tlaxcala y el Distrito Federal, al emitir su propia legislación sobre protección de datos personales en poder de entes públicos, como se señala a continuación:

N°	Estado	Ley	Fecha de emisión y/o publicación	Órgano encargado	Aspectos relevantes
1	Campeche	Ley de Protección de Datos Personales	Emisión: 25 junio 2012 Publicación: 9 de julio de 2012	Comisión de Transparencia y Acceso a la Información Pública.	Destaca que el objeto de la ley sea la protección de los datos personales en poder de los entes públicos del Estado y no los derechos de los titulares. Contempla los derechos de acceso, rectificación, cancelación y oposición. Exceptuándolos en caso de seguridad pública. Contra las resoluciones procede el recurso de revisión. Por infracciones a la ley contempla la aplicación de sanciones administrativas.
2	Colima	Ley de Protección de Datos Personales	Emisión: 14 junio 2003 Publicación: 21 junio 2003	Comisión Estatal para el Acceso a la información Pública.	La acción de protección de datos personales o *habeas data* puede ser interpuesta por personas físicas o morales. Considera los derechos de acceso, rectificación, cancelación y oposición. El afectado puede solicitar la indemnización por daño o lesión en sus bienes o derechos. Contempla un Registro de Protección de Datos que estará a cargo de la Comisión. Por infracciones a la ley se aplicarán multas.
3	Distrito Federal	Ley de Protección de Datos Personales	Emisión: 27 agosto 2008 Publicación: 3 octubre 2008	Instituto de Acceso a la Información Pública y Protección de Datos Personales	Regula el sistema de datos personales y un responsable del mismo. Contempla los derechos de acceso, rectificación, cancelación y oposición, así como un procedimiento para su ejercicio. Regula de manera amplia las medidas de seguridad a través de niveles de seguridad: básico, medio y alto. Considera el recurso de revisión ante el Instituto en caso de inconformidad. Señala las infracciones a la ley y la aplicación de sanciones administrativas.

4	Guanajuato	Ley de Protección de Datos Personales	Publicación: 19 mayo 2006	Instituto de Acceso a la Información Pública	Contempla los derechos de acceso, rectificación y cancelación, así como un procedimiento para su ejercicio. Considera como dato personal, las claves informáticas o cibernéticas, códigos personales encriptados u otros análogos vinculados a la intimidad de la persona física. Establece como medio de impugnación, el recurso de queja ante el Instituto. Constituye el Registro Estatal de Protección de Datos Personales. Señala las infracciones a la ley y como sanciones: la amonestación, multa y destitución.
5	Oaxaca	Ley de Protección de Datos Personales	Emisión: 7 agosto 2008 Publicación: 23 agosto 2008	Instituto Estatal de Acceso a la Información Pública	Establece principios generales. Contempla los derechos de acceso, rectificación y cancelación, así como el procedimiento para su ejercicio, denominado como *Habeas Data*. Considera el derecho de acceso a información de personas fallecidas, a sus sucesores. Establece como medio de impugnación, el recurso de revisión ante el Instituto. Señala las causales de responsabilidad administrativa.
6	Tlaxcala	Ley de Protección de Datos Personales	Emisión: 26 abril 2012	Comisión de Acceso a la Información Pública y Protección de Datos Personales	Establece principios de protección de datos personales. Contempla para la interpretación de la ley, a la Constitución Federal y a los tratados internacionales suscritos por México. Considera el ejercicio de los derechos ARCO y su procedimiento. Señala como obligación de los "sujetos obligados" contar con el aviso de privacidad. Establece tipos de medidas de seguridad y niveles. Contempla la figura de la denuncia ante la Comisión. Constituye el Registro Estatal de Protección de Datos Personales. Establece como medio de impugnación, el recurso de revisión ante la Comisión y el de revocación contra sus resoluciones. Señala las infracciones a la ley, distinguiendo las consideradas como graves. Y sanciones administrativas como la amonestación.

Fuente: El cuadro fue elaborado con la información obtenida en http://www.diputados.gob.mx/LeyesBiblio/gobiernos.htm, a través de la cual se tuvo acceso a cada una de las páginas de Internet de los congresos estatales y de la Asamblea Legislativa del Distrito Federal, mismas que fueron consultadas del 8 al 17 de junio de 2012. Y actualizado el 7 de octubre de 2012.

Con la anterior información podemos observar que Colima fue el primer Estado en emitir una ley particular sobre la protección de datos personales en poder de entes públicos, lo cual en su momento fue novedoso, sin embargo ahora la de Tlaxcala resulta ser la más completa y acorde con los temas actuales sobre la materia.

Otros Estados han emitido legislación todavía más específica sobre protección de datos personales, lo cual los hace innovadores en la materia, tal es el caso de Chihuahua con la Ley Reguladora de la Base de Datos Genéticos, publicada en su periódico oficial el 1 de abril de 2009, donde a través de la Fiscalía General del Estado, se regula el Sistema Estatal de Registro de ADN, constituido sobre la base de huellas genéticas y muestras biológicas, información considerada como datos sensibles de sus titulares y respecto de la cual no es posible constituir base o fuente alguna de discriminación, estigmatización o vulneración de la dignidad, intimidad, privacidad u honra de persona alguna, tal y como lo establecen sus artículos 3 y 4.

Asimismo, de acuerdo con lo señalado en el artículo 21, inciso B), se contempla el derecho de eliminación de las huellas dactilares, a solicitud de la víctima o del imputado, cuando acrediten la conclusión del procedimiento correspondiente.

Por otra parte, y a pesar de tratarse sólo de proyectos, consideramos relevante mencionar los "lineamientos y criterios para la presentación pública de presuntos responsables de delitos y transcripción de sus datos personales en comunicados de prensa" y los "lineamientos y criterios para la protección de datos personales en materia de procuración de justicia", documentos que trabajan en conjunto, el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, la Procuraduría de Justicia del Distrito Federal, la Comisión de Derechos Humanos del Distrito Federal y la Universidad Nacional Autónoma de México, con lo cual se pretende colocar al Distrito Federal como ejemplo y vanguardia a nivel nacional, en la protección de datos personales.[120]

De estas legislaciones estatales cabe destacar que en la mayoría consideran todos los derechos ARCO, situación que no se contempla de igual forma a nivel federal, al incluir únicamente los derechos de acceso y rectificación. De esta revisión consideramos que la multiplicidad de disposiciones que pueden existir para garantizar el derecho a la protección de datos personales en poder de entes públicos, puede provocar incertidumbre en el titular de los datos personales, y con ello falta de seguridad y certeza jurídica en el ejercicio de su derecho.

En relación a esta diversidad de procedimientos, plazos, criterios y garantías establecidas en las distintas leyes estatales, la Comisionada del IFAI, Sigrid Arzt se ha pronunciado por la emisión de una Ley General de Transparencia y Acceso a la Información Pública, para avanzar en el fortalecimiento de la transparencia y rendición de cuentas.[121] Y no obstante, de no señalar nada con respecto a la protección de datos personales, es evidentemente el impacto que tendrá dicha propuesta en la protección de datos personales en poder de entes públicos, por ser éste, como ya se ha expuesto, un tema regulado dentro de las leyes de transparencia y acceso a la información, tanto federal como estatales; en cuyo caso, será importante valorar la conveniencia de traspasar este derecho a una ley específica que regule la protección de datos personales, independientemente de

---

120 Ver noticia del 19 de junio de 2012, publicada en el periódico El Sol de México, Sección Ciudad, "Preparan lineamientos para exhibir a presuntos delincuentes", disponible en http://www.tedf.org.mx/sala_prensa/sintesis/sm2012/jun/120619/120619_cdhdf_preparan_lineamientos.pdf.

121 Comunicado IFAI/081/12, Oaxaca, Oaxaca, 18 de junio de 2012, "Propone Sigrid Arzt promover una Ley General de Transparencia y Acceso a la Información", Foro Regional *Los órganos autónomos en las propuestas para una política de rendición de cuentas ¿Centralismo, federalismo o cooperación?*, disponible en http://www.ifai.org.mx/Publicaciones/comunicados, consultada el 16 de julio de 2012

quien posea los mismos (ente público o privado), pues lo realmente trascendente será garantizar a los titulares, el ejercicio de este derecho fundamental.

4. Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

El Reglamento de la LFTAIPG, publicado en el DOF el 11 de junio de 2003, refiere a la protección de datos personales, en su Capítulo VIII, integrado por los artículos 47 y 48, donde establece obligaciones aplicables sólo para las dependencias y entidades federales, consistentes en:

1. Garantizar en los procedimientos para acceder a los datos personales, la protección de los derechos de los individuos, en especial los relativos a la vida privada y la intimidad, así como los derechos de acceso y corrección de datos personales, de acuerdo con los lineamientos que expida el IFAI y demás disposiciones aplicables.
2. Hacer del conocimiento al IFAI y del público en general, a través de sus sitios de internet, los sistemas de datos personales con los que cuenten, así como los listados de los mismos, e indicar el objeto del sistema, tipo de datos y uso de los mismos, así como la unidad administrativa y el nombre del responsable que los administra.

De lo anterior se desprenden los siguientes comentarios:

- El Reglamento de la LFTAIPG remite para efectos del procedimiento de acceso y corrección de datos personales (únicos derechos considerados en la LFTAIPG), a otras disposiciones como son los lineamientos de protección de datos personales, sin embargo el Capítulo XIII del mismo Reglamento ya establece un procedimiento para el ejercicio de estos derechos por parte de sus titulares, por lo que se considera innecesaria la emisión de otra normativa en esta materia.
- La obligación de dar aviso al IFAI se encuentra regulada en el artículo 23 de la LFTAIPG y es únicamente para aquellas dependencias y entidades que cuenten con el sistema de datos personales (“Sistema Persona”), sin señalar como se llevará el control para aquéllas que no cuente con aquél. Por lo cual se considera infructuosa la tarea de llevar un registro de sistemas de datos incompleto y, tal vez, desactualizado al no existir ninguna obligación para registrarse.
- En cuanto a los elementos integrantes del sistema, éstos son similares a los requisitos básicos que debe contener todo aviso de privacidad, entendido como aquel documento elaborado por los entes privados y puesto a disposición del titular previo al tratamiento de sus datos personales; sin embargo, difieren en razón de no tener la misma fuerza

obligatoria para su emisión, ya que para los entes públicos sólo lo es, en caso de contar con un sistema de datos, en cambio para los particulares es obligatorio por el sólo hecho de tratar datos personales. Además, en el caso del aviso de privacidad no existe obligación para los particulares de registrarlo ante el Instituto sino hacerlo del conocimiento del titular.

En cuanto a las disposiciones relativas al procedimiento de acceso y corrección de datos personales, previsto en el Reglamento de la LFTAIPG, son mínimas y generales, en virtud de que los Comités de cada dependencia y entidad podrán establecer sus propios plazos y procedimientos internos para dar trámite a las solicitudes de acceso y corrección de datos personales. Es importante mencionar que este procedimiento únicamente lo podrá iniciar el titular de los datos personales o su representante legal y las resoluciones de los Comités podrán ser impugnables a través del recurso de revisión interpuesto ante el IFAI.

5. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

El Reglamento de la LFPDPPP fue publicado en el DOF el 21 de diciembre de 2011, y entró en vigor al día siguiente de su publicación, éste consta de diez capítulos relativos a:

I. Disposiciones Generales;
II. De los Principios de Protección de Datos Personales;
III. De las Medidas de Seguridad en el Tratamiento de Datos Personales;
IV. De las Transferencias de Datos Personales;
V. De la Coordinación entre Autoridades;
VI. De la Autorregulación Vinculante;
VII. De los Derechos de los Titulares de Datos Personales y su Ejercicio;
VIII. Del Procedimiento de Protección de Derechos;
IX. Del Procedimiento de Verificación;
X. Del Procedimiento de Imposición de Sanciones; y

Los cuatro últimos temas serán analizados más adelante, toda vez que se refieren al ejercicio del derecho de protección de datos personales y los procedimientos existentes para garantizarlo, los cuales son objeto de análisis del siguiente capítulo, por tanto, ahora únicamente abordaremos los seis primeros temas antes enunciados.

En disposiciones generales resulta de interés el señalamiento de las siguientes excepciones mencionadas en los artículos 3 y 5 del Reglamento de la LFPDPPP, de lo cual es importante destacar que sólo refieren a la aplicación del Reglamento y no así de la LFPDPPP, lo cual pudiere resultar incongruente:

- No se aplicará el Reglamento cuando para acceder a los datos personales se requieran plazos o actividades desproporcionadas. En ese mismo sentido el artículo 22 de la LFPDPPP señala que los datos personales deben ser resguardados de tal manera que permita el ejercicio sin dilación de los derechos ARCO. Es por esta razón que la información debe constar en soportes físicos o electrónicos debidamente organizados y clasificados, de lo contrario estarán exceptuados.
- Para información relativa a personas morales.
- Información que refiera a personas físicas en su calidad de comerciantes y profesionistas.
- Datos de contacto para fines de representación del empleador o contratista, entendidos como aquella información de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, que consisten en nombre y apellidos, las funciones o puestos desempeñados, y datos laborales como: domicilio físico, dirección electrónica, teléfono y número de fax.

Por otra parte, señala dos casos en los cuales sí aplican las disposiciones del referido Reglamento, en sus artículos 6 y 8:

- Cuando tenga como propósito cumplir una obligación derivada de una relación jurídica, en cuyo caso no se considerará información de uso exclusivamente personal (excepción señalada en el artículo 2, fracción II de la LFPDPPP).
- Serán considerados Responsables o Encargados, las personas integrantes de un grupo que actúe sin personalidad jurídica y que trate datos personales para finalidades específicas o propias del grupo.

En relación con los principios de protección de datos personales, el Reglamento de la LFPDPPP regula ampliamente cada uno de los principios señalados en el artículo 6 de la LFPDPPP, que son: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, los cuales son prácticamente obligaciones a cargo de los Responsables.

Uno de los principios más importantes y mayormente abordados en el Reglamento, es el del consentimiento, en razón de ser el sustento en el tratamiento de datos personales. En ese sentido, se hace una extensa explicación de la diferencia, en qué casos aplica, cómo se acredita y su revocación. Los tipos de consentimiento contemplados son: tácito, expreso, verbal y escrito, cuya aplicación

será libremente establecida por el Responsable, a excepción de datos sensibles, financieros y patrimoniales, donde se exige el consentimiento expreso para su tratamiento.

En el principio de información prevalece la regulación del aviso de privacidad como obligación para el Responsable y documento base para ejercer los derechos ARCO, el cual debe contener como mínimo los requisitos establecidos en el artículo 16 de la LFPDPPP que son:

1. Identidad y domicilio del Responsable.
2. Finalidad del tratamiento de datos.
3. Opciones y medios que el Responsable ofrezca a los titulares para limitar el uso y divulgación de los datos.
4. Medios para ejercer los derechos ARCO.
5. Transferencias de datos que se efectúen en su caso.
6. Procedimiento y medio por el cual comunicará cambios al aviso de privacidad.

Además de dichos requisitos, también se encuentran los señalados por los artículos 8, 15 y 36 de la LFPDPPP, los cuales consisten en:

1. Mecanismos y procedimientos para revocar el consentimiento.
2. Información que se recaba de los titulares y con qué fines.
3. En caso de transferencia de datos personales a terceros nacionales o extranjeros, distintos del encargado, el aviso de privacidad deberá contener una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, excepto para los casos señalados en el artículo 37 de la LFPDPPP, entre los que se contemplan: las transferencias para la prestación de asistencia sanitaria o tratamiento médico; para salvaguarda de un interés público o para la procuración o administración de justicia; y para el mantenimiento o cumplimiento de una relación jurídica entre el Responsable y el Titular.

Asimismo, respecto del aviso de privacidad, cabe hacer los siguientes comentarios:

- La regla general consiste en que el Responsable ponga a disposición del titular el aviso de privacidad de manera personal o directa, por los medios que tenga a su alcance y considere convenientes (incluye cualquier tipo de formato: impresos, digitales, visuales, sonoros o cualquier otra tecnología, y cualquier tipo de medio: electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología).

Este aviso de privacidad será otorgado en la forma completa prevista en los artículos 8, 15, 16 y 36 de la LFPDPPP, o en la forma simplificada, establecida en el artículo 17, fracción II de la LFPDPPP, es decir, cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, en cuyo caso bastará que se le informe la identidad y domicilio del Responsable y la finalidad del tratamiento de los datos, así como los mecanismos necesarios para conocer el texto completo del aviso de privacidad. También se aplicará esta forma simplificada, cuando el aviso de privacidad se emita a través de formatos con espacio limitado, en razón que los datos obtenidos son mínimos.

- Sólo podrá exceptuarse de la entrega del aviso de privacidad de manera personal o directa, cuando resulte imposible dar a conocerlo o ello exija al Responsable esfuerzos desproporcionados, ello en consideración al número de titulares o a la antigüedad de los datos.
- En este caso de excepción, se utilizará una forma alterna de dar a conocer a los titulares de los datos personales, de manera masiva, la existencia de su tratamiento, prevista en el artículo 18, párrafo tercero de la LFPDPPP denominada: Medidas Compensatorias.
- Para el uso de medidas compensatorias se requiere contar con la autorización del IFAI.
- El supuesto de excepción a esa autorización se establece en los “Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del IFAI” (Criterios Generales), publicados en el DOF el 18 de abril de 2012, y sólo será para el caso de que el Responsable haya obtenido los datos personales antes del vencimiento del plazo para emitir los avisos de privacidad (antes del 6 de julio de 2011) y además: a) exista imposibilidad de dar a conocer al titular el aviso de privacidad ó, b) la puesta a disposición exija esfuerzos desproporcionados.
- Los Criterios Generales establecen que cuando el tratamiento involucre datos sensibles, patrimoniales o financieros, los criterios se podrán aplicar, sólo cuando no se requiera el consentimiento del titular, de conformidad con lo establecido en los artículos 10 y 37 de la LFPDPPP y el 17 de su Reglamento.
- Dentro de los medios para comunicar el aviso de privacidad en forma masiva se encuentra la página de Internet del Responsable. Sin embargo, ésta sólo se utilizará cuando los datos personales hayan sido recabados por ese mismo medio; o bien el perfil de los titulares, permita al Responsable suponer, de manera razonable, que los titulares tienen

acceso a ese medio y lo visitan con determinada frecuencia. En todo caso se debe atender al criterio de máximo alcance.

- Actualmente con los Lineamientos del Aviso de privacidad, publicados en el DOF el 17 de enero de 2013, se reconocen tres tipos de avisos de privacidad: el integral, el simplificado y el corto; en todos los cuales se deberá señalar con claridad, las finalidades del tratamiento de los datos personales.

Otro punto relevante en el apartado de principios, es la inclusión del criterio de minimización señalado dentro del principio de proporcionalidad, mediante el cual se establece la obligación al Responsable de realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento; por dicho contenido consideramos que este criterio debe ser considerado más bien, como otro de los principios que rigen el derecho a la protección de datos personales.

En el tema de medidas de seguridad, es donde se desarrolla la autorregulación, porque es a través de ella como el Responsable determina las medidas y los niveles de protección en función a los datos personales tratados, y que actualmente se encuentra regulada en los “Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares”, publicados en el DOF el 17 de enero de 2013.

En cuanto al Capítulo de las transferencias, se distinguen dos tipos, nacionales e internacionales, y es aquí donde surge la figura del receptor de datos personales, distinta al Responsable o Encargado de los datos personales, pero también con responsabilidades, por el sólo hecho de tratar los datos. En ello destaca también la autorregulación, en razón de que los miembros de un grupo o sector determinado, pueden establecer libremente su regulación en esta materia.

Finalmente en relación con la coordinación entre autoridades, establece la posibilidad de emitir o modificar regulación específica en esta materia, en caso de así requerirse en algún sector determinado, pudiendo el IFAI en todo momento hacer las propuestas correspondientes.

Consideramos que en general el Reglamento de la LFPDPPP es algo complejo y técnico, especialmente en esta primera parte, e incompleto o con lagunas en la parte relativa a los procedimientos, lo cual puede dar lugar a diversas interpretaciones o emisión de criterios probablemente contradictorios, que afecten en la adecuada aplicación de la LFPDPPP y su Reglamento, lo cual repercutirá finalmente en perjuicio del ejercicio del derecho de los titulares de datos personales,

motivo por el cual será necesario realizar una profunda revisión al momento de su aplicación a casos concretos, a fin de valorar su posible modificación o la emisión de uno nuevo.

6. Otras disposiciones

En este punto haremos una breve referencia del contenido de aquellas disposiciones que se han emitido en materia de protección de datos personales, en el ámbito federal, sólo como una pequeña muestra de la gran diversidad de disposiciones que existen al respecto y con el único propósito de evidenciar tal situación sin ser nuestro objetivo realizar un análisis detallado de las mismas, por lo cual sólo se mencionarán alguna de sus características. Previo a señalarlas, es importante recordar lo comentado líneas arriba en el análisis de la LFTAIPG, en cuanto a que no sólo existen ordenamientos aplicables para los sujetos obligados que forman parte de la Administración Pública Federal, sino también los emitidos por otros órganos de gobierno federales en su carácter de sujetos obligados, como son los Poderes Legislativo y Judicial, como se indica a continuación.

- **Lineamientos de Protección de Datos Personales emitidos por el Instituto Federal de Acceso a la Información Pública** (Lineamientos), fueron publicados en el DOF el 30 de septiembre de 2005 y modificados por acuerdo publicado en dicho Diario, el 17 de julio de 2006, y emitidos en cumplimiento a lo dispuesto en el artículo 47 del Reglamento de la LFTAIPG. Tienen por objeto, establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal, para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales.

De su contenido cabe destacar el establecimiento de las condiciones y los requisitos mínimos para el debido manejo de los sistemas y custodia de datos personales. Asimismo establece los principios rectores que aplican en la protección de datos personales consistentes en: licitud, calidad de datos, seguridad, custodia y cuidado de la información y consentimiento para la transmisión; también contempla dentro de dichos principios los de acceso y corrección; sin embargo, estos corresponden a derechos, los únicos que puede ejercer el titular de los datos personales ante los sujetos obligados de la Administración Pública Federal. Los Lineamientos otorgan facultades de supervisión al IFAI, a fin de verificar en sitio los sistemas de datos personales que operan cada dependencia y entidades de la Administración Pública Federal.

- **Lineamientos del Aviso de privacidad**, publicados en el DOF el 17 de enero de 2013 y entrarán en vigor el 17 de abril de 2013. Estos Lineamientos fueron emitidos por la Secretaría de Economía, para dar cumplimiento a lo dispuesto por el artículo 43 de la LFPDPPP, y establecer de manera más precisa, el contenido y alcance de los avisos de privacidad, de los que distingue tres tipos: el integral, el simplificado y el corto.

- **Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares** (Parámetros), publicados en el DOF el 17 de enero de 2013, y los cuales entraron en vigor al día siguiente de su publicación. En dichos Parámetros destaca la posibilidad de que los Responsables o encargados se adhieran voluntariamente a esquemas de autorregulación vinculante y puedan obtener una certificación total o parcial, otorgada por certificadores acreditados por el IFAI. Esta certificación determinará la conformidad de tratamientos, políticas, programas, procedimientos y demás normatividad aplicable en materia de protección de datos personales, estándares y mejores prácticas, o en su caso con principios, deberes u obligaciones específicos, que desarrollen o promuevan personas físicas o morales en esta materia, a fin de armonizar el tratamiento de los datos personales, facilitar el ejercicio de los derechos de los titulares y favorecer el cumplimiento a la LFPDPPP y su Reglamento.

- **Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de la Cámara de Diputados**, fue publicado en el DOF el 6 de abril de 2009, tiene entre otros objetos, el garantizar la protección de los datos personales en la Cámara de Diputados, de conformidad con los principios y criterios establecidos en la Constitución Política de los Estados Unidos Mexicanos y la LFTAIPG.

Dentro de los puntos relevantes destacan la inclusión de un banco de datos personales integrado por información recabada periódicamente y el reconocimiento de ocho derechos a favor de los titulares de los datos personales, dentro de los cuales se encuentran el derecho a otorgar los datos; negarse a otorgarlos; ser informados de su inclusión en otra fuente; ratificarlos; y los cuatro derechos ARCO. No obstante lo anterior, cuando se refiere al ejercicio de los derechos por parte de su titular, sólo contemplan los derechos ARCO. Otro punto a destacar es el que se refiere a la supresión total y definitiva de las bases de datos, cuando dejen de ser necesarios o pertinentes para la finalidad para la cual hubieren sido recabados, considerando la figura del “bloqueo”, como plazo para hacer aclaraciones y determinar responsabilidades, situación no considerada en la LFTAIPG.

- **Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental**, fue aprobado el 30 de marzo de 2004 y publicado en el DOF el 2 de abril de ese mismo año; fue reformado por Acuerdo del 14 de noviembre de 2007, publicado en el DOF el 12 de diciembre de ese año. Su objeto es establecer criterios, procedimientos y órganos para garantizar el acceso a la información en posesión de la SCJN, del Consejo de la Judicatura Federal, de los Tribunales de Circuito y de los Juzgados de Distrito, dentro de los cuales se encuentran también disposiciones relativas al derecho a la protección de datos personales.

De acuerdo con este Reglamento, en principio la información bajo su resguardo podrá ser consultada por cualquier persona, sin embargo, las partes involucradas en los procedimientos ante los órganos jurisdiccionales podrán oponerse a la publicación de sus datos personales, cuando se presente una solicitud de acceso a resoluciones públicas, pruebas o demás constancias que obren en el expediente respectivo; en este caso se deberá generar una versión pública de las resoluciones requeridas suprimiendo el nombre de las partes, así como cualquier información de carácter personal que contengan. Se aclara que los datos sensibles siempre serán suprimidos aún y cuando no se hayan opuesto las partes. El Reglamento contempla los derechos ARCO y la solicitud de información por parte del representante de la sucesión para el supuesto de personas fallecidas.

- **Acuerdo General de la Comisión para la Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales de la Suprema Corte de Justicia de la Nación**, su denominación es “Acuerdo General de la Comisión para la Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales de la Suprema Corte de Justicia de la Nación, del nueve [diez] de julio de dos mil ocho, relativo a los órganos y procedimientos para tutelar en el ámbito de este Tribunal los derechos de acceso a la información, a la privacidad y a la protección de datos personales garantizados en el artículo 6o. constitucional”, fue publicado en el DOF el 15 de julio de 2008, y en él se regula de manera amplia, el derecho a la protección de datos personales en su Título Quinto “Del tratamiento y protección de los datos personales”, dentro del cual se establecen las condiciones y requisitos mínimos para la debida administración y custodia de los datos personales, a fin de garantizar a los gobernados el derecho de decidir sobre su uso y destino, así como asegurar el adecuado tratamiento.

Es de llamar la atención que se considera como dato personal, la información concerniente a personas morales, identificadas o identificables, situación no contemplada en la LFTAIPG. En cuanto a los principios rectores de este derecho señala el de licitud, calidad, información, seguridad y consentimiento. Además

contempla el procedimiento de acceso, rectificación, cancelación u oposición de publicación de datos personales, aunque este último derecho está limitado únicamente para la publicación de los datos. Las solicitudes podrán ser presentadas por el interesado, sus tutores, curadores y sucesores, por sí o por medio de apoderado, para todos los derechos ARCO, en caso de fallecer el titular.

Finalmente es relevante mencionar que en contra de la negativa de todo o parte de la solicitud o por no resolver en el plazo respectivo, se podrá promover el *habeas data*, donde es posible establecer como medida preventiva, el bloqueo provisional del archivo cuando sea manifiesto el carácter discriminatorio, falso e inexacto de la información de que se trate.

Ahora bien, existe legislación a nivel federal que, desde antes de las reformas constitucionales antes citadas e incluso de la emisión de la LFTAIPG y la reciente LFPDPPP, ya regulaban dentro de sus propias materias, la protección de datos personales, mismas que a continuación serán señaladas igualmente con el único objetivo de conocerlas, pues en el ámbito de su competencia, también podrán ser aplicadas en la protección de datos personales, como se observa a continuación:

- El **Código Civil Federal** contempla en su Capítulo XI, la rectificación, modificación y aclaración de las actas del Registro Civil, donde evidentemente constan datos personales. La indemnización por causar un daño moral por afectación entre otros al honor y a la vida privada, se regula en los artículos 1910 y 1916.
- El **Código Penal Federal** regula en el Título Noveno, el delito de revelación de secretos (obtenidos con motivo del empleo, cargo o puesto, secreto industrial, o información obtenida en comunicaciones privadas) y acceso ilícito a sistemas y equipos de informática (incluye la modificación, destrucción o pérdida de la información, o que sin autorización o indebidamente conozca, obtenga o copie información contenida en sistemas o equipos del Estado o del sistema financiero).
- El **Código Fiscal de la Federación** señala en su artículo 69 que el personal oficial que interviene en los diversos trámites relativos a la aplicación de las disposiciones tributarias, estará obligado a guardar absoluta reserva en las declaraciones y datos suministrados por los contribuyentes o por terceros relacionados con ellos, así como los obtenidos en el ejercicio de las facultades de comprobación.
- La **Ley de Protección y Defensa al Usuario de Servicios Financieros** establece en sus artículos 13, 14 y 15 que la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros debe guardar estricta reserva sobre la información y documentos que conozca con motivo de su objeto, salvo que sea solicitada por autoridad judicial.

Los servidores públicos de la Comisión, serán responsables por violación de la reserva o secreto; por lo que tanto la Comisión como sus servidores públicos deberá reparar los daños y perjuicios que causen en caso de revelación del secreto bancario, fiduciario o bursátil.

- La **Ley de Seguridad Nacional** regula en su Título Quinto, la protección de los derechos de las personas, en donde señala en su artículo 64 que: "En ningún caso se divulgará información reservada que, a pesar de no tener vinculación con amenazas a la Seguridad Nacional o con acciones o procedimientos preventivos de las mismas, lesionen la privacidad, la dignidad de las personas o revelen datos personales".
- La **Ley de Vías Generales de Comunicación** establece en su artículo 383, la obligación de empleados y funcionarios de comunicaciones eléctricas, dedicados al servicio, a guardar secreto absoluto y riguroso en el contenido de mensajes y a no dar ningún informe en relación con los mismos, bajo pena de ser sancionados.
- La **Ley del Sistema Nacional de Información Estadística y Geográfica** señala en relación con los informantes del sistema que su información será considerada como confidencial y no podrá ser utilizada para otro fin que no sea el estadístico, para ello hará uso de la disociación, por la cual no es posible identificar, a través de los datos, a una persona. En su artículo 41 contempla el ejercicio del derecho de rectificación de datos.
- La **Ley Federal de Protección al Consumidor** establece en su artículo 16 la obligación de empresas y proveedores de mantener informados a los consumidores de información que de ellos han obtenido, principalmente con fines mercadotécnicos o publicitarios, así como permitirles el acceso a la misma, y en su caso su corrección, además debe informar de su transmisión a terceros. En el artículo 17 señala el derecho del consumidor a solicitar no ser molestado con publicidad en su domicilio, trabajo o dirección electrónica y no sean transmitidos sus datos a terceros.
- La **Ley Federal de Telecomunicaciones** señala en su artículo 49 que la información transmitida a través de redes y servicios de telecomunicaciones será confidencial, salvo que sea pública o medie orden de autoridad competente. La intercepción de información será sancionada (artículo 71 fracción V).
- La **Ley Federal de los Derechos del Contribuyente** dentro de los derechos del contribuyente que se regulan en este ordenamiento legal se encuentra el derecho al carácter reservado de los datos, informes o antecedentes que de los contribuyentes y terceros con ellos relacionados, conozcan los servidores públicos de la administración tributaria (Artículo 2, fracción VII). Por otra parte regula el derecho de acceso al establecer en su artículo 3 que los contribuyentes podrán acceder a los registros y documentos que forman parte de un expediente abierto a su nombre y

obre en los archivos administrativos correspondientes a procedimientos terminados. Y para efectos de los datos estadísticos sobre el ingreso, impuestos, deducciones y otros datos relevantes de los contribuyentes que el Servicio de Administración Tributaria informa al Instituto Nacional de Estadística, Geografía e Informática, el artículo 10 señala que se deberá respetar la confidencialidad de los datos individuales.

- La **Ley Federal del Derecho de Autor** en relación con el retrato de una persona estipula en su artículo 87 que sólo podrá ser usado o publicado, con su consentimiento expreso, excepto cuando recibe a cambio una remuneración, cuando el retrato de la persona forme parte menor de un conjunto de la fotografía, o ésta haya sido tomada en un lugar público y con fines informativos o periodísticos. El utilizar la imagen de una persona sin su autorización, constituye una infracción en materia de comercio (Artículo 231, fracción II). No son materia de reserva de derechos, los títulos, nombres, denominaciones, características físicas o psicológicas que incluyan el nombre, seudónimo o imagen de una persona, sin su consentimiento expreso (Artículo 188, fracción I, inciso e)). Por otra parte, de acuerdo con su artículo 109, para llevar a cabo el acceso a la información de carácter privado que consta en bases de datos, así como su publicación, reproducción, divulgación, comunicación pública y transmisión de dicha información, se requiere de la autorización previa de las personas.
- La **Ley General de Salud**, en general toda la información relacionada con la salud de una persona, será considerada como dato sensible, por tanto exige confidencialidad, protección y reserva para su uso y tratamiento; como en el tratamiento de datos genéticos (artículo 103 Bis 3), así como en la donación y trasplantes de órganos (artículo 314 Bis 1).
- La **Ley para regular las Sociedades de Información Crediticia** en su artículo 28, último párrafo señala que las sociedades, sus empleados y funcionarios tienen prohibido proporcionar información relativa a datos personales de los clientes para comercialización de productos o servicios, con la salvedad de la revisión del historial crediticio; quien contravenga dicha disposición incurrirá en el delito de revelación de secretos (artículo 210 del Código Penal Federal). Además regula las bases de datos que se conforman con información crediticia.

Con estas disposiciones y las antes analizadas en el presente Capítulo, todas relativas a la protección de datos personales en el sistema jurídico mexicano, podemos llegar a las siguientes reflexiones:

- Las disposiciones analizadas sólo representan una muestra de la diversidad de disposiciones que existen a nivel federal y estatal, en materia de protección de datos personales, lo cual es evidencia de la existencia de un sinnúmero de criterios, principios y mecanismos aplicables para su regulación.
- Esta multiplicidad de disposiciones es causada principalmente, porque el derecho a la protección de datos personales en posesión de entes públicos, se encuentra regulado en las leyes de transparencia y acceso a la información, materia que al ser concurrente es regulada a nivel federal y estatal, sin lograr una protección uniforme.
- El hecho de regular de manera distinta, a través de legislaciones diversas, el derecho a la protección de datos personales que están en poder de entes públicos y los que se encuentran en poder de entes privados, pareciera referir a dos derechos distintos, sin embargo ello no es así, toda vez que la Constitución Política de los Estados Unidos Mexicanos garantiza un derecho fundamental, sin división alguna, el cual debe ser regulado, con sus excepciones, en una sola ley de la materia. En consecuencia, el argumento para llevar a cabo dicha separación, no tiene sustento constitucional, por lo que ambos debieran ser regulados en una misma disposición legal. Ahora bien, el argumento para disgregar este derecho, basado en que los fines de los particulares son de comercio y los de entes públicos no, carece de todo valor al establecerse en los artículos 18 fracción II y 21 de la LFTAIPG, la posibilidad de que las dependencias y entidades públicas puedan comercializar los datos personales.
- Algunas disposiciones son completas, desarrolladas e innovadoras en la materia de protección de datos personales, pero otras resultan ser tan sólo una reproducción de las existentes, por lo que no hay homogeneidad en la regulación de este derecho y por ende, en los niveles de protección.
- Existen materias especializadas como la fiscal, financiera, derechos de autor, protección al consumidor, entre otras, que también otorgan cierta protección a los datos personales, lo cual permite una mejor salvaguarda de este derecho, y la posibilidad de llevar procedimientos y, en su caso, aplicación de sanciones, en forma paralela, pues cada autoridad actuará conforme a su ámbito de competencia, aunque también es relevante que exista la coordinación entre las mismas. Al ser este un modelo sectorial, puede representar ciertas desventajas al momento de la actualización de la normatividad aplicable, por lo cual es recomendable llevar a cabo su revisión detallada, a fin de conocer si se encuentra conforme o no, con las nuevas disposiciones emitidas en la materia.
- En las disposiciones analizadas se observaron algunos aspectos útiles que fueron destacados en cada una de ellas y los cuales serán más adelante retomados para incluirlos en las propuestas de reformas legales o incluso constitucionales, que se realicen en el último capítulo de este trabajo.

De esta manera, el estudio realizado al marco jurídico del sistema jurídico mexicano permitió observar la diversidad de criterios y procedimientos que existen para ejercer el derecho a la protección de datos personales e incluso en algunos casos a través del *habeas data* (considerado sólo como un procedimiento administrativo), y con ello la pluralidad de autoridades, plazos y recursos existentes. Sin embargo, dicha complejidad de procedimientos permitirá su contrastación con los establecidos en la LFPDPPP y la LFTAIPG, los cuales serán sujetos de un análisis detallado en el siguiente capítulo, a fin de entender la importancia de contar con un procedimiento ágil, claro y sencillo, para los titulares de datos personales en el ejercicio adecuado de sus derechos ARCO, y que redundará en una mayor certeza y seguridad jurídica en la protección de sus datos personales. De ahí que consideramos al procedimiento como el elemento medular en la protección de datos personales, por tratarse del medio con el que cuenta el titular para la defensa y ejercicio de sus derechos.

CAPÍTULO TERCERO
PROCEDIMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES A NIVEL FEDERAL

I. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO).

El ejercicio de los derechos ARCO es el primero, y en algunos casos (cuando es atendida debidamente la solicitud del titular), el único procedimiento que el titular de los datos personales lleva a cabo para ejercer su derecho a la autodeterminación informativa. Es un procedimiento que se caracteriza por llevarse entre el titular y el Responsable sin intervención de la autoridad, a menos que el Responsable impida el ejercicio de los derechos ARCO, al no recibir la solicitud del titular, no darle respuesta en el plazo estipulado en la ley de la materia, negarle los derechos ARCO o darle una respuesta incomprensible o incompleta.

Como señalamos en el capítulo anterior, la protección de los datos personales y los derechos de acceso, rectificación, cancelación y oposición, se encuentran regulados en el artículo 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, y el ejercicio de cualquiera de estos derechos no es requisito previo ni impide el ejercicio de otro. Los derechos ARCO son la forma como se ejercerá el derecho fundamental de la protección de los datos personales, y se encuentran regulados a nivel federal, en la LFPDPPP y en la LFTAIPG. Al respecto, recordemos como en el capítulo anterior se hizo una crítica a esta última ley, por contemplar únicamente dos derechos, el de acceso y el de rectificación, con lo cual no sólo se limita este derecho fundamental sino también impide su adecuada salvaguarda, en la forma estipulada por aquél precepto constitucional.

En este sentido, es incomprensible que en el caso del tratamiento de datos personales, por parte de entes públicos de la Administración Pública Federal, no puedan ejercerse ciertos derechos ARCO, cuando en diversas legislaciones de entidades federativas ya están incorporados y operando, incluso en las disposiciones emitidas por la SCJN y la Cámara de Diputados antes analizadas, se encuentran previstos dichos derechos, lo cual es una evidencia más de la incongruencia y heterogeneidad en la materia, ocasionada en gran medida, por la existencia de diversa regulación.

Por otra parte, el ejercicio de los derechos ARCO se da como consecuencia del derecho a la autodeterminación informativa que tiene toda persona para cuidar, controlar y mantenerse informado de los datos personales obtenidos y tratados por entes públicos o privados, a través del cual puede impedir el tratamiento de sus datos personales, sin antes contar previamente con la información necesaria

para emitir su consentimiento. Así afirmamos que cada titular es quien determina, en primer lugar, el nivel de seguridad y control que quiere darle a sus datos personales, pues sólo él decidirá a quién y para qué los proporcionará. Por esta razón el requisito básico para que el titular ejerza sus derechos ARCO es la acreditación previa de su identidad ante el Responsable, pues únicamente él o su representante podrán hacer valer estos derechos.

El derecho a la protección de datos personales no es un derecho absoluto o superior a otros derechos fundamentales, por tanto, tampoco lo serán los derechos ARCO. Al respecto, en materia de protección de datos personales en posesión de entes privados, las restricciones al ejercicio de estos derechos se encuentran señaladas de manera general, en el artículo 88 del Reglamento de la LFPDPPP, las cuales pueden ser por razones de: "… seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, o bien mediante resolución de la autoridad competente debidamente fundada y motivada".

Como se mencionó en el anterior capítulo, dichas excepciones debieron haber sido establecidas de manera precisa en LFPDPPP y no en su Reglamento, a fin de dar cumplimiento a lo dispuesto en el artículo 16 de la Carta Magna, el cual dispone que la ley "… establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos …", ello ante la posibilidad de que el derecho a la protección de datos personales se encuentre en contraposición con otros derechos, en donde deberá prevalecer el bien común. Sin embargo, en la LFPDPPP sólo se mencionan de manera general, los siguientes supuestos de excepción en las materias antes citadas, en sus artículos 10, fracciones V, VI y VII (en cuanto al consentimiento para el tratamiento de datos personales), 26, fracciones II, III, V y VII (para negar la cancelación de datos) y 34, fracciones III y IV (para negar los derechos ARCO):

- Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes (Artículo 10, fracción V).
- Sean indispensables para la atención médica, prevención, diagnóstico, prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar su consentimiento y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente (Artículo 10, fracción VI).
- Se dicte resolución de autoridad competente (Artículo 10, fracción V).

- Los datos se obtienen, usan, divulgan y almacenan, por disposición legal (Artículo 26, fracción II).[122]
- La cancelación de datos obstaculice actuaciones judiciales o administrativas, vinculadas a obligaciones fiscales, la investigación y persecución de delitos o actualización de sanciones administrativas (Artículo 26, fracción III).
- Los datos sean necesarios para realizar una acción en función del interés público (Artículo 26, fracción V).
- Los datos sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud (Artículo 26, fracción VII).
- Se lesionen los derechos de un tercero (Artículo 34, fracción III).
- Exista un impedimento legal o por resolución de autoridad competente que restrinja los derechos ARCO (Artículo 34, fracción IV).

En cuanto a la LFTAIPG no establece expresamente limitación alguna para el ejercicio de los derechos de acceso y rectificación de datos personales, tampoco supuestos de excepción específicos como ordena el artículo 16 constitucional, únicamente en el artículo 22 de la LFTAIPG, señala como excepciones al consentimiento para proporcionar datos personales, la emisión de una orden judicial y, en términos generales, para los demás casos remite a lo que establezcan otras leyes; por ello y a fin de brindar certeza en el ejercicio de los derechos ARCO, se sugiere incluir y regular de manera precisa los supuestos de excepción en la ley de la materia.

Ahora bien, para el ejercicio de los derechos ARCO será de gran importancia el aviso de privacidad que emita cada Responsable, el cual como se mencionó en el capítulo anterior, debe hacerse del conocimiento de los titulares previo al tratamiento de sus datos personales, así como cubrir ciertos requisitos mínimos que permitan la presentación de solicitudes de derechos ARCO[123] de

---

[122] Al respecto citamos como ejemplo, la permisión establecida en la Ley para Regular las Sociedades de Información Crediticia, a fin de que dichas sociedades recopilen, manejen y entreguen información relativa al historial crediticio de personas físicas y morales a Entidades Financieras, Empresas Comerciales y Sociedades Financieras de objeto múltiple no reguladas, conductas que no serán violatorias del Secreto Financiero, siempre y cuando se transmitan en los términos señalados por la ley de la materia.

[123] La LFPDPPP refiere a esta solicitud como “Solicitud de acceso, rectificación, cancelación u oposición” o “Solicitud de los titulares para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición”. En cambio el Reglamento hace referencia a la misma como: “Solicitud para el ejercicio de los derechos ARCO”, “Solicitud en ejercicio de los derechos de acceso, rectificación, cancelación u oposición”, “Solicitud para el acceso, rectificación, cancelación u oposición” y “Solicitud del ejercicio de los derechos ARCO”. Por lo tanto, al no existir uniformidad en los términos ni en la Ley y su Reglamento, para efectos prácticos en su referencia, en el presente trabajo se

manera ágil, clara y sencilla. Consideramos que el aviso de privacidad es el documento base de esta acción, sin el cual, independientemente de la falta cometida por el Responsable, se dejaría en estado de indefensión al titular, al no tener conocimiento previo de quién tratará sus datos personales, con qué finalidad serán tratados, si serán transferidos a Terceros y con qué medios cuenta para ejercer sus derechos ARCO.

De igual forma para entes públicos federales, en el artículo 20 fracción III de la LFTAIPG se establece la obligación a cargo de los sujetos obligados, para poner a disposición de los individuos, a partir del momento de recabar sus datos personales, el documento en el que establezcan los propósitos para su tratamiento; y si bien este documento no es denominado aviso de privacidad,[124] sí cumple con la misma finalidad, es decir brindar al titular la información necesaria, previo al tratamiento de sus datos personales. De acuerdo con lo dispuesto en el numeral Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el DOF el 30 de septiembre de 2005, las dependencias y entidades de la Administración Pública Federal, a través de formatos físicos o electrónicos, informarán al titular al momento de recabar sus datos personales, los que serán tratados, su fundamento legal, con qué finalidad y si serán transmitidos.

El mantener informado al titular a través del aviso de privacidad es una de las primeras y principales obligaciones que tiene el Responsable en el tratamiento de datos personales que se encuentra acorde con el principio de información, pero esta obligación no sólo se limita a su emisión y la forma o medio en que se hará del conocimiento del titular, sino también implica garantizar su cumplimiento. En este sentido, el artículo 14 de la LFPDPPP establece que el Responsable: "… deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica".

De esta manera, con la emisión del aviso de privacidad se garantiza, en cierta forma, que los datos personales no sean obtenidos a través de medios engañosos o fraudulentos, al señalar de manera clara y fehaciente la forma y el fin para el cual serán tratados, lo que implica una mayor seguridad y confianza para los titulares en el tratamiento de sus datos personales, al conocer previamente las

---

utilizará la denominación de "Solicitud de derechos ARCO" cuando se refiera al ejercicio en general de los derechos ARCO.

[124] Este documento que es emitido a través de formatos escritos o electrónicos por las dependencias y entidades de la Administración Pública Federal, no tienen ninguna denominación. De acuerdo con los Lineamientos citados los sujetos obligados podrán utilizar el modelo de leyenda señalado en su numeral Decimoctavo, que contiene la información básica a informar al titular al momento de recabar sus datos personales.

condiciones y términos de su uso. Es por ello que en el artículo 7, último párrafo de la LFPDPPP se habla de la “expectativa razonable de privacidad” entendida como “… la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes, en los términos establecidos por esta Ley”.

Así las cosas, el aviso de privacidad es como un contrato o acuerdo entre las partes, pues requiere de la emisión del consentimiento expreso o tácito, por parte del titular, condición necesaria para todo tratamiento de datos personales, salvo las excepciones establecidas en la ley, comentadas líneas arriba. El consentimiento podrá ser revocado en cualquier momento, de acuerdo con los mecanismos y procedimientos establecidos en el aviso de privacidad.

La omisión del aviso de privacidad, el no encontrarse de manera completa, establecerse de manera confusa, o simplemente incumplirlo en los términos ahí estipulados, puede provocar en el titular la desconfianza o inconformidad en el tratamiento de sus datos personales, lo cual manifestará a través del ejercicio de sus derechos ARCO ante el Responsable, ello sin menoscabo de la presentación de una denuncia ante el IFAI, por presuntas violaciones a la ley.

No obstante lo anterior, actualmente muchos Responsables no cuentan con avisos de privacidad en los términos establecidos en la LFPDPPP y su Reglamento, al omitir algunos datos o señalarlos de manera incompleta o confusa, o simplemente al carecer de ellos. Asimismo es de observarse la forma como los hacen del conocimiento del titular, al publicarlos en sus páginas de Internet sin cerciorarse que efectivamente lo conozcan los titulares, lo cual como se analizó en el capítulo anterior no es posible. De esta forma se considera que aún falta mucho por hacer en la materia y que se tendrá que trabajar intensamente en la capacitación y fomento de la cultura en la protección de datos para todos los sujetos involucrados.

Por otra parte, es importante mencionar que el ejercicio de los derechos ARCO no necesariamente deriva de una inconformidad sino también por fines meramente informativos, donde el titular mediante el ejercicio de su derecho de acceso, solicita al Responsable le informe qué datos personales tiene de él y, en su caso, las condiciones y términos con los cuales son tratados, como son las medidas de seguridad adoptadas por el Responsable para su protección y resguardo.

Cabe destacar lo dispuesto en el artículo 25, último párrafo de la LFPDPPP, en donde se indica que cuando el Responsable transmite a un Tercero datos personales, con anterioridad a la solicitud de los derechos de rectificación o cancelación presentada por un titular, el Responsable será quien avise al Tercero de estas acciones para que éste último a su vez, realice lo propio respecto de dichos

datos; luego entonces el titular no tendrá que presentar otra solicitud de rectificación o cancelación ante el Tercero a quien le fueron transmitidos sus datos, pero sí consideramos debe ser informado cuando esto sea realizado, aun y cuando dicha disposición no mencione expresamente esa obligación para el Tercero, pues se deberá brindar certeza al cumplimiento del derecho solicitado.

Ahora bien, antes de revisar cómo opera este procedimiento ante los sujetos obligados o Responsables, según sea el caso, es conveniente analizar cada uno de los derechos ARCO, a fin de conocer cómo son entendidos en la ley, sus alcances y límites en su ejercicio, lo cual se explica a continuación:

1. Significado, alcances y límites de los derechos ARCO.

En el dictamen de las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos de la Cámara de Senadores, emitido el 4 de diciembre de 2008, mediante el cual se aprobó el proyecto de Decreto que adiciona un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, se expone claramente en una de sus consideraciones, los motivos por los cuales se incluyeron los derechos ARCO en dicho artículo como parte del derecho fundamental a la protección de datos personales, principalmente por tratarse de derechos internacionalmente reconocidos en otros instrumentos, como lo es, la Directiva Europea 95/46 CE del 24 de octubre de 1995, así como por ser una forma de dotar al gobernado de un poder de disposición sobre sus datos personales. De esta manera fueron reconocidos constitucionalmente cuatro derechos para ser ejercidos por el titular de datos personales: acceso, rectificación, cancelación y oposición, conocidos como derechos ARCO.

A. Acceso

El artículo 24 de la LFTAIPG refiere al derecho de acceso de la siguiente manera: "… sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales…".

En similar sentido el artículo 23 de la LFPDPPP señala en relación con este derecho lo siguiente: "Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento". El Reglamento de la LFPDPPP amplía esa definición, pues además de lo anterior, incluye en su artículo 101, el derecho del titular a obtener del Responsable, cualquier información relativa a las condiciones y generalidades del tratamiento de sus datos personales, como son las medidas de seguridad con las que cuenta el Responsable para su protección.

Un requisito para ejercer el derecho de acceso, es que el “interesado” o titular, según sea el caso, o su representante legal, acrediten previamente su identidad, sin embargo como se mencionó en el análisis de la LFTAIPG realizado en el capítulo anterior, el uso del término “interesado” no implica que se trate necesariamente del titular de los datos personales sino de cualquier persona que demuestre tener un interés en el ejercicio de este derecho, por lo cual no se considera adecuado su uso, además de ser contrario a la naturaleza de la protección de datos personales concebida como un derecho personal. Este problema se subsana en el Reglamento de la LFTAIPG, donde en su artículo 76 hace referencia al término de “particulares titulares de los datos personales” en congruencia con este derecho.

Por otra parte, en ambas leyes la obligación de acceso a la información se da por cumplida por parte del Responsable o sujeto obligado, según sea el caso, cuando se pone a disposición del titular los datos personales o información (en el Reglamento de la LFPDPPP se aclara que dicha disposición es en sitio) previa acreditación de su identidad, o bien, cuando se le expidan las copias simples o documentos electrónicos solicitados. Esta entrega será gratuita, y el titular sólo cubrirá los gastos justificados de envío o por copias. La LFPDPPP también señala que la obligación se dará por cumplida cuando se le indique al titular que no cuenta con dicha información por no ser el Responsable, lo cual significa que éste tiene la obligación de brindar una respuesta a toda solicitud, aún cuando sea en sentido negativo.

La LFPDPPP establece que el Responsable podrá determinar cualquier otro medio para la entrega de la información en su aviso de privacidad, medios que detalla su Reglamento, como pueden ser los magnéticos, ópticos, sonoros, visuales u holográficos, o cualquier otra tecnología.

El derecho de acceso es donde podemos observar claramente el poder de disposición y control que tienen los titulares sobre sus datos personales, pues se traduce en el derecho del titular a estar debidamente informado respecto de sus datos, no sólo desde su inicio sino en cualquier momento y por el tiempo que dure su tratamiento por parte del Responsable. En el aviso de privacidad el Responsable debe señalar la siguiente información básica y general: quién, cómo, dónde y para qué tratan los datos personales; sin embargo cuando dicha información no es clara o suficiente, ha sido modificada, o simplemente quiere conocerse de manera particular, el titular a través del derecho de acceso podrá solicitar le sea proporcionada, lo cual le permitirá tener un mayor control sobre sus datos.

B. Rectificación

La LFTAIPG regula el derecho de rectificación en su artículo 25 al señalar que: “Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifique sus datos que obren en cualquier sistema de datos personales…”.

Por su parte el artículo 24 de la LFPDPPP establece en relación con el derecho de rectificación: “El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos”. El artículo 103 del Reglamento de la LFPDPPP se limita a reiterar lo ya señalado por la ley, pero en su artículo 104 establece tres requisitos para su ejercicio que son: 1) identificar los datos motivo de la rectificación, 2) especificar la corrección que se solicita y 3) acompañar la documentación que ampare la solicitud. No obstante lo anterior, permite que el Responsable pueda establecer mecanismos que faciliten el ejercicio de este derecho en beneficio del titular, lo cual pudiera interpretarse como una posibilidad para sustituir u omitir algunos de los requisitos antes señalados.

La viabilidad del derecho de rectificación, no debe subsanar en modo alguno, la obligación del Responsable para mantener sus bases con datos personales exactos, completos, pertinentes, correctos y actualizados, tal y como lo exige el principio de calidad; por lo cual consideramos que los errores u omisiones en las bases atribuibles a ellos, deben ser debidamente sancionados, independientemente de haber atendido la rectificación solicitada por el titular, pues es su obligación adoptar los mecanismos necesarios para contar con información veraz, a fin de no provocar consecuencia alguna en perjuicio del titular.

C. Cancelación

En cuanto a la cancelación, la LFPDPPP establece en su artículo 25 que: “El titular tendrá en todo momento el derecho a cancelar sus datos personales”; según su Reglamento, la cancelación implica el cese en el tratamiento por parte del Responsable, cuando el titular considera que sus datos no están siendo tratados conforme a los principios y deberes establecidos en la LFPDPPP y su Reglamento. Asimismo, considera la posibilidad de realizar una cancelación sobre la totalidad de los datos o sólo respecto de parte de ellos.

El Reglamento de la LFPDPPP aclara que la supresión de datos no es inmediata, pues para ello será necesario que se dé primero un periodo de bloqueo de los mismos, con el propósito de determinar posibles responsabilidades, el cual será equivalente al plazo de prescripción legal o contractual que corresponda. Durante el bloqueo no será posible tratar o tener acceso a los datos personales, salvo las

acciones que sean necesarias para su almacenamiento. Concluido el periodo de bloqueo se procederá a la cancelación, misma que se deberá comunicar al titular.

Este derecho es el único que tiene excepciones específicamente señaladas en la LFPDPPP en su artículo 26,[125] algunas de ellas ya vistas en las excepciones generales a la ley, de la primera parte de este capítulo. En dicho artículo se establece que el Responsable no tiene obligación de cancelar los datos cuando:

1) Se refieran a datos de un contrato privado, social o administrativo, y sean necesarios para su desarrollo y cumplimiento.
2) Los datos deban ser tratados (uso, divulgación o almacenamiento) por disposición legal.
3) Obstaculice actuaciones judiciales o administrativas.
4) Sean necesarios para proteger los intereses jurídicamente tutelados del titular.
5) Sean necesarios para realizar una acción en función del interés público.
6) Sean necesarios para cumplir con una obligación legalmente adquirida por el titular.
7) Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud.

Estas excepciones serán entonces el límite para la cancelación de datos personales, pero no sólo para el titular en el ejercicio de su derecho, sino también para el Responsable, quien previo a realizar cualquier cancelación de datos, tiene la obligación de cerciorarse de no estar en presencia de alguno de estos supuestos de ley.

Por otra parte, el derecho de cancelación está estrechamente vinculado con el principio de finalidad, el cual consiste en señalar de manera clara y sin lugar a confusión, el objeto determinado y específico del tratamiento de los datos personales, el cual al concluir, cumplirse o dejar de ser necesario, dará lugar a la cancelación. El tratamiento de datos personales puede tener diversas finalidades[126], pero las que dieron origen y fueron necesarias para la relación jurídica entre el titular y el Responsable, son las únicas causantes de la cancelación de datos al ser satisfechas.

---

125 El artículo 34 de la LFPDPPP establece en forma genérica la no procedencia de los derechos ARCO.

126 Es importante mencionar que todas las finalidades existentes en el tratamiento de datos personales deben ser compatibles o análogas con las finalidades originarias y que fueron previstas en el aviso de privacidad.

Otra forma en la que procede la cancelación es a través del incumplimiento de las obligaciones contractuales, motivo del tratamiento de los datos personales, en cuyo caso la LFPDPPP establece en su artículo 11, la obligación del Responsable de eliminar los datos una vez que transcurra un plazo de setenta y dos meses, contado a partir del referido incumplimiento, lo cual implica la procedencia de la cancelación, sin necesidad de que el titular ejerza directamente este derecho. Por lo anterior y aunque la ley no lo señale expresamente, el plazo antes referido equivale al periodo de bloqueo de los datos.

La cancelación tendrá primero el efecto de suspender el tratamiento de los datos por parte del Responsable y después la supresión o acción de eliminar, borrar o destruir los datos personales bajo las medidas de seguridad correspondientes.

Ahora bien, la ley no prohíbe que el Responsable cancele los datos personales sin mediar solicitud por parte del titular, a quien en su caso, sólo le deberá avisar que ha realizado la cancelación. Incluso el artículo 37 del Reglamento de la LFPDPPP señala que al cumplirse los plazos de conservación de los datos personales,[127] el Responsable debe proceder a la cancelación, previo bloqueo de los datos para su posterior supresión. En ese sentido, el Responsable puede cancelar de manera oficiosa los datos, sin ser violatorio del derecho del titular, en virtud de que se han cumplido o concluido las finalidades para su tratamiento, además debemos recordar que la cancelación no equivale a eliminación, pues previo a realizar dicha acción se dará un periodo de bloqueo de los datos personales, el cual al concluir debe también ser comunicado al titular, pues es cuando se procederá a la eliminación definitiva de los datos.

Como podemos observar, este derecho no concluye con el sólo aviso al titular de la cancelación, sino termina con la eliminación total o parcial, según se haya solicitado, de los datos personales. Pero la LFPDPPP y su Reglamento no contemplan la forma cómo el Responsable acreditará la eliminación de los datos personales de sus bases de datos, lo cual lleva a cuestionar si realmente se logra garantizar, de manera efectiva, el derecho de cancelación y con éste el de protección de los datos personales.

Por lo anterior, debe ser obligación del Responsable establecer los mecanismos necesarios para garantizar al titular la eliminación definitiva de sus

[127] De acuerdo con el artículo 37 del Reglamento de la LFPDPPP, los plazos de conservación de los datos personales serán aquellos necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, atiendan las disposiciones aplicables de la materia de que se trate y tomen en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

bases de datos,[128] a fin de que pueda cerciorarse de manera plena y con certeza de la realización de dicha acción y, en caso contrario, pueda solicitar la intervención del Instituto para garantizar su derecho, so pena en caso de observar algún incumplimiento a la ley, de iniciar un procedimiento de imposición de sanciones en contra del Responsable, por continuar con el uso ilegítimo de los datos personales.

Por otra parte, resulta de interés exponer una conducta social actual que tiene un impacto directo con este derecho, consistente en la entrega de datos personales a entes públicos o privados con el propósito de iniciar una relación jurídica, la cual por diversas circunstancias no llega a concretarse. Tal es el caso de la entrega de solicitudes de empleo, [129] crédito, citas médicas, cotizaciones, incorporación a clubes, asociaciones o escuelas, entre otras, en las cuales el titular de los datos proporciona diversa información personal, con el fin de obtener un servicio o beneficio, sin embargo puede suceder que la relación jurídica no se dé, y los datos quedan en manos de dichos entes.

En esos supuestos, proponemos la cancelación y eliminación inmediata de los datos, si así lo solicita su titular, pues no se justifica un periodo de bloqueo equivalente a la prescripción de acciones, en virtud de que no surgió ninguna relación jurídica entre el Responsable y el titular. Además, en dichos casos la finalidad no llega a concretarse o es incierta, porque está supeditada al cumplimiento de diversos requisitos, perfiles, necesidades y otros elementos o circunstancias a veces ajenos a los propios Responsables y titulares.

También es relevante mencionar que una proyección de este derecho y el de oposición, es el llamado derecho al olvido, el cual no está expresamente regulado en la LFPDPPP ni en su Reglamento, sin embargo se considera importante su inclusión, aun y cuando se encuentre regulado en otros ordenamientos legales, en razón que no se prevé como un derecho de cancelación a ejercer por el titular. El sector donde generalmente opera este derecho es el financiero, en donde es regulado en el artículo 23 de la Ley para Regular las Sociedades de Información

---

[128] Un ejemplo de la eliminación definitiva es la que anunció el director general del corporativo URIOS, Gerardo Galicia Amor, quien señaló que esa empresa está a cargo del "Primer Laboratorio Nulificador de Archivo Muerto Informático" en México, el cual a través del uso de tecnología avanzada, permitirá la destrucción completa de los datos almacenados en un dispositivo electrónico, garantizando la eliminación certificada de la información sensible y confidencial. Información disponible en http://www.vanguardia.com.mx/promueventecnologiaparaeliminarensutotalidadarchivosdigitales-1361370.html, consultada el 9 de septiembre de 2012.

[129] De acuerdo con lo dispuesto en el artículo 5 fracción II, la información relativa a personas físicas en su calidad de comerciantes y profesionistas no serán objeto de aplicación de las disposiciones del Reglamento. Sin embargo, no se establecen como excepción de aplicación de la ley.

Crediticia, el cual establece que después de setenta y dos meses de darse el cumplimiento de cualquier obligación, dichas sociedades podrán eliminar la información correspondiente del historial crediticio, salvo las excepciones señaladas en su artículo 24 (cuando el monto adeudado rebase el establecido en la ley o cuando exista sentencia firme por el delito patrimonial intencional relacionado con el crédito).

D. Oposición

El dictamen del 4 de diciembre de 2008 emitido por las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos de la Cámara de Senadores, citado líneas arriba, señala que el derecho de oposición surgió en el derecho francés, como una facultad que tiene el individuo para manifestar su conformidad al tratamiento de sus datos personales obtenidos de fuentes accesibles al público para fines de publicidad. Asimismo destaca que este derecho funciona como una herramienta para impugnar los efectos jurídicos de las denominadas “decisiones individuales automatizadas”, las cuales consisten en un tratamiento automatizado de datos personales para evaluar ciertos aspectos relativos a la personalidad de los individuos, con los cuales se pueden obtener perfiles bien definidos, útiles para fines mercadotécnicos o publicitarios.

El ejercicio del derecho de oposición ha operado desde antes de la emisión de la LFPDPPP, a través del Registro Público de Consumidores y del Registro Público de Usuarios, previstos en los artículos 18 y 18 BIS de la Ley Federal de Protección al Consumidor y 8o. de la Ley de Protección y Defensa al Usuario de Servicios Financieros, respectivamente, los cuales consisten en padrones de consumidores o usuarios del sistema financiero mexicano, según sea el caso, que manifiestan su negativa en recibir publicidad o promociones con fines de mercadotecnia o publicidad.

Independientemente de la existencia de dichos registros y sin menoscabo que el titular pueda hacer uso de los mismos, la LFPDPPP contempla la posibilidad que los Responsables cuenten con listados de exclusión propios o comunes, por sectores o generales, en donde el titular también pueda inscribirse, en cuyo caso el Responsable deberá otorgarle una constancia de su inscripción.

El derecho de oposición se explica en el artículo 27 de la LFPDPPP de la siguiente manera: “El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular”.

Al respecto, el Reglamento de la LFPDPPP establece en su artículo 109 dos supuestos por los cuales el titular podrá oponerse al tratamiento o a exigir su cese:

- Para evitar que la persistencia en su tratamiento cause un perjuicio al titular, debe existir una causa legítima y justificarse el motivo por el cual se solicita el cese.
- Para que no se lleve a cabo el tratamiento para fines específicos, lo cual podría interpretarse como una oposición parcial al tratamiento de sus datos.

Este derecho está relacionado con el principio de finalidad, toda vez que si ésta es contraria a la establecida en el aviso de privacidad, el titular podrá negar o revocar su consentimiento o ejercer su derecho de oposición. Por lo anterior también tiene un vínculo estrecho con el principio de consentimiento, el cual es necesario para cualquier tratamiento de datos por parte de los Responsables. El consentimiento debe referirse a una finalidad o finalidades determinadas, por lo tanto en caso de considerarse las transferencias nacionales o internacionales, será necesario obtener el consentimiento previo del titular, a través de una cláusula donde se indique su aceptación o no a las mismas, ello de conformidad con lo dispuesto en el artículo 36, segundo párrafo de la LFPDPPP.

En ese mismo sentido, debería obtenerse el consentimiento del titular para el caso de transferencias entre sociedades integrantes del mismo grupo del Responsable, sin embargo el artículo 37 fracción III de la LFPDPPP lo exceptúa. Al respecto, consideramos inadecuada esta excepción, toda vez que el hecho de pertenecer a un mismo grupo comercial no implica que todas las sociedades tendrán idéntica o similar finalidad para el tratamiento de los datos personales. Por ejemplo si el titular emite su consentimiento para el tratamiento de sus datos, a fin de que una empresa le proporcione el servicio de telefonía celular, y ésta transfiere a su vez los datos a una asegurada, porque se encuentra dentro del grupo comercial del Responsable, ésta podrá, con fundamento en la referida disposición, hacer uso de los datos personales sin necesidad de recabar el consentimiento de su titular, sin embargo la finalidad que tiene la aseguradora es totalmente distinta a la originaria que tiene el Responsable, a quien se le otorgó el consentimiento.

Por lo anterior, proponemos eliminar de las excepciones al consentimiento, contempladas en el referido artículo 37 de la LFPDPPP, la relativa a esas sociedades de un mismo grupo comercial, a fin de que estén obligados también a recabar, previo a cualquier transferencia, el consentimiento del titular. Con lo anterior, se evitarán las prácticas comerciales que algunos grupos realizan para incluir de manera irregular, la contratación de otros servicios no solicitados por el

titular o envío de publicidad sin su conocimiento informado. Además que el titular podrá conocer con certeza quien es el Responsable de sus datos personales, pues de otra manera, se crea una confusión respecto del sujeto que trata sus datos, lo cual se convierte en un obstáculo para el control y seguimiento de sus datos personales.

La adquisición y desarrollo de una cultura en la protección de datos personales en la sociedad mexicana, permitirá especialmente que los titulares tomen consciencia en la protección de sus datos personales mediante el control adecuado e informado de su tratamiento, por tratarse no solo de una prerrogativa sino también de una obligación a ejercer de manera responsable.

2. La protección de datos personales en el ejercicio de los derechos ARCO.

Las solicitudes de derechos ARCO pueden ser presentadas por los titulares, según quien posea sus datos personales, ante entes públicos,[130] en cuyo caso el procedimiento estará regulado por la LFTAIPG o, ante entes privados donde el procedimiento se establecerá en la LFPDPPP, como se explica a continuación.

A. Entes públicos.

Para promover las solicitudes de acceso o corrección de datos personales ante las unidades de enlace o su equivalente de los entes públicos, los particulares titulares de los datos personales o sus representantes deberán acreditar previamente su personalidad. Los plazos que se establecen para estos procedimientos serán improrrogables y máximos, en los cuales se incluirán las notificaciones al solicitante. Es importante mencionar que los Comités de Información de cada dependencia o entidad, sujetándose a estos plazos máximos, podrán establecer sus propios plazos y procedimientos internos para el desahogo de las solicitudes.

El procedimiento para el ejercicio del derecho de acceso, establecido en los artículos 24 de la LFTAIPG y 76, 77 y 78 de su Reglamento, se desarrolla de la siguiente manera:

[130] Los entes públicos referidos en este capítulo corresponden a las dependencias y entidades de la administración pública federal, regulados para efectos de la protección de datos personales por la LFTAIPG.

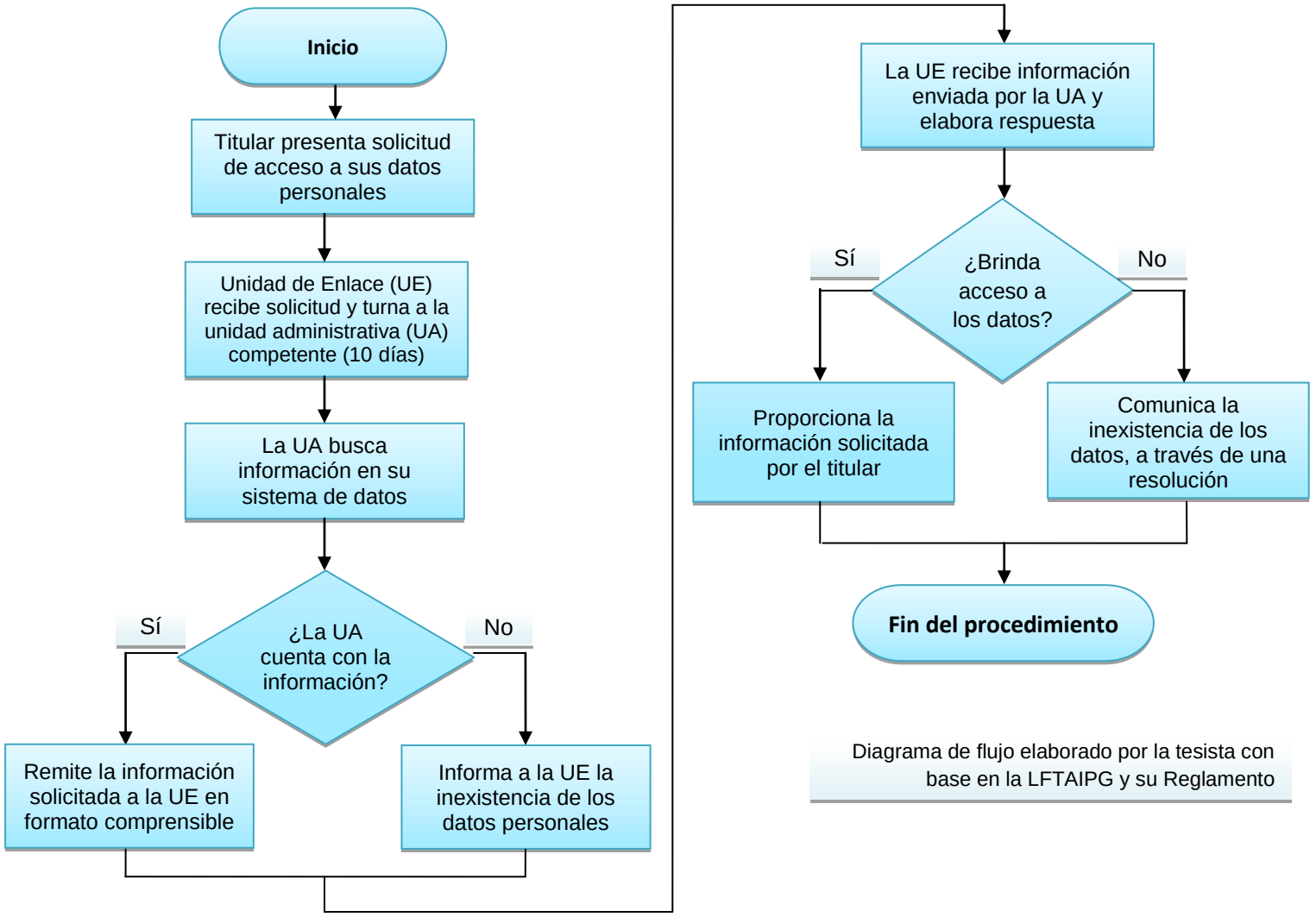


Diagrama de flujo elaborado por la tesista con base en la LFTAIPG y su Reglamento

Las unidades de enlace contarán con un plazo máximo de 10 días hábiles contados a partir de la presentación de la solicitud de acceso, para proporcionar al titular la información remitida por la unidad administrativa o, en su caso, comunicar mediante resolución, la inexistencia de datos del titular en su sistema de datos personales.

Por lo que se refiere al ejercicio del derecho de rectificación regulado en los artículos 25 de la LFTAIPG y 79 de su Reglamento, éste se desenvuelve de la siguiente manera:

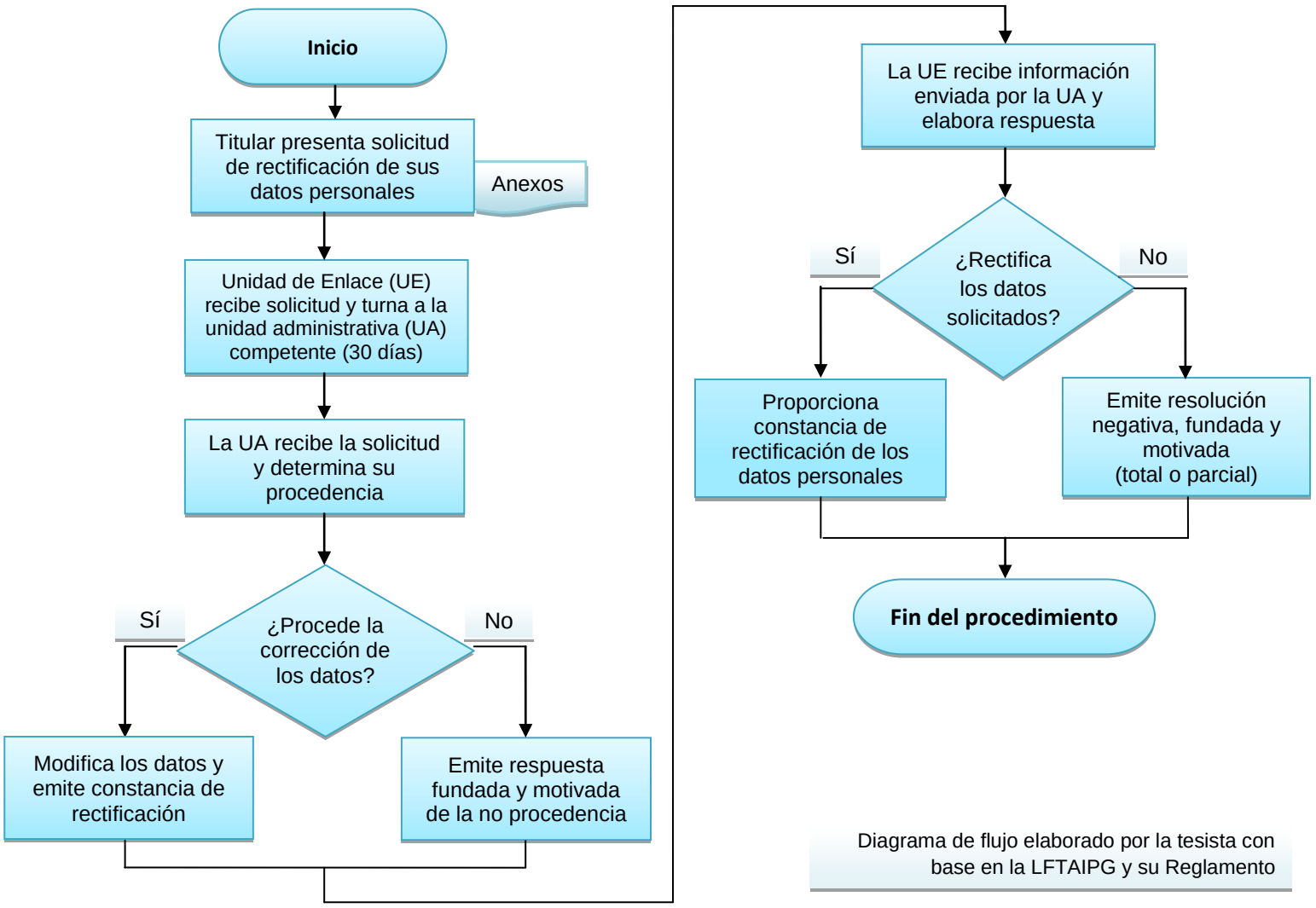


Diagrama de flujo elaborado por la tesista con base en la LFTAIPG y su Reglamento

En la solicitud el titular de los datos personales deberá señalar el sistema de datos personales donde constan los datos a corregir, así como las modificaciones a realizarse, además de anexar la documentación que motive su petición. Una vez presentada la solicitud, la unidad de enlace o su equivalente contará con un plazo de 30 días hábiles para emitir su respuesta, la cual puede ser en sentido afirmativo o negativo. La improcedencia de la solicitud podrá ser total o parcial.

En las resoluciones del Comité se comunicará al titular la procedencia del recurso de revisión. El artículo 26 en relación con el 50 de la LFTAIPG establecen los siguientes supuestos en los cuales procederá el recurso de revisión dentro de los 15 días hábiles siguientes a la notificación de la respuesta:

- Negativa de entregar al solicitante los datos personales solicitados, o lo haga en formato incomprensible (artículos 26 y 50).
- Negativa de efectuar modificaciones o correcciones a los datos personales (artículos 26 y 50).
- Por falta de respuesta en los plazos antes señalados (artículo 26).
- Inconformidad con el tiempo, costo o modalidad de entrega (artículo 50).
- Por información incompleta o no corresponda a la información requerida en la solicitud (artículo 50).

A pesar de proceder también el recurso de revisión en contra de la falta de respuesta, el artículo 53 de la LFTAIPG aclara que para la solicitud de acceso, es aplicable la figura jurídica de la afirmativa ficta, pues en el caso de no obtener la respuesta en el plazo señalado por la ley, la solicitud deberá entenderse resuelta en sentido positivo, en cuyo supuesto la dependencia o entidad estarán obligados a brindar el acceso al titular en un plazo no mayor a 10 días hábiles y cubrir todos los costos por reproducción del material, salvo si el IFAI determina que se trata de documentos clasificados como reservados o confidenciales.

Para la falta de respuesta, el IFAI llevará a cabo un procedimiento expedito de 20 días hábiles, el cual tendrá como fin asegurar que los entes públicos tengan la oportunidad de probar que respondieron en tiempo y forma al solicitante, el cual se encuentra regulado en los artículos 93 y 94 del Reglamento de la LFTAIPG. El diagrama de flujo de este procedimiento se presenta a continuación de la siguiente manera:

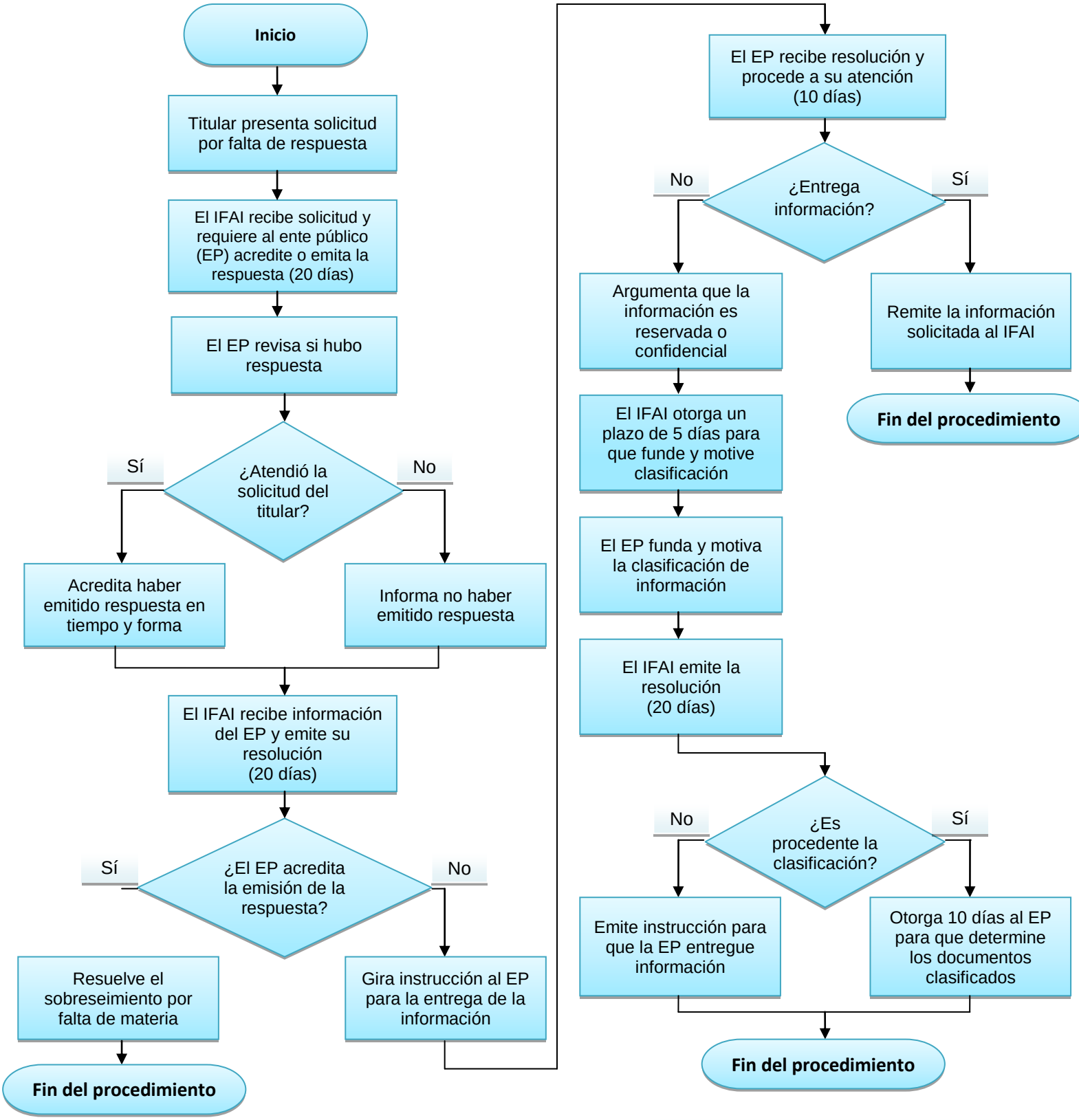


Diagrama de flujo elaborado por la tesista con base en la LFTAIPG y su Reglamento

Por lo que se refiere al plazo de los 5 días hábiles para fundar y motivar la clasificación de la información, el IFAI puede otorgar al ente público, un plazo por el mismo tiempo, en caso de considerarse insuficiente el primero.

En relación con este procedimiento, es oportuno comentar que la LFPDPPP también establece un procedimiento para la falta de respuesta, independiente al de protección de derechos, como se verá más adelante. Sin embargo en éste no se otorgan las facultades necesarias al IFAI para requerir al Responsable la entrega de la información, limitando su intervención a ser un mero intermediario sin mayor autoridad para exigir la respuesta y, en su caso, el cumplimiento de la solicitud del titular, lo cual impide la adecuada salvaguarda del derecho fundamental a la protección de datos personales.

B. Entes privados

Al igual que los procedimientos anteriores, el ejercicio de los derechos ARCO ante los entes privados inicia con la presentación de la solicitud, la cual será en la forma y medios como lo haya determinado el Responsable en su aviso de privacidad. Asimismo en similar sentido que en los entes públicos y derivado del principio de la autorregulación, los Responsables podrán establecer sus propios plazos y procedimientos internos para la recepción y atención de estas solicitudes, sujetándose únicamente a los plazos máximos y criterios básicos señalados en la LFPDPPP, como lo es el de designar a una persona o departamento de datos personales encargado de la tramitación de las solicitudes de derechos ARCO.

Conforme con lo dispuesto en los artículos 29 y 31 de la LFPDPPP, las solicitudes de derechos ARCO que presenten los titulares ante los Responsables contendrán lo siguiente:

- Nombre del titular y su domicilio u otro medio donde se le comunicará la respuesta.
- Documentos que acreditan su identidad o, en su caso, el de su representante legal.
- Descripción clara y precisa de los datos personales sobre los que ejercerá sus derechos ARCO.
- Cualquier otro elemento o documento que facilite la localización de sus datos personales.
- En el caso de solicitudes de rectificación de datos personales, deberá indicar las modificaciones a realizarse y aportar la documentación que sustente su petición.

El procedimiento para ejercer alguno de los derechos ARCO se encuentra regulado en los artículos del 28 al 35 de la LFPDPPP y del 87 al 100 de su Reglamento, y se desarrolla de la siguiente forma:

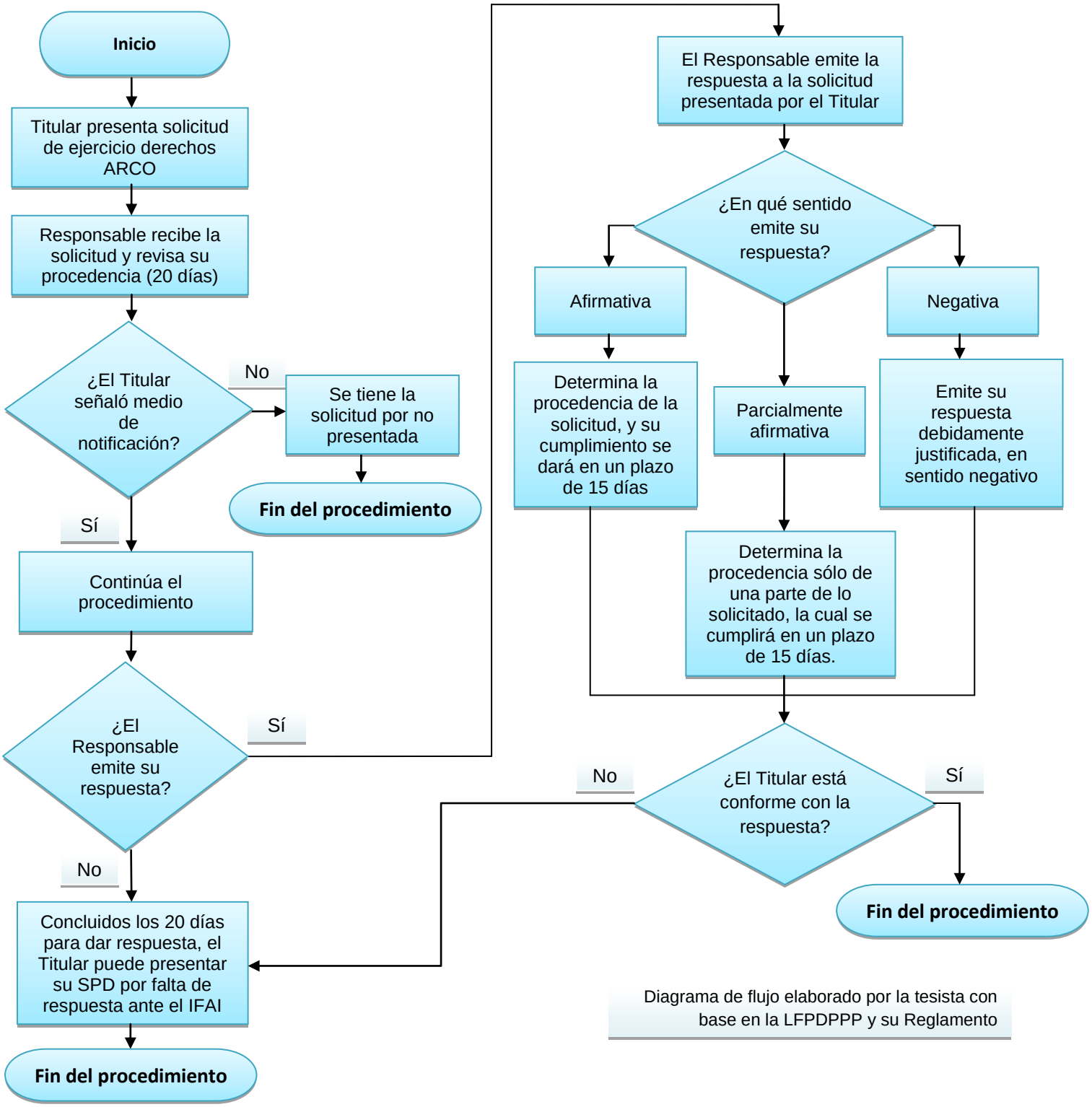


Diagrama de flujo elaborado por la tesista con base en la LFPDPPP y su Reglamento

La respuesta deberá comunicarse al titular en un plazo máximo de 20 días contados desde la fecha en que se recibió la solicitud y referirse exclusivamente a los datos personales del titular y emitirse en formato legible, comprensible y de fácil acceso. Si la respuesta se emite en sentido positivo o parcialmente negativa, el Responsable tendrá un plazo de 15 días hábiles, contados a partir del día siguiente a la notificación de la respuesta, para hacer efectiva la solicitud, ya sea total o parcialmente, según corresponda.

De esta manera, el Responsable tiene un plazo total de 35 días hábiles para atender la solicitud de ejercicio de derechos ARCO del titular. No obstante ello, el artículo 32, último párrafo de la LFPDPPP permite la ampliación debidamente justificada y notificada al titular, de los plazos de 20 días para emitir la respuesta y 15 días para dar cumplimiento al derecho ARCO solicitado, por una sola ocasión y hasta por un periodo igual, lo cual significa que este procedimiento podría llevarse a cabo hasta por un plazo de 70 días hábiles, el cual consideramos debe estar debidamente justificado y proceder sólo en casos excepcionales, de lo contrario dicho plazo se consideraría excesivo y no razonable, al ser el resultado de la carencia de mecanismos adecuados para facilitar y atender de manera ágil y rápida, la solicitud de derechos ARCO de los titulares, mismos que debieron ser previstos por el Responsable, previo al tratamiento de los datos personales.

Por otra parte, y como se mencionó antes, el artículo 98, primer párrafo del Reglamento de la LFPDPPP establece como obligación del Responsable el emitir en todo momento y dentro de los plazos antes señalados, una respuesta al titular, independientemente de no ser el Responsable o, no contar con datos personales del titular solicitante en su base de datos, pues el objetivo principal de este procedimiento debe ser garantizar el ejercicio de los derechos ARCO del titular y mantenerlo en todo momento informado respecto de sus datos personales, brindándole de esta manera, la certeza de obtener una respuesta a su solicitud, aun y cuando ésta pudiere encontrarse en sentido negativo a sus pretensiones, pero debidamente justificada.

Por lo anterior, consideramos que cuando el Responsable no emite respuesta alguna de manera justificada a la solicitud presentada por el titular y sí cuenta con información de éste, dicha omisión debe ser entendida como dolosa por parte del Responsable, así como un obstáculo para el libre ejercicio del derecho o derechos ARCO del titular, conductas que al adecuarse a los supuestos de infracción establecidos en el artículo 63, fracciones II y XVII de la LFPDPPP, podrían ser sancionadas conforme en la misma se establece.

Cuando el Responsable emita una respuesta negativa a lo solicitado por el titular, debe señalar en la misma los motivos de su decisión, así como en su caso,

acompañarla con las pruebas que resulten pertinentes, de tal manera que la respuesta se encuentre debidamente justificada. Asimismo, el Responsable debe informar al titular su derecho a solicitar el inicio del procedimiento de protección de derechos ante el IFAI, en caso de inconformidad con la respuesta recibida.

Los supuestos por los cuales el Responsable puede negar los derechos ARCO, se establecen en el artículo 34 de la LFPDPPP de la siguiente manera:

- Cuando el solicitante no sea el titular de los datos personales, o el represente legal no esté debidamente acreditado; lo cual confirma que este derecho es personal y únicamente puede ser ejercido por quien acredite la titularidad de los datos personales.
- Cuando en la base de datos del Responsable no se encuentren los datos personales del solicitante; en cuyo caso, opinamos que no basta con el simple señalamiento en la respuesta, sino será necesario acompañarla con las pruebas correspondientes.
- Cuando se lesionen los derechos de un tercero. Lo anterior indica un conflicto de intereses, lo cual de acuerdo al caso en particular y la gravedad del daño que se pueda causar a cada uno de los sujetos involucrados en sus derechos respectivos, pudiere no ser un asunto para resolver por parte del Responsable, quien carece de autoridad para ponderar derechos en conflicto; sin embargo reiteramos, esto dependerá de cada asunto en particular y en todo caso la respuesta del Responsable deberá exponer claramente los motivos que justifiquen este supuesto, así como presentar las pruebas que fueren pertinentes.
- Cuando exista un impedimento legal, o la resolución de una autoridad competente que restrinja los derechos ARCO.
- Cuando la rectificación, cancelación u oposición haya sido previamente realizada, lo cual deberá acreditar el Responsable; en este supuesto faltaría agregar, salvo que los derechos no hubieren sido debidamente atendidos o se hicieron en una forma parcial.

Además de los supuestos antes señalados podrán aplicarse los establecidos en el artículo 26 de la LFPDPPP, revisados como excepciones a la cancelación, al inicio del presente capítulo.

Un vez recibida la respuesta por parte del Responsable o concluido el plazo para que se emitiera la misma, el titular podrá debido a su inconformidad con la respuesta o por su falta de emisión, solicitar al IFAI inicie con el procedimiento de protección de derechos, tal y como lo establece el artículo 35, último párrafo de la LFPDPPP que a la letra dice: “El titular podrá presentar una solicitud de protección

de datos por la respuesta recibida o falta de respuesta del responsable, de conformidad con lo establecido en el siguiente Capítulo".

Del artículo citado observamos la mención de una solicitud de protección de "datos", término como se denomina en toda la LFPDPPP al escrito libre o formato mediante el cual el titular de los datos personales solicita el inicio del procedimiento de protección de "derechos" ante el IFAI. Sin embargo es de resaltar que en su Reglamento se le denomina solicitud de protección de "derechos", es decir de manera distinta, como si se tratara de documentos diversos, y si bien esto parece no ir más allá que una simple discrepancia de términos, consideramos debe ser corregido para evitar posibles confusiones.

En nuestra opinión el término correcto debió ser el de solicitud de protección de derechos en congruencia con el nombre del procedimiento que se inicia el cual se denomina "protección de derechos", sin embargo en este caso, el reglamento no puede ir más allá de la ley, por lo que deberá prevalecer el señalado por esta última hasta en tanto este término no se adecue en la LFPDPPP. Aunado a lo anterior, hay que recordar que el fin de este derecho no es la protección de los datos personales sino de las personas titulares de los datos en el ejercicio de sus derechos ARCO, por lo cual en el presente trabajo se utilizará la referencia de procedimiento de protección de derechos.

Por otra parte, el artículo 35 antes citado ubicado dentro del Capítulo IV de la LFPDPPP señala en su parte final que la presentación de la solicitud de protección de derechos, se hará conforme a lo establecido en el "siguiente Capítulo", el cual conforme al orden de la ley corresponde al Capítulo V relativo a las Transferencias de Datos. Sin embargo, en su contenido no consta regulación alguna relativa a dicha solicitud, por tanto la cita es errónea, y en su lugar debió haberse referido al Capítulo VII "Del Procedimiento de Protección de Derechos", donde se regula ampliamente la presentación de la solicitud de protección de derechos ante el IFAI, como autoridad encargada de conocer y resolver este y el procedimiento de verificación señalados en la LFPDPPP e imponer las sanciones que correspondan, así como otros temas que serán analizados en el siguiente punto.

II. Procedimiento de protección de los derechos ARCO.

Antes de iniciar con el análisis del procedimiento de protección de derechos, revisaremos el supuesto previsto en el artículo 116, último párrafo del Reglamento de la LFPDPPP, el cual si bien no implica el inicio de un procedimiento propiamente dicho, y tampoco forma parte del procedimiento de protección de derechos, si requiere de la intervención del IFAI, a solicitud del titular de los datos personales, como se observa en el siguiente diagrama:

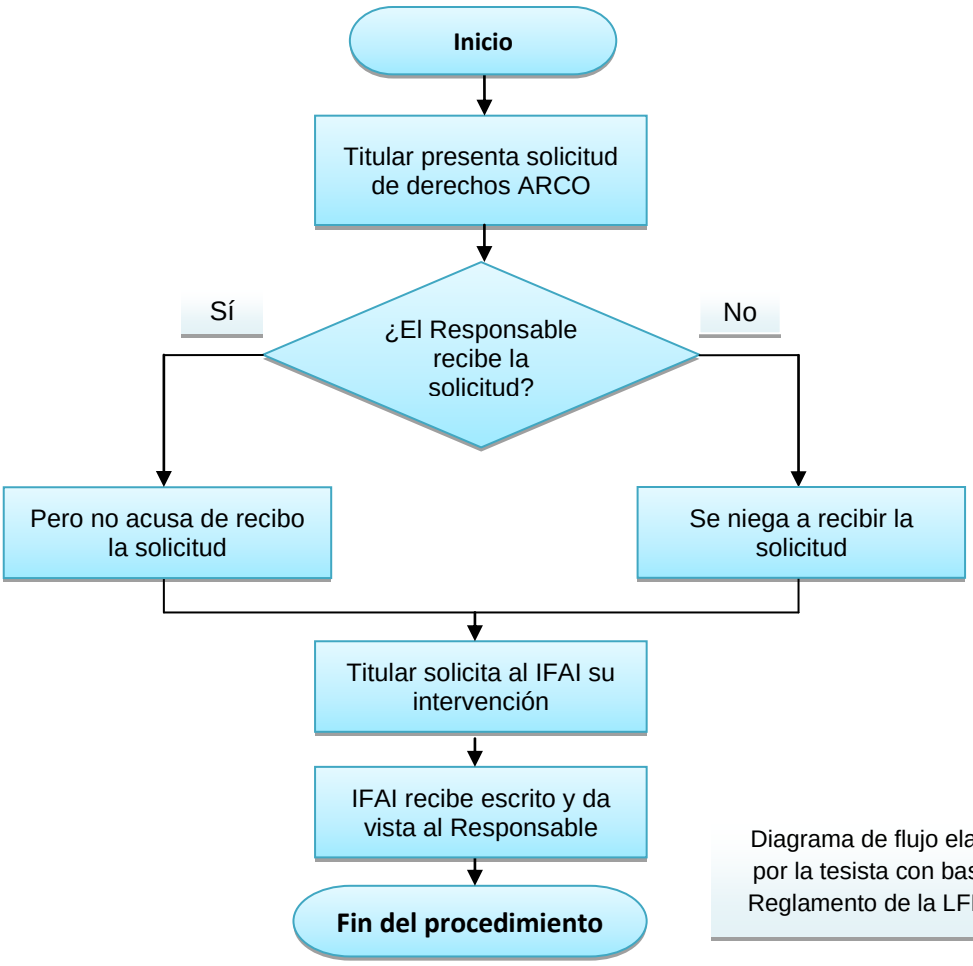


Diagrama de flujo elaborado por la tesista con base en el Reglamento de la LFPDPPP

El artículo 116, último párrafo del Reglamento de la LFPDPPP refiere al supuesto de que el Responsable se niegue a recibir la solicitud de derechos ARCO del titular o a emitir el acuse de su recepción, motivo por el cual el titular no está en posibilidad de acreditar ante el IFAI que acudió ante el Responsable y solicitó alguno de los derechos ARCO y, por tanto, tampoco cumple con uno de los documentos necesarios para solicitar el inicio del procedimiento de protección de derechos, señalado en el artículo 116, fracción IV del Reglamento de la LFPDPPP, consistente en la copia del acuse o constancia de recepción de la solicitud de derechos ARCO, por parte del Responsable.

Al no contar con dichos elementos, el titular podrá solicitar por escrito, la intervención de IFAI, a quien hará de su conocimiento tales hechos, para que dé vista al Responsable y manifieste lo que a su derecho convenga, con la única finalidad de garantizar al titular el ejercicio de sus derechos ARCO. De lo anterior se desprenden los siguientes comentarios:

- En esta disposición podemos observar dos conductas negativas por parte del Responsable y, por lo tanto, requisitos para que proceda esta solicitud del titular: 1) se niega a recibir la solicitud de derechos ARCO ó 2) recibe la solicitud pero se niega a acusar su recepción.
  Al parecer, la segunda conducta negativa sería una falta de respuesta, sin embargo no puede seguir el mismo procedimiento en razón de no existir constancia alguna para acreditar la presentación de la solicitud del titular ante el Responsable y, por tanto, prueba alguna para señalar de manera fehaciente esa conducta.
- El escrito mediante el cual el titular hace del conocimiento al IFAI la conducta del Responsable, no debe limitarse a ese sólo señalamiento, pues al no contar con constancia documental para acreditar su presencia ante el Responsable, debe detallar claramente los hechos sucedidos, así como especificar circunstancias de modo, tiempo y lugar, y si es necesario, nombres o media filiación del personal del Responsable que se negó a recibir la solicitud, a fin de aportar mayor elementos en el asunto.
- Al dar vista al Responsable para manifestar lo que a su derecho convenga, se respetan sus derechos procesales para defenderse y se actúa de manera imparcial sin dar la razón a ninguna de las partes hasta que alguna de ellas no demuestre lo contrario.
- No se establece el plazo para que el Responsable de respuesta a la vista realizada por el IFAI, por lo que de conformidad con lo dispuesto por el artículo 5, segundo párrafo de la LFPDPPP, se aplicará supletoriamente lo dispuesto en la LFPA, en donde en su artículo 32 establece que para efectos de vistas, a falta de términos o plazos establecidos en las leyes administrativas, para la realización de trámites, aquéllos no excederán de diez días.
- El IFAI actúa en este caso únicamente como un intermediario entre las partes, sin embargo ello no es impedimento para que en cualquier momento pueda ejercer sus atribuciones previstas en los artículos 38 y 39 fracción I de la LFPDPPP, consistentes en vigilar y verificar el cumplimiento de las disposiciones previstas en la ley, en cuyo caso, si observa alguna conducta contraria a la misma actúe en consecuencia, pues la finalidad es garantizar el ejercicio de los derechos ARCO del titular. No obstante lo anterior, es bien sabido que una autoridad no puede ir más allá de lo expresamente señalado en la ley, por lo que la actuación del IFAI se encuentra limitada en este caso; por ello consideramos debe contar con atribuciones especificas en la ley para aplicar, en su caso, medidas de apremio ante la insistente negativa del Responsable, así como iniciar un procedimiento de protección de derechos por falta de respuesta o incluso uno, de manera directa, de sanciones.

Un punto muy importante en esta intervención del IFAI, es que la ley no prevé el procedimiento que deberá seguir, una vez que haya dado vista al Responsable, pues es factible el surgimiento de diversos supuestos concluido el plazo otorgado al Responsable, como son los siguientes:

POSIBLES CONDUCTAS DEL RESPONSABLE	POSIBLES ACTUACIONES DEL IFAI
1) No responde a la vista emitida por el IFAI.	1) Comunica al titular la omisión y deja a salvo sus derechos para presentar la solicitud para iniciar el procedimiento de protección de derechos por falta de respuesta, o en su caso, una denuncia para iniciar el procedimiento de verificación.
2) Niega los hechos expuestos por el titular y por tanto que intentó presentar la solicitud.	2) Remite al titular la respuesta del Responsable y deja a salvo sus derechos para presentar la solicitud de derechos ARCO.
3) Confirma los hechos expuestos por el titular, pero señala que la solicitud no fue presentada en la forma descrita en su aviso de privacidad.	3) Remite al titular la respuesta del Responsable y deja a salvo sus derechos para presentar una nueva solicitud de derechos ARCO.
4) Remite la respuesta correspondiente a la solicitud de derechos ARCO, ya sea en sentido afirmativo o negativo.	4) Remite al titular la respuesta del Responsable y le otorga un plazo para que manifieste lo que a su derecho convenga. Si manifiesta su inconformidad con la respuesta puede iniciar el procedimiento de protección de derechos.

Ante esta multiplicidad de probables conductas por parte del Responsable y posibles actuaciones de la autoridad, no queda más que estar a los criterios que al respecto tome el IFAI, sin embargo ello no deja de crear incertidumbre jurídica y falta de certeza en el procedimiento, motivo por el cual sugerimos que el supuesto señalado en el artículo 116, último párrafo del Reglamento de la LFPDPPP sea regulado. Al respecto, sugerimos que en caso de omisión a la vista, se inicie de oficio un procedimiento de verificación y para el supuesto de que el Responsable remita su respuesta y el titular manifieste su inconformidad con la misma, se inicie con dicha manifestación, el procedimiento de protección de derechos; en los demás casos, se dejarían a salvo los derechos del titular.

Por lo anterior, consideramos que el supuesto establecido en el artículo 116, último párrafo del Reglamento de la LFPDPPP es incompleto e insuficiente para salvaguardar los derechos del titular, y no obstante la buena intención de dicha disposición por cumplir ese objetivo; éste no se logra al omitir el procedimiento y plazos específicos a seguir, ante los diversos supuestos y probables consecuencias

que pueden llegar a presentarse. Por lo tanto, no existe certeza en el procedimiento y una adecuada protección a este derecho.

Dentro del procedimiento de protección de derechos se encuentra el de falta de respuesta, el cual si bien inicia con la presentación de la solicitud de protección de derechos ante el IFAI y concluye con una resolución, su desarrollo y objetivo son distintos; por lo que podría considerarse como una subespecie del procedimiento de protección de derechos. Como su nombre lo indica, el procedimiento por falta de respuesta tiene por objeto solicitar la intervención del IFAI para obtener del Responsable la respuesta a la solicitud de derechos ARCO que el titular le presentó en su momento y no atendió dentro del plazo de los 20 días hábiles.

De acuerdo con lo previsto en el artículo 45, segundo párrafo de la LFPDPPP, este procedimiento inicia con la presentación, por parte del titular, de su solicitud de protección de derechos, la cual podrá llevar a cabo “a partir” de que haya vencido el plazo de respuesta previsto para el Responsable, con lo cual observamos el inicio (a partir del día 21) pero no el tiempo de conclusión para su presentación, dejándolo al parecer de manera abierta e indefinida. Sin embargo, al dar lectura al mismo artículo 45, primer párrafo de la LFPDPPP se observa en su parte final, el siguiente señalamiento: “La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable”.

De lo anterior, se observa un plazo de 15 días hábiles para la presentación de las solicitudes de protección de derechos, el cual al no estar expresamente referido para un procedimiento en específico, será de aplicación para todos los que se lleven a cabo dentro del “Capítulo VII. Del Procedimiento de Protección de Derechos”, capítulo donde se encuentra localizado el referido artículo 45 de la LFPDPPP. No obstante lo anterior, es recomendable que la ley defina claramente este plazo en el supuesto por falta de respuesta a efecto de brindar certeza en el procedimiento, toda vez que el referido precepto legal ya ha sido objeto de estudio por parte de la autoridad judicial en un caso particular, la cual se inclinó por el criterio de no condicionar la presentación de la solicitud de protección de derechos por falta de respuesta, cuando la propia ley no prevé un plazo en particular, y menos que tenga por efecto la preclusión del derecho a ejercer.

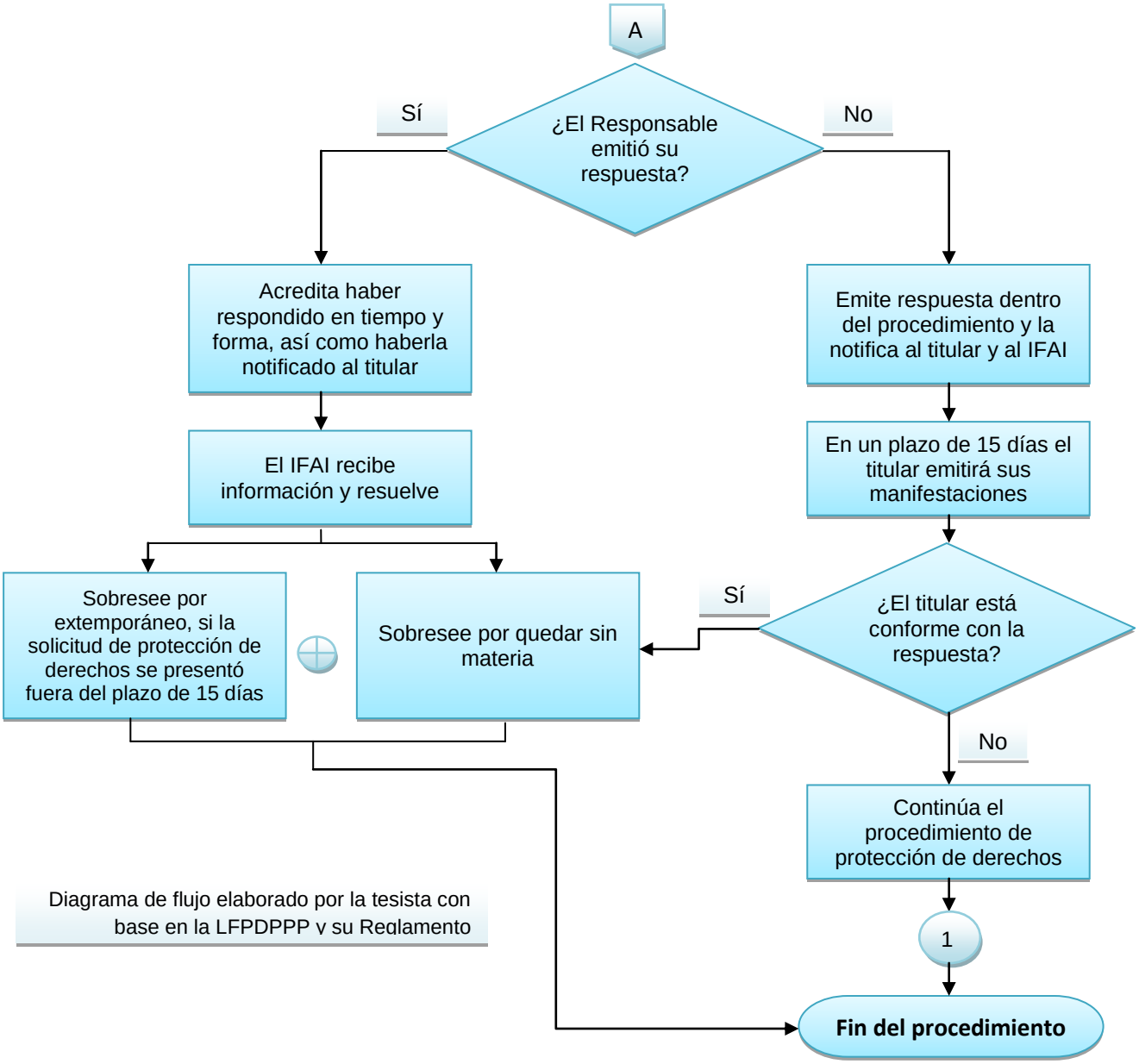
Al respecto, se difiere del citado criterio jurisdiccional, porque bajo ese esquema se otorgaría un trato desigual al distinguir dos clases de titulares, porque por un lado se encontrarían los titulares que cuentan con la respuesta del Responsable, quienes tienen un plazo de 15 días hábiles para presentar su solicitud del procedimiento de protección de derechos, y en caso de hacerlo fuera del mismo,

su solicitud se desecharía por extemporánea. Pero por otro lado, estarían aquellos titulares que no cuentan con la respuesta del Responsable, y que por ese sólo motivo, tienen la ventaja de no correr para ellos, plazo alguno en la presentación de la solicitud de protección de derechos, es decir no aplica en esos casos, la extemporaneidad.

Así las cosas, y acorde al criterio personal antes señalado, la solicitud de protección de derechos por falta de respuesta deberá presentarse dentro del plazo de los 15 días hábiles, contados a partir del vencimiento de los 20 días hábiles con los cuales contaba el Responsable para dar respuesta al titular, fuera del primer plazo mencionado (15 días), la solicitud del titular será desechada por extemporánea, en términos de lo dispuesto en el artículo 52, fracción V de la LFPDPPP.

Por la característica particular de este supuesto en donde es imposible presentar la respuesta del Responsable, los artículos 45, segundo párrafo, 46, penúltimo párrafo de la LFPDPPP y 116, fracción IV de su Reglamento, establecen que bastará la presentación de la solicitud de derechos ARCO, en donde conste el acuse o constancia de su recepción por parte del Responsable; fuera de esta excepción deberá cumplirse con todos los requisitos señalados en los artículos 46 de la LFPDPPP y 116 de su Reglamento para la presentación de la solicitud de protección de derechos.

El procedimiento por falta de respuesta se encuentra regulado en el artículo 55 de la LFPDPPP y 124 de su Reglamento, el cual se desarrolla como se observa en el siguiente diagrama de flujo:



De lo anterior, se desprenden diversos supuestos regulados en el artículo 124 del Reglamento de la LFPDPPP de la siguiente manera:

- Si el Responsable acredita haber dado respuesta en tiempo y forma a la solicitud de derechos ARCO, así como haberla notificado al titular o su representante, el procedimiento se sobresee por quedar sin materia.

- Si el Responsable acredita haber dado respuesta en tiempo y forma a la solicitud de derechos ARCO, pero la solicitud de protección de derechos no fue presentada en el plazo de los 15 días hábiles, se sobreseerá por extemporánea. Como se explicó anteriormente, lo mismo debe suceder en caso de no contar con respuesta, y la solicitud de protección de derechos se presenta fuera del plazo de los 15 días.
- Si el Responsable emite su respuesta fuera del plazo de los 20 días hábiles o dentro de este procedimiento de protección de derechos por falta de respuesta, el Responsable tiene la obligación de notificar dicha respuesta al IFAI y al titular, para que este último en el plazo de 15 días hábiles contados a partir de la notificación, manifieste lo que a su derecho convenga, a efecto de continuar con el curso del procedimiento.

  Al respecto, no se observa si el Responsable tiene la obligación de informar en su misma respuesta, que el titular cuenta con un plazo de 15 días para manifestar lo que a su derecho convenga con la misma, por lo cual al no quedar clara esta situación y a efecto de impedir la preclusión del derecho del titular, se sugiere que el IFAI al momento de recibir la respuesta a través de acuerdo, haga el señalamiento de los 15 días hábiles que tiene el titular para manifestar su conformidad, ello independientemente que el Responsable así lo señale en su respuesta.

  Otro problema no regulado en la ley, es como debe ser tratada la ausencia de manifestación por parte del titular dentro del plazo de los 15 días hábiles, pues dicha omisión no podría ser interpretada por la autoridad como afirmativa o negativa, pues iría más allá de sus facultades para garantizar el derecho fundamental y tampoco podría aplicarse como una suplencia de la deficiencia de la queja conforme a lo dispuesto en el artículo 50 de la LFPDPPP, porque en este caso se trata de la voluntad y consentimiento de la persona, en el manejo de sus datos personales.

  Ahora bien, hay que considerar que dicha disposición refiere a la continuación del procedimiento, lo cual resulta relevante para el asunto en discusión, pues independientemente que el titular manifieste su conformidad o no, el IFAI debe continuar y resolver el procedimiento conforme se establece en la LFPDPPP y su Reglamento, aun cuando dichos ordenamientos no sean muy claros al respecto. De esta manera, al concluir el plazo de los 15 días hábiles otorgados al titular, el IFAI deberá continuar con el procedimiento mediante el desahogo de las pruebas si las hubiere y otorgar el plazo de alegatos, para posteriormente emitir la resolución correspondiente, en donde determinará la procedencia o no de la solicitud de derechos ARCO en concordancia con la respuesta recibida del Responsable. En caso de ser procedente la solicitud, requerirá al

Responsable el cumplimiento a la misma, según se trate del derecho solicitado. Y aunque la ley no establece la atención que se dará en caso de determinarse la no procedencia de la solicitud, en términos del artículo 51, fracción I, en relación con el 53 fracción IV, ambos de la LFPDPPP, la solicitud podrá sobreseerse.

- Si el Responsable no atiende el requerimiento en el plazo de 10 días hábiles, el IFAI resolverá conforme a los elementos que consten en el expediente, disposición considerada poco acertada, toda vez que como se describió en este procedimiento, las únicas constancias que obran en el expediente son las aportadas por el titular, consistentes en su solicitud de protección de derechos, su identificación o la de su representante, el acuse de recibo de la solicitud de derechos ARCO y, en su caso, pruebas (es poco viable que se presenten debido a la ausencia de respuesta por parte del Responsable); elementos insuficientes para resolver un procedimiento, en el cual todavía no se logra cumplir con su objetivo principal, que es obtener una respuesta por parte del Responsable.

  Aunado a lo anterior y en el supuesto de resolver, debemos tomar en cuenta las únicas posibilidades que al efecto señala el artículo 51 de la LFPDPPP para una resolución dentro del procedimiento de protección de derechos: 1) sobreseer o desechar la solicitud; ó 2) confirmar, revocar o modificar la respuesta; sentidos que no resultan aplicables para este caso en particular, y menos aun el segundo de ellos, por no existir respuesta del Responsable. Entonces si no son aplicables estos supuestos de resolución, ¿en qué sentido podrá ser la resolución emitida por el IFAI ante una falta de respuesta? ¿Cómo puede resolver algo en donde no hay punto de controversia ni mayores elementos de prueba? Al respecto pueden darse los siguientes supuestos de resolución:

  1) Dejar constancia de la falta de respuesta por parte del Responsable y a salvo los derechos del titular, o

  2) Dejar constancia de la falta de respuesta por parte del Responsable e iniciar de oficio un procedimiento de verificación ante posibles violaciones a la LFPDPPP, resolución considerada como la más viable.

Por lo anterior, y como se mencionó en el procedimiento análogo para entes públicos, estas lagunas en la ley traen como consecuencia la imposibilidad de brindar una adecuada salvaguarda de este derecho fundamental, al encontrarse el titular de los datos personales imposibilitado para ejercer sus derechos ARCO y, por tanto, en estado de indefensión frente a un Responsable que impide el ejercicio de los derechos del titular, al no brindar respuesta alguna a su solicitud y no sólo a ésta

sino también al requerimiento de la autoridad competente (IFAI). Ante este escenario consideramos que la insistente negativa en responder, debe ser señalada como una conducta dolosa que impide el ejercicio de los derechos ARCO del titular, la cual debe ser sancionada conforme se establezca en la ley; aunado a lo anterior, sería conveniente dotar al IFAI de las facultades necesarias para imponer ciertas medidas de apremio, con las cuales se garantice el cumplimiento de sus requerimientos.

Del análisis realizado en los dos anteriores procedimientos, se observan aún diversas conductas y supuestos sin regular, los cuales serán resueltos conforme a los criterios pronunciados por el IFAI y, más adelante, los emitidos por la autoridad jurisdiccional competente hasta alcanzar la jurisprudencia en esta materia; pero mientras eso sucede, la LFPDPPP y su Reglamento serán objeto de diversas interpretaciones usadas tanto a favor como en contra de los sujetos involucrados en los procedimientos, con lo cual se puede llegar a vulnerar, en lugar de garantizar, el derecho a la protección de datos personales del titular; por ello, es importante que la autoridad no pierda de vista en el desahogo de cualquier procedimiento que sustancie, su deber de salvaguardar en primer término el derecho fundamental del titular.

En consecuencia, observamos que no sólo la diversidad de regulación puede ser motivo de una inadecuada protección de derechos sino también el uso de términos ambiguos y las lagunas en la ley, lo cual implica una revisión detallada de los ordenamientos legales en la materia.

Visto lo anterior y hechas las precisiones pertinentes a los anteriores procedimientos, enseguida realizaremos el análisis del procedimiento de protección de derechos conforme se establece en los artículos del 45 al 58 de la LFPDPPP y del 113 al 127 de su Reglamento, integrado por cuatro etapas básicas que son:

La admisión, es la primera etapa del procedimiento de protección de derechos, y se desarrolla de la siguiente forma:

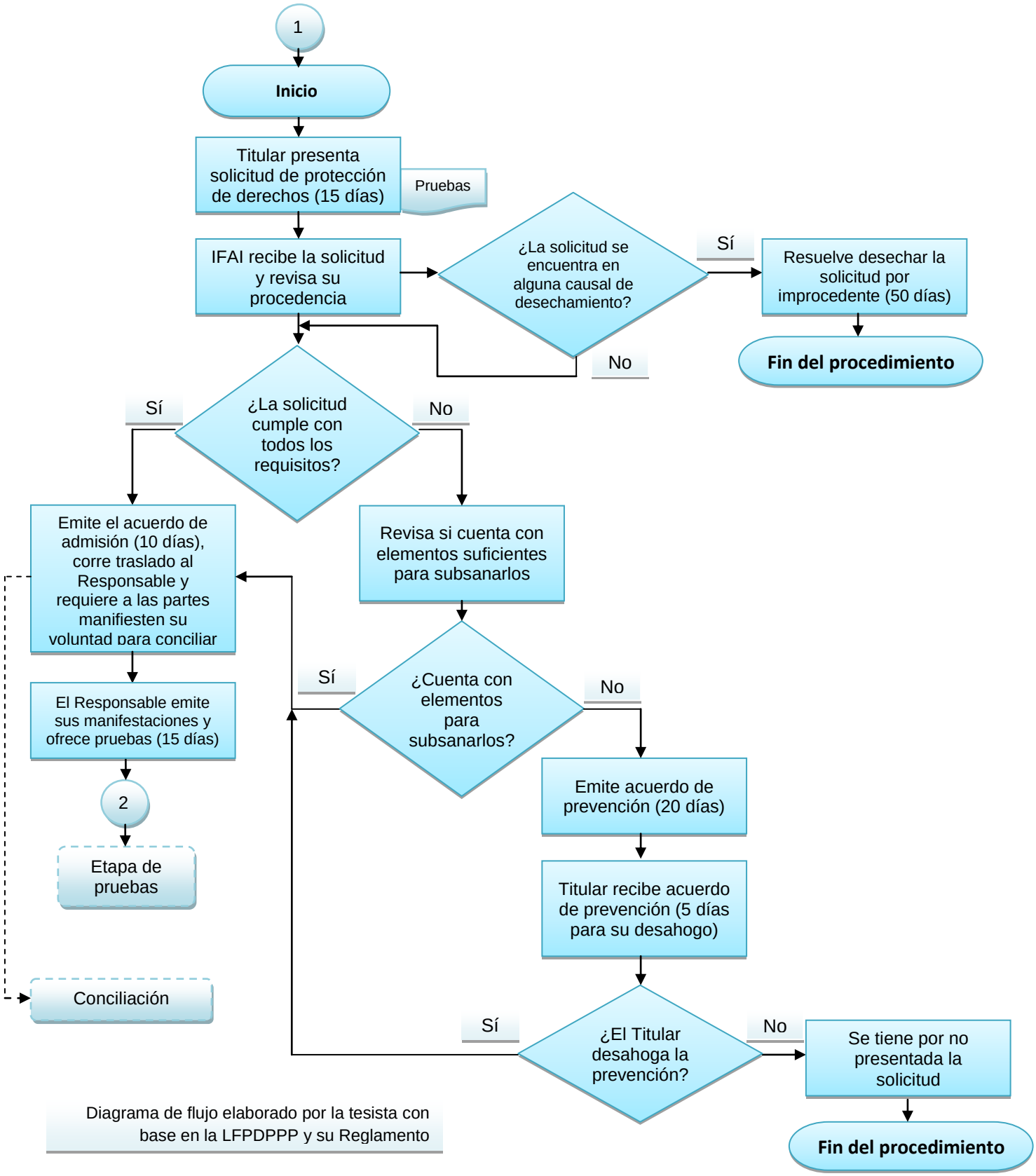


Diagrama de flujo elaborado por la tesista con base en la LFPDPPP y su Reglamento

El procedimiento de protección de derechos, al igual que los anteriores, inicia a instancia de parte, por lo cual sólo el titular de los datos, o su representante, podrá presentar la solicitud de protección de derechos cuando considere vulnerado alguno o algunos de sus derechos ARCO, dentro de los 15 días hábiles siguientes a la fecha en que el Responsable le comunique su respuesta.

De acuerdo con lo dispuesto en los artículos 45, tercer párrafo de la LFPDPPP y 115 de su Reglamento, la solicitud de protección de derechos procede, además de la falta de respuesta antes vista, cuando se den alguno de los siguientes supuestos:

- El Responsable no entregue al titular los datos personales solicitados (No se otorgue acceso a los datos personales).
- El Responsable los entregue en un formato incomprensible.
- El Responsable se niegue a efectuar las modificaciones o correcciones a los datos personales (Negativa en efectuar las rectificaciones de datos).
- El titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la información requerida (o esté inconforme con el costo o modalidad de la reproducción).
- El Responsable se niegue a cancelar los datos personales.
- El Responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición.
- Por otras causas que a juicio del IFAI sean procedentes conforme a la LFPDPPP o a su Reglamento.

La solicitud de protección de datos puede presentarse mediante escrito libre, los formatos que determine el IFAI o a través del sistema electrónico que al efecto establezca el IFAI en su página de Internet y debe contener además de su reclamación expuesta en forma clara, la siguiente información y documentación señaladas en los artículos 46 de la LFPDPPP y 116 de su Reglamento:

- El nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay.
- El nombre del Responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales.
- El domicilio para oír y recibir notificaciones.
- La fecha en que se le dio a conocer la respuesta del Responsable.
- Los actos que motivan su solicitud de protección de datos.
- Copia de la solicitud del ejercicio de derechos que corresponda, así como copia de los documentos anexos y de traslado.

- El documento que acredite que actúa por su propio derecho o en representación del titular; para lo cual el titular debe acreditar su identidad o el representante su personalidad. Es importante mencionar que el IFAI podrá tener por reconocidas esta identidad o personalidad, según sea el caso, cuando la misma ya hubiere sido acreditada ante el Responsable al ejercer el titular sus derechos ARCO.
- El documento en que conste la respuesta del Responsable.
- Las pruebas documentales públicas o privadas, de inspección, la presuncional, pericial, testimonial y fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.
- Cualquier otro documento y demás elementos que se considere procedente hacer del conocimiento y someter a juicio del IFAI.
- En los formatos emitidos por el IFAI también consta un apartado para seleccionar el medio de notificación, el cual puede ser por correo certificado, correo electrónico o a través del sistema que al efecto establezca el IFAI. Asimismo se establece un apartado para que el titular manifieste si está de acuerdo en someterse a audiencias conciliatorias.

Una vez recibida la solicitud de protección de datos, empezarán a correr dos plazos para el IFAI, uno de 50 días hábiles para dictar resolución y el de 10 días hábiles para acordar la admisión de la solicitud, ambos contados a partir de su recepción.

Durante el plazo de revisión de la solicitud de protección de derechos, es posible que el IFAI observe alguna de las siguientes situaciones:

- La solicitud se encuentra en alguna de las causales para desechar la misma, señaladas en el artículo 52 de la LFPDPPP (más adelante se detallarán); en cuyo caso el Pleno del IFAI [131] emitirá resolución de desechamiento con la cual concluirá el procedimiento.
- No se actualiza alguna de las causales de procedencia previstas en el artículo 115 del Reglamento de la LFPDPPP (antes referidas) y de su contenido se desprende la solicitud de una verificación, en cuyo caso se realizará la reconducción del procedimiento y la solicitud será turnada a la unidad administrativa competente (Dirección General de Verificación) en un plazo de 10 días hábiles, contados a partir de la fecha de recepción de

[131] De conformidad con lo dispuesto en los artículos 3 fracción V, 5 fracción I, 6, 7 y 10 del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos, publicado en el DOF el 29 de octubre de 2012, el Pleno es el órgano máximo de dirección y decisión del IFAI, integrado por cinco comisionados. Es la autoridad frente a los comisionados en su conjunto y en lo particular, y sus decisiones y resoluciones se adoptarán por mayoría simple y el Comisionado Presidente tendrá voto de calidad.

la solicitud, para que conforme a sus atribuciones inicie el procedimiento de verificación.

- La solicitud satisface todos los requisitos señalados en los artículos 46 de la LFPDPPP y 116 de su Reglamento (antes mencionados), por lo que procede a emitir el acuerdo de admisión correspondiente.
- De la revisión de la solicitud de protección de datos se desprende la falta de alguno de los requisitos previstos en la LFPDPPP y su Reglamento; en este caso el IFAI tendrá dos opciones:

  1) De acuerdo con su facultad de suplencia de la queja establecida en el artículo 50 de la LFPDPPP, el IFAI puede subsanar el requisito que faltare, siempre y cuando no altere el contenido original de la solicitud de ejercicio de derechos ARCO, ni modifique los hechos o peticiones expuestos en esta o en la solicitud de protección de derechos, o
  2) Si no contare con elementos suficientes para subsanarlo, prevendrá al titular, por una sola ocasión y dentro del plazo de 20 días hábiles[132] siguientes a la presentación de la solicitud de protección de derechos, para que subsane las omisiones en un plazo de 5 días hábiles. Durante este tiempo se interrumpirá el plazo de los 50 días hábiles que tiene el IFAI para resolver la solicitud. Si el titular no desahoga la prevención su solicitud se tendrá por no presentada.

Una vez satisfechos todos los requisitos de la solicitud de protección de derechos, el IFAI emitirá el acuerdo de admisión, donde ordenará correr traslado al Responsable con la copia de la solicitud de protección de derechos y sus anexos, para que en un plazo de 15 días hábiles contados a partir de la notificación, ofrezca pruebas y manifieste por escrito lo que a su derecho convenga.

De conformidad con la facultad que tiene el IFAI para buscar en cualquier momento la conciliación entre las partes, a través del acuerdo de admisión, requerirá al titular y al Responsable para que en un plazo no mayor a 10 días hábiles contados a partir de la notificación del mismo, manifiesten su voluntad para conciliar, en los términos de lo dispuesto en los artículos 54, primer párrafo de la LFPDPPP y 120 de su Reglamento. Para estos efectos el acuerdo deberá contener un resumen de la solicitud de protección de derechos y de la respuesta del Responsable, así como los elementos comunes y los puntos de controversia. Lo anterior no implica que en

[132] Es conveniente que el plazo de 20 días hábiles para prevenir sea coincidente con el de 10 días hábiles para admitir la solicitud, señalado en el artículo 117 del Reglamento de la LFPDPPP, en razón que el objeto para ambos es el mismo, es decir que la autoridad cuente con un plazo suficiente para realizar el estudio previo de la solicitud, a fin de determinar si previene o admite la solicitud, considerando como suficiente el plazo de los 10 días hábiles.

cualquier momento del procedimiento, el IFAI pueda conminar a las partes a la conciliación.

La audiencia de conciliación podrá celebrarse de manera presencial, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el IFAI, siempre y cuando pueda acreditarse su existencia. Dicha audiencia tiene como objeto avenir los intereses entre el titular y el Responsable, mediante la intervención del IFAI quien fungirá como conciliador, a fin de llegar a un acuerdo que tendrá efectos vinculantes, y con el cual, después de haberse acreditado su cumplimiento, podrá darse por terminado el procedimiento. La conciliación es un mecanismo de solución de controversias que permite conocer de cerca las pretensiones e intereses de cada una de las partes y concluir de la mejor manera algún conflicto, en muchos de los casos con óptimos resultados.

Actualmente la conciliación ha sido un excelente medio de solución de controversias en los procedimientos de protección de derechos que se han presentado ante el IFAI. El procedimiento de conciliación se encuentra regulado en los artículos 54 de la LFPDPPP y 120 de su Reglamento, y se lleva a cabo de la siguiente manera:

Diagrama de flujo elaborado por la tesista con base en la LFPDPPP y su Reglamento

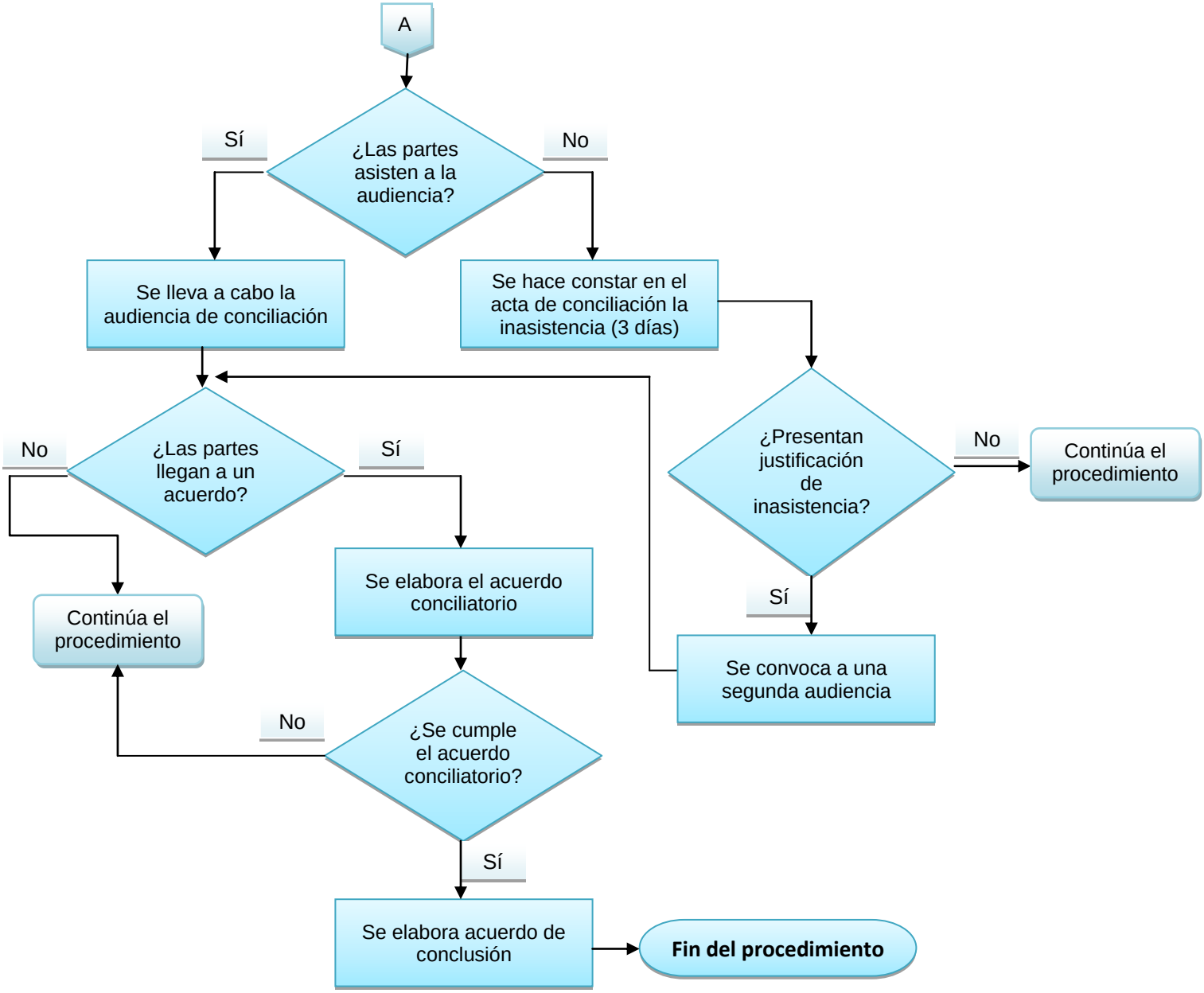


Diagrama de flujo elaborado por la tesista con base en la LFPDPPP y su Reglamento

La conciliación inicia cuando ambas partes manifiestan su voluntad para conciliar dentro del plazo de 10 días hábiles. En cualquier momento de la conciliación, el conciliador podrá solicitar a las partes, presenten algún elemento de convicción que estimen necesarios, dentro del plazo máximo de 5 días hábiles. La audiencia de conciliación podrá ser suspendida hasta en dos ocasiones, por el conciliador o a instancia de ambas partes y se reanudará en la fecha y hora que al efecto se señalen.

Cuando alguna de las partes no pueda acudir a la audiencia en el día y hora señalados, tendrá un plazo de 3 días hábiles para justificar su ausencia, en cuyo caso se convocará a una segunda audiencia. Si no se justifica la inasistencia o no se acude a esta segunda audiencia, se continuará con el procedimiento de protección de derechos.

De cada audiencia de conciliación se levantará un acta en la que conste el resultado de la misma, la cual será firmada por el titular y el Responsable o sus respectivos representantes; sin embargo en caso de negarse a firmar alguna de las partes, se hará constar la negativa sin afectar su validez.

En caso de lograr la conciliación entre el titular y el Responsable, se deberá emitir un acuerdo de conciliación por escrito con efectos vinculantes para las partes, en donde se señalará un plazo para su cumplimiento, el cual será verificado por el IFAI. Durante este periodo de cumplimiento el plazo para emitir la resolución será suspendido. Una vez acreditado el cumplimiento del acuerdo se dará por concluido el procedimiento de protección de derechos, sin embargo en caso de no cumplirse éste será reanudado.

Si las partes no llegaren a algún arreglo en la audiencia de conciliación, el procedimiento de protección de derechos continuará con la etapa siguiente, es decir la de pruebas. Asimismo, cuando no se lleva a cabo la conciliación, la etapa de pruebas inicia después de concluido el plazo de los 15 días hábiles concedidos al Responsable en el acuerdo de admisión, para que manifieste lo que a su derecho convenga.

La etapa de pruebas se encuentra regulada en los artículos 45, quinto párrafo de la LFPDPPP y 118 y 119 de su Reglamento, para la cual presentamos el siguiente diagrama de flujo:

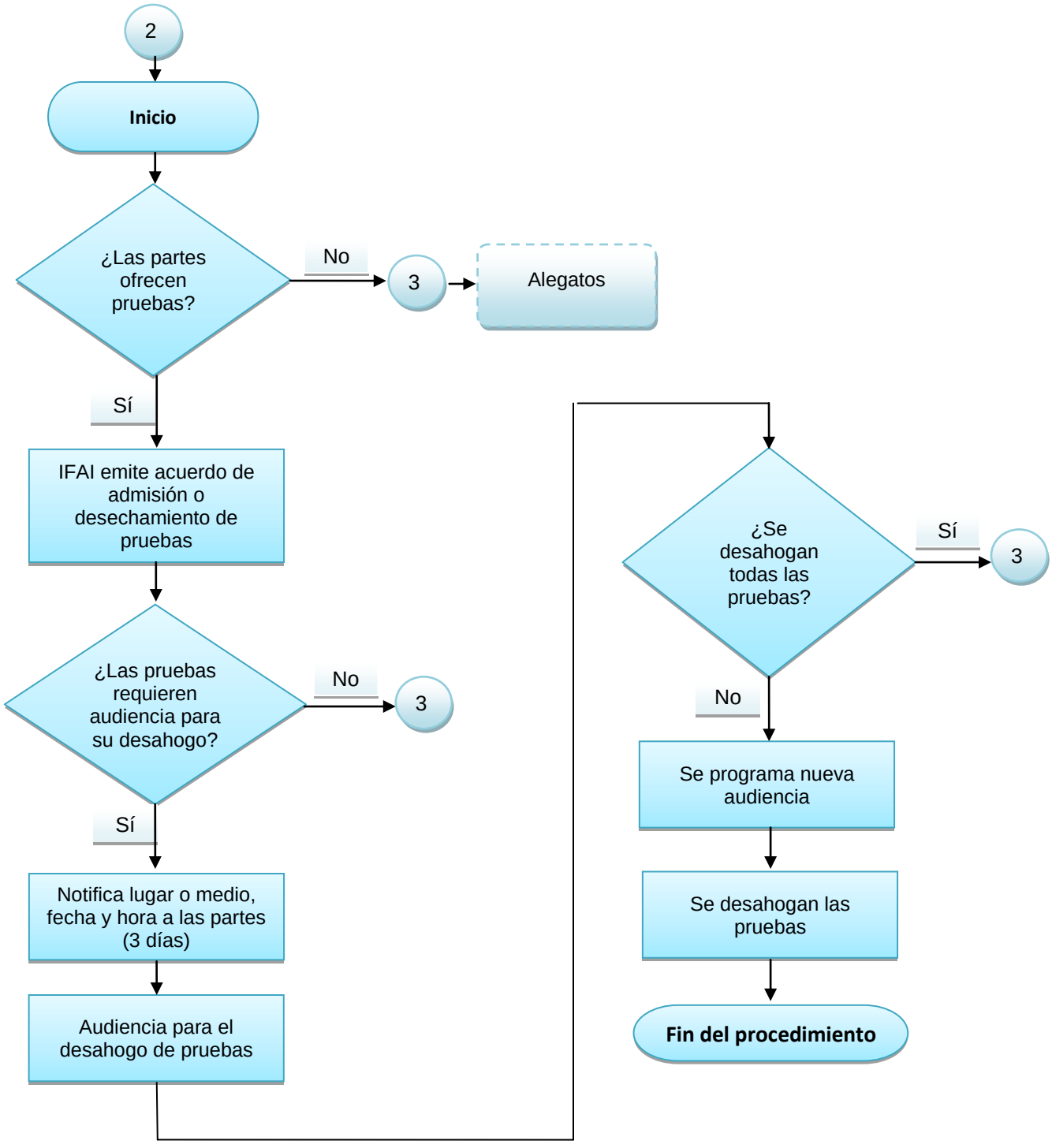


Diagrama de flujo elaborado por la tesista con base en la LFPDPPP y su Reglamento

Es importante señalar que el IFAI cuenta con facultades suficientes para solicitar del Responsable las demás pruebas que estime necesarias, conforme con lo señalado en el artículo 45, quinto párrafo de la LFPDPPP. Sin embargo es posible solicitarlas a cualquiera de las partes, de acuerdo con lo dispuesto en el artículo 50, párrafo segundo de la LFPA, en el cual se establece la facultad de la autoridad para allegarse de los medios de prueba que considere necesarios. Por otra parte, en términos de lo señalado en el artículo 20 del Reglamento de la LFPDPPP, para efectos de demostrar la obtención del consentimiento del titular, la carga de la prueba recaerá en todos los casos, en el Responsable.

Como se ha ya señalado, con fundamento en lo dispuesto en el artículo 5, segundo párrafo de la LFPDPPP, se aplicarán de manera supletoria, para la sustanciación del procedimiento de protección de derechos, las disposiciones del CFPC y de la LFPA, en este caso para la etapa de pruebas, las relativas a su admisión o desechamiento, desahogo y valoración.

La etapa de pruebas iniciará con el acuerdo de admisión o desechamiento de las pruebas ofrecidas por las partes, las cuales en términos del artículo 119 del Reglamento de la LFPDPPP podrán consistir en las siguientes:

- Documentales públicas o privadas.
- De inspección, siempre y cuando se realice a través de autoridad competente.
- Presuncional, en su doble aspecto, legal y humana.
- Pericial, deberá ir acompañada del escrito donde se precisen los hechos sobre los que debe versar la prueba, así como el nombre y domicilio del perito y el cuestionario respectivo en preparación de la misma. Sin estos requisitos se tendrá por no ofrecida la prueba.
- Testimonial, deberá ir acompañada del escrito donde se precisen los hechos sobre los que debe versar la prueba, así como los nombres y domicilios de los testigos y el interrogatorio respectivo en preparación de la misma. Sin estos requisitos se tendrá por no ofrecida la prueba.
- Las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y la tecnología.

Cabe mencionar que de las pruebas antes citadas no se encuentra la confesional, en los mismos términos que lo establece la LFPA. Por otro lado, en relación con la prueba de inspección destacamos el señalamiento que sólo procederá si se realiza a través de autoridad competente, sin precisar qué tipo de autoridad podrá llevarla a cabo, si judicial o administrativa, o si la podrá realizar el propio personal del IFAI. Por lo que se refiere a la prueba de inspección, el artículo 379 del CFPC establece: “Cuando una parte requiera indispensablemente, para

entablar una demanda la inspección de determinadas cosas, documentos, libros o papeles, la autoridad judicial puede decretar su exhibición, previa comprobación del derecho con que se pide la medida y de la necesidad de la misma".

En ese sentido, la autoridad ante quien se está llevando el procedimiento de protección de derechos, puede determinar se lleve a cabo la inspección solicitada por alguna de las partes; en este caso sería la autoridad competente del IFAI que cuente con facultades para ello. De conformidad con lo dispuesto en el artículo 37 fracciones I, II y III del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos[133] (Reglamento Interior del IFAI), el Director General de Sustanciación y Sanción es la autoridad facultada para aplicar la normatividad para la sustanciación de los procedimientos de protección de derechos y de imposición de sanciones previsto en la LFPDPPP y sustanciar los mismos. Sin embargo, de acuerdo con el artículo 39 fracciones I y VI del Reglamento Interior del IFAI, el Director General de Verificación es quien tiene atribuciones para realizar investigaciones, dictaminar y emitir opiniones en materia de vigilancia y verificación relacionadas con el cumplimiento de la LFPDPPP, la LFTAIPG, sus respectivos Reglamentos y demás disposiciones aplicables, así como requerir a particulares y autoridades, la información o documentación necesaria para su investigación.

De esta manera, consideramos que el Director General de Sustanciación y Sanción tiene atribuciones para ordenar se lleve a cabo la inspección, pues es quien sustancia el procedimiento de protección de derechos, pero será el personal de la Dirección General de Verificación quien la lleve a cabo, por tener la facultad para dicha actuación, así como el personal técnico para realizarla. Es importante tomar en cuenta que actualmente la mayoría de los datos personales son tratados a través de medios electrónicos o que requieren de cierta tecnología, por tanto será más probable que la prueba de inspección verse sobre la verificación de las bases de datos de los Responsables, lo cual requerirá de expertos en esas materias.

Por otra parte, y en cuanto al desechamiento de pruebas, el artículo 50 de la LFPA señala que sólo podrán rechazarse aquellas pruebas que no fuesen ofrecidas conforme a derecho, no tengan relación con el fondo del asunto, sean improcedentes e innecesarias o contrarias a la moral y al derecho.

Si por la naturaleza de las pruebas se requiere para su desahogo la celebración de una audiencia, en el acuerdo de admisión de las mismas se señalará lugar o medio, fecha y hora para su celebración, la cual debe notificarse con una

[133] El Reglamento Interior del IFAI fue publicado en el DOF el 29 de octubre de 2012 y abroga el publicado el 2 de mayo de 2007.

anticipación de 3 días de llevarse a cabo las actuaciones y sólo podrá posponerse por causa justificada. De cada audiencia se levantará el acta correspondiente.

El desahogo de las pruebas, de acuerdo con el artículo 51 de la LFPA, se realizará dentro de un plazo no menor a tres ni mayor de quince días, contado a partir de su admisión, y si se ofreciesen pruebas que ameriten ulterior desahogo, se concederá al interesado un plazo no menor de 8 ni mayor de 15 días para tal efecto.

Una vez desahogadas todas las pruebas se procederá conforme el artículo 45, párrafo quinto de la LFPDPPP donde en la parte conducente menciona lo siguiente: "Concluido el desahogo de las pruebas, el Instituto notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación".

De la lectura del texto anterior, se desprende que el Responsable es el único que podrá presentar alegatos, lo cual evidentemente es un error, mismo que fue subsanado en el artículo 122 del Reglamento de la LFPDPPP, al señalar que "Dictado el acuerdo que tenga por desahogadas todas las pruebas, se pondrán las actuaciones a disposición de las partes, para que éstos, en caso de quererlo, formulen alegatos …".

Concluido el plazo de los 5 días hábiles para formular alegatos, se cerrará la instrucción y el IFAI emitirá su resolución en el plazo de 50 días hábiles contando a partir de la solicitud de protección de derechos, el cual durante el procedimiento puede ser ampliado por el Pleno del IFAI con causa justificada, una sola vez y hasta por un periodo igual de dicho plazo, dando un total de 100 días hábiles para resolver.

Dicho plazo sólo podrá ser suspendido en caso de prevención y durante el periodo de cumplimiento del acuerdo de conciliación. Sin embargo, pensemos en un caso hipotético donde los tiempos de notificación y demás actuaciones del procedimiento se dan al límite de los plazos. Por ejemplo, presentada la solicitud de protección de derechos por el titular donde manifiesta su voluntad para conciliar, se corre traslado de ella y se notifica al Responsable, quien dentro de los 10 días también manifiesta su voluntad para conciliar. Se fija fecha de audiencia de conciliación[134] y llegado el día para su celebración, una de las partes no se presenta, por lo que se le otorgan 3 días para justificar su ausencia. Una vez justificada la inasistencia, se fija otro día y hora de audiencia, la cual es suspendida por el

[134] En este caso hipotético, las fechas para la celebración de las audiencias de conciliación, son señaladas dentro de los 10 días hábiles siguientes a la notificación correspondiente, de conformidad con lo dispuesto por el artículo 595 del CFPC.

conciliador hasta en dos ocasiones; sin embargo, las partes no logran llegar a un acuerdo, por lo cual se continúa con el procedimiento.

Para ese momento, ya transcurrieron un poco más de 50 días hábiles, con lo cual se rebasa el plazo señalado en el referido artículo 47 de la LFPDPPP, y aunque es posible solicitar su ampliación, todavía faltaría por llevar a cabo la etapa de pruebas, la cual puede llegar a ser igualmente extensa, cuando por la naturaleza de las mismas sea necesario la celebración de audiencias para su desahogo.

Como podemos observar con dicho caso hipotético, el tiempo de resolución resulta insuficiente, aun si se autoriza su ampliación, por lo cual sería conveniente analizar la posibilidad de suspenderlo también durante el tiempo de la conciliación y no sólo cuando exista un acuerdo entre las partes, y con mayor razón si tomamos en cuenta que en cualquier momento, durante el procedimiento, puede ser solicitada. De esta forma, con la suspensión de plazo durante la conciliación, se aprovecharía el plazo para emitir resolución y su ampliación, para sustanciar el procedimiento de protección de derechos, especialmente para el desahogo de pruebas que así lo requieran.

Por otra parte, la resolución que ponga fin al procedimiento será emitida por el Pleno del IFAI y podrá ser en cualquiera de los siguientes sentidos, según lo dispuesto en el artículo 51 de la LFPDPPP:

1) Sobreseer o desechar la solicitud de protección de derechos por improcedente, o
2) Confirmar, revocar o modificar la respuesta del Responsable.

De acuerdo con el artículo 52 de la LFPDPPP, la solicitud de protección de derechos puede ser desechada por improcedente cuando:

1) El IFAI no sea competente.
2) El IFAI haya conocido anteriormente de la solicitud de protección de derechos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente.
3) Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo.
   Este punto implica que el derecho a la protección de datos también puede ser recurrido por otros medios ante autoridades jurisdiccionales.
4) Se trate de una solicitud de protección de derechos ofensiva o irracional.
5) Sea extemporánea.

Por lo que se refiere al sobreseimiento, el artículo 53 de la LFPDPPP señala los siguientes cuatro supuestos:

1) El titular fallezca.
2) El titular se desista de manera expresa.
3) Admitida la solicitud de protección de derechos, sobrevenga una causal de improcedencia, y
4) Por cualquier motivo quede sin materia la misma.

En cuanto al cumplimiento o ejecución de las resoluciones emitidas por el IFAI en el procedimiento de protección de derechos, no existe disposición alguna que regule la forma cómo se llevará a cabo su seguimiento o la consecuencia ante un posible incumplimiento. No obstante lo anterior, en el procedimiento de verificación se establece en su artículo 59 de la LFPDPPP que: “La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos …”.

Luego entonces, el incumplimiento de una resolución dictada en el procedimiento de protección de derechos será motivo para iniciar de oficio un procedimiento de verificación, sin embargo consideramos que en este caso y después de sustanciar el procedimiento de protección de derechos, la conducta violatoria del Responsable ya se encuentra debidamente acreditada, no siendo necesaria la verificación, sino basta la inobservancia de una determinación de la autoridad, no recurrida, para confirmar dicha conducta como contraria a la LFPDPPP. De esta manera, sería viable proceder directamente con la imposición de una sanción, e incluir dicho incumplimiento como infracción en la ley.

Por otro lado, la LFPDPPP establece si como resultado del estudio realizado por el IFAI para resolver el procedimiento de protección de derechos, el IFAI observare alguna probable violación a la LFPDPPP y su Reglamento, éste resolverá se inicie con el procedimiento de imposición de sanciones. Bajo este supuesto consideramos se debe justificar dicha actuación, mediante el señalamiento preciso de la probable conducta del Responsable, así como los principios y preceptos vulnerados de la LFPDPPP y su Reglamento. No obstante ello, proponemos la viabilidad para que la autoridad cuente con las facultades necesarias para imponer sanciones desde este procedimiento de protección de derechos, cuando derivado de las actuaciones observare claramente una infracción y cuente con elementos suficientes para acreditarla, ya sin necesidad de iniciar un procedimiento de imposición de sanciones.

Finalmente es importante mencionar la relevancia e impacto social de este y todos los procedimientos previstos en la LFPDPPP y su Reglamento, los cuales si bien son de naturaleza administrativa, tienen una función especial que los hace diferentes frente a los demás, la de garantizar el derecho a la protección de datos personales, reconocido como derecho fundamental y previsto en nuestra Carta Magna. De esta manera, el compromiso de la autoridad encargada de garantizarlo (IFAI) será mayor, y la forma más evidente de cumplirlo será a través de sus resoluciones, en las cuales dada la trascendencia de esta encomienda, deberá valorar los hechos y constancias presentadas por las partes, no sólo con la ley de la materia y su reglamento y leyes supletorias, sino también con aquél conjunto de principios e instrumentos internacionales que también forman parte del sistema jurídico mexicano y en los cuales se establecen las bases de este derecho fundamental y a los cuales las autoridades están obligadas a aplicar bajo el principio de *pro homine* o *pro personae*, a fin brindar su más amplia y adecuada salvaguarda.

III. Procedimiento de verificación.

El procedimiento de verificación regulado en los artículos 59 y 60 de la LFPDPPP inicia a través de instrucción emitida por el Pleno del IFAI debidamente fundada y motivada, bajo alguna de las siguientes formas:

1) A petición de parte, a través de la denuncia, o
2) De oficio, cuando la autoridad presuma fundada y motivadamente la existencia de violaciones a la LFPDPPP y su Reglamento, o cuando exista incumplimiento de las resoluciones emitidas en el procedimiento de protección de derechos.

El objeto del procedimiento de verificación se señala en el artículo 128 del Reglamento de la LFPDPPP y consiste en el siguiente: “El Instituto, con el objeto de comprobar el cumplimiento de las disposiciones previstas en la Ley o en la regulación que de ella derive, podrá iniciar el procedimiento de verificación, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas”.

Este procedimiento se encuentra regulado en los artículos 59 y 60 de la LFPDPPP y del 128 al 139 de su Reglamento, y se lleva a cabo de la siguiente manera:

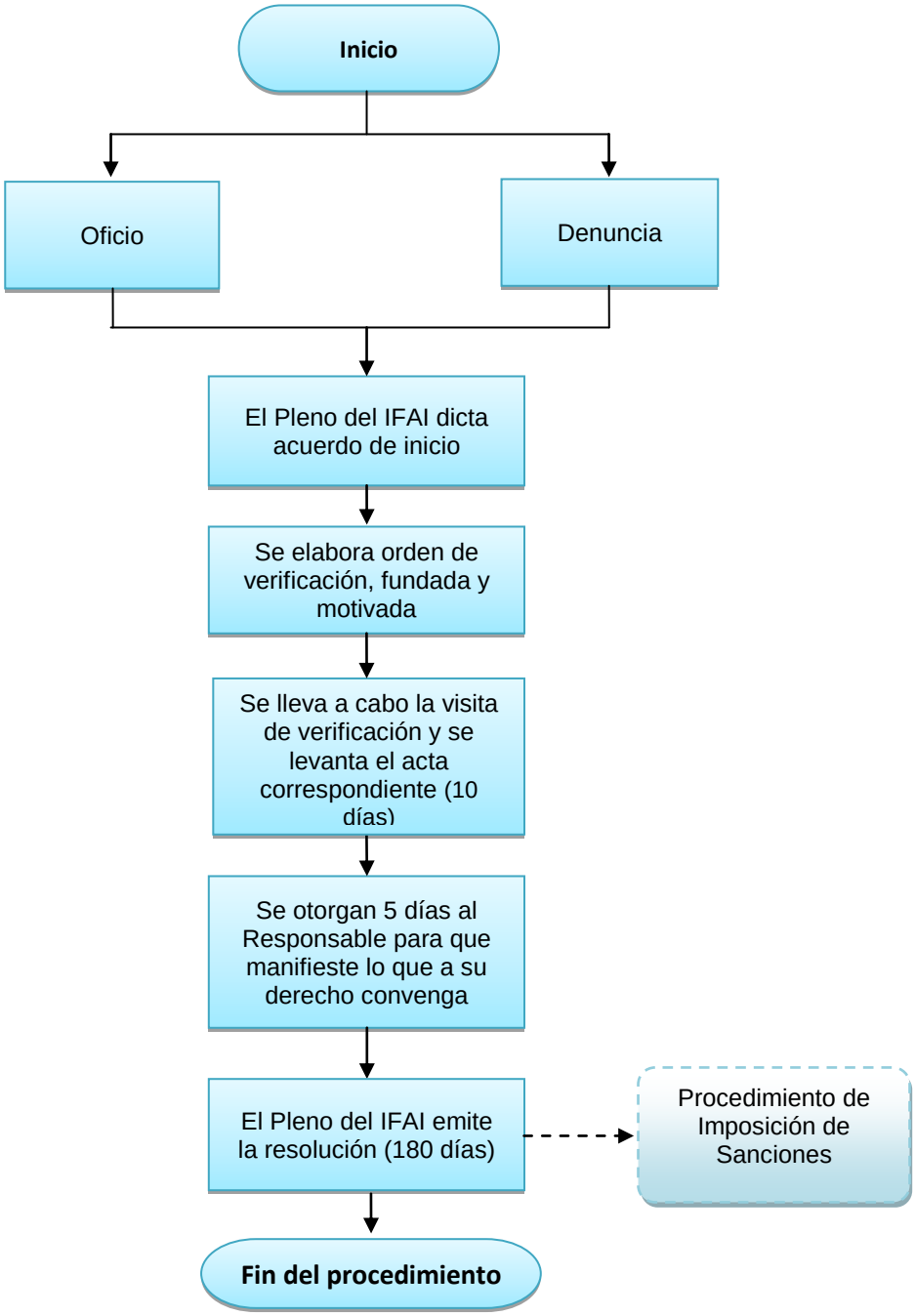


Diagrama de flujo elaborado por la tesista con base en la LFPDPPP y su Reglamento

Un punto relevante es el señalado en el artículo 130 del Reglamento de la LFPDPPP, donde se establece lo siguiente: “En el ejercicio de las funciones de verificación, el personal del IFAI estará dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo”. De lo anterior puede entenderse que todo el personal del IFAI está investido de fe pública, sin embargo dicha disposición limita esta facultad únicamente para la verificación, luego entonces, el personal que estará dotado de dicha fe, será quien cuente con atribuciones para verificar.

Así las cosas, y de conformidad con lo dispuesto en el artículo 39 del Reglamento Interior del IFAI, la Dirección General de Verificación, adscrita a la Secretaría de Protección de Datos Personales del IFAI, tiene atribución para realizar verificaciones, por tanto su personal será el único que cuente con fe pública. Aunado a lo anterior, para llevar a cabo la verificación, dicho personal deberá contar con orden escrita fundada y motivada suscrita por autoridad competente, la cual con fundamento en el artículo 24 fracción XX del Reglamento Interior del IFAI corresponde al Secretario de Protección de Datos Personales. Dicha orden de verificación debe contener:

- Lugar en donde se encuentra el establecimiento del Responsable o las bases de datos objeto de la verificación.
- Objeto de la visita.
- Alcance de la visita.
- Disposiciones legales que la fundamenten.

Al respecto, es de comentar que el referido artículo 24 fracción XX del Reglamento Interior del IFAI establece que el Secretario de Protección de Datos Personales también tiene atribuciones para suscribir oficios de comisión para la sustanciación del procedimiento de verificación, por lo cual además de la orden de verificación, el verificador cuenta con su oficio de comisión, sin embargo sería conveniente que en el Reglamento Interior del IFAI se previera expresamente la figura de los verificadores y se establecieran sus atribuciones.

La Dirección General de Verificación tendrá facultades para solicitar el acceso a la información y documentación que consideren necesaria o realizar las visitas en el establecimiento en donde se encuentren las bases de datos respectivas, siempre y cuando cuenten con resolución que motive dichas actuaciones. Por otra parte, su personal tendrá en todo momento la obligación de guardar confidencialidad sobre la información que conozcan con motivo de la verificación, lo cual también debe aplicar para todo servidor público que en el ejercicio de sus funciones tenga conocimiento de dicha información.

En cuanto al procedimiento de verificación, como se mencionó antes puede iniciar con la denuncia, la cual a diferencia de la solicitud de protección de derechos, puede ser presentada por cualquier persona, siempre y cuando las presuntas violaciones manifestadas, no se encuentren en alguno de las causales de procedencia del procedimiento de protección de derechos, señaladas en el artículo 115 del Reglamento de la LFPDPPP, ya comentadas. En caso de encontrarse en una de estas casuales, el asunto será turnado en un plazo no mayor a 10 días hábiles, contados a partir de la recepción de la solicitud, a la unidad administrativa competente, es decir la Dirección General de Sustanciación y Sanción, quien podrá iniciar el procedimiento de protección de derechos.

La denuncia podrá ser presentada por escrito libre, por los formatos establecidos para esos efectos o a través del sistema que establezca el IFAI, y deberá cumplir con los siguientes requisitos señalados en el artículo 131 del Reglamento de la LFPDPPP:

- Nombre del denunciante y el domicilio o el medio para recibir notificaciones.
- Relación de los hechos en los que basa su denuncia y los elementos con los que cuente para probar su dicho, y
- Nombre y domicilio del denunciado o, en su caso, datos para su ubicación.

Además de lo anterior, el IFAI tendrá la facultad para solicitar la documentación que estime oportuna para el desarrollo del procedimiento. Una vez dictado por el Pleno del IFAI el acuerdo de inicio del procedimiento de verificación, empezará a correr el plazo máximo de 180 días hábiles para llevarlo a cabo y concluirlo. Este plazo también podrá ser ampliado por una sola vez y hasta por un periodo igual, es decir hasta 360 días hábiles, plazo que puede llegar a ser excesivo sino está debidamente justificado.

Para la sustanciación de este procedimiento también serán de aplicación supletoria las disposiciones del CFPC y de la LFPA conforme se establece en el artículo 5, párrafo segundo de la LFPDPPP. Durante el procedimiento de verificación, se podrán realizar cuántas verificaciones sean necesarias, sin embargo cada una tendrá como plazo máximo para su realización 10 días hábiles, el cual deberá ser notificado al Responsable o encargado y, en su caso, al denunciante. La LFPDPPP no establece si las visitas también podrán ser extraordinarias, es decir que se pueden realizar en cualquier tiempo, sin embargo al estar contempladas en el artículo 62 de la LFPA, se considera ello posible.

En cada visita, el personal verificador deberá identificarse con credencial vigente con fotografía, expedida por el IFAI que lo acredite para desempeñar dicha función y exhibir la orden de verificación, de la cual dejará en copia a quien atienda la visita. De conformidad con lo señalado en el artículo 64 de la LFPA, los propietarios, responsables, encargados u ocupantes de establecimientos objeto de verificación, están obligados a permitir el acceso y brindar las facilidades e informes a los verificadores para el desarrollo de su labor. La obstrucción a los actos de verificación es considerada como infracción y será sancionada a través del procedimiento de imposición de sanciones con multa.

Al concluir la visita de verificación se levantará en presencia de dos testigos, un acta en original y por duplicado, donde consten las actuaciones practicadas durante la verificación. El acta será firmada por el verificador actuante y sólo para constancia de recepción, por la persona que haya atendido la visita, quien en caso de negarse a firmar se dejará constancia de su negativa en el acta, sin afectar su validez, de la cual se le entregará un ejemplar en original.

La persona que atiende la diligencia puede formular sus observaciones en el acto de verificación y manifestar lo que a su derecho convenga, o bien, posteriormente y por escrito, dentro del término de 5 días siguientes a la fecha del acta de verificación.

Concluidas las actuaciones de verificación, las constancias se someterán al Pleno del IFAI para la emisión de la resolución correspondiente, en la cual podrá establecer:

1) Las medidas que deberá adoptar el Responsable y su plazo de cumplimiento.
2) Instruir el inicio del procedimiento de imposición de sanciones o establecer un plazo para dicho efecto.

Al igual que sucede en el procedimiento de protección de derechos, en el procedimiento de verificación no se otorgan facultades expresas al personal verificador para aplicar medidas precautorias durante las visitas,[135] ni tampoco regula la forma como se exigirá el cumplimiento de las medidas establecidas en la resolución, en caso de su inobservancia. De esta manera, se reitera la propuesta de tomar esta conducta del Responsable como una infracción sancionada conforme a la LFPDPPP, de lo contrario se seguirán llevando a cabo procedimientos infructuosos que concluyan con resoluciones carentes de fuerza, por no contar con las medidas y

[135] El artículo 39 fracción VII del Reglamento Interior del IFAI otorga atribuciones genéricas a la Dirección General de Verificación para suscribir todo tipo de actuaciones y resoluciones para el desarrollo de las investigaciones que lleve a cabo.

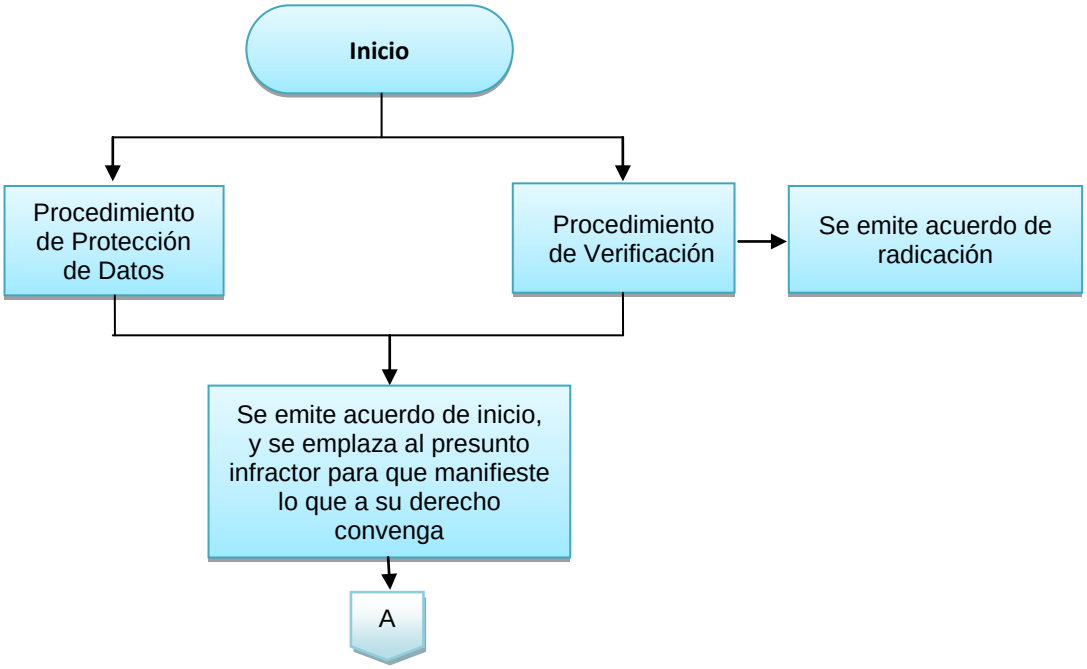
mecanismos adecuados para su ejecución, lo cual ineludiblemente afectará en la salvaguarda del derecho fundamental a la protección de datos personales.

IV. Procedimiento de imposición de sanciones.

El procedimiento de imposición de sanciones inicia como resultado de la sustanciación de los procedimientos de protección de derechos o de verificación, donde al determinar presuntas infracciones a la LFPDPPP susceptibles de ser sancionadas, se instruirá, a través de resolución, el inicio de este procedimiento.

De acuerdo con lo dispuesto en el artículo 37 del Reglamento Interior del IFAI, la Dirección General de Sustanciación y Sanción, adscrita a la Secretaría de Protección de Datos Personales del IFAI, es la autoridad competente para sustanciar el procedimiento de imposición de sanciones.

El procedimiento de imposición de sanciones, regulado en los artículos 61 y 62 de la LFPDPPP y del 140 al 143 de su Reglamento, iniciará con la notificación del acuerdo de inicio realizada al presunto infractor, la cual irá acompañada de un informe donde se describan los hechos constitutivos de la presunta infracción, procedimiento que se explica con el siguiente diagrama de flujo:



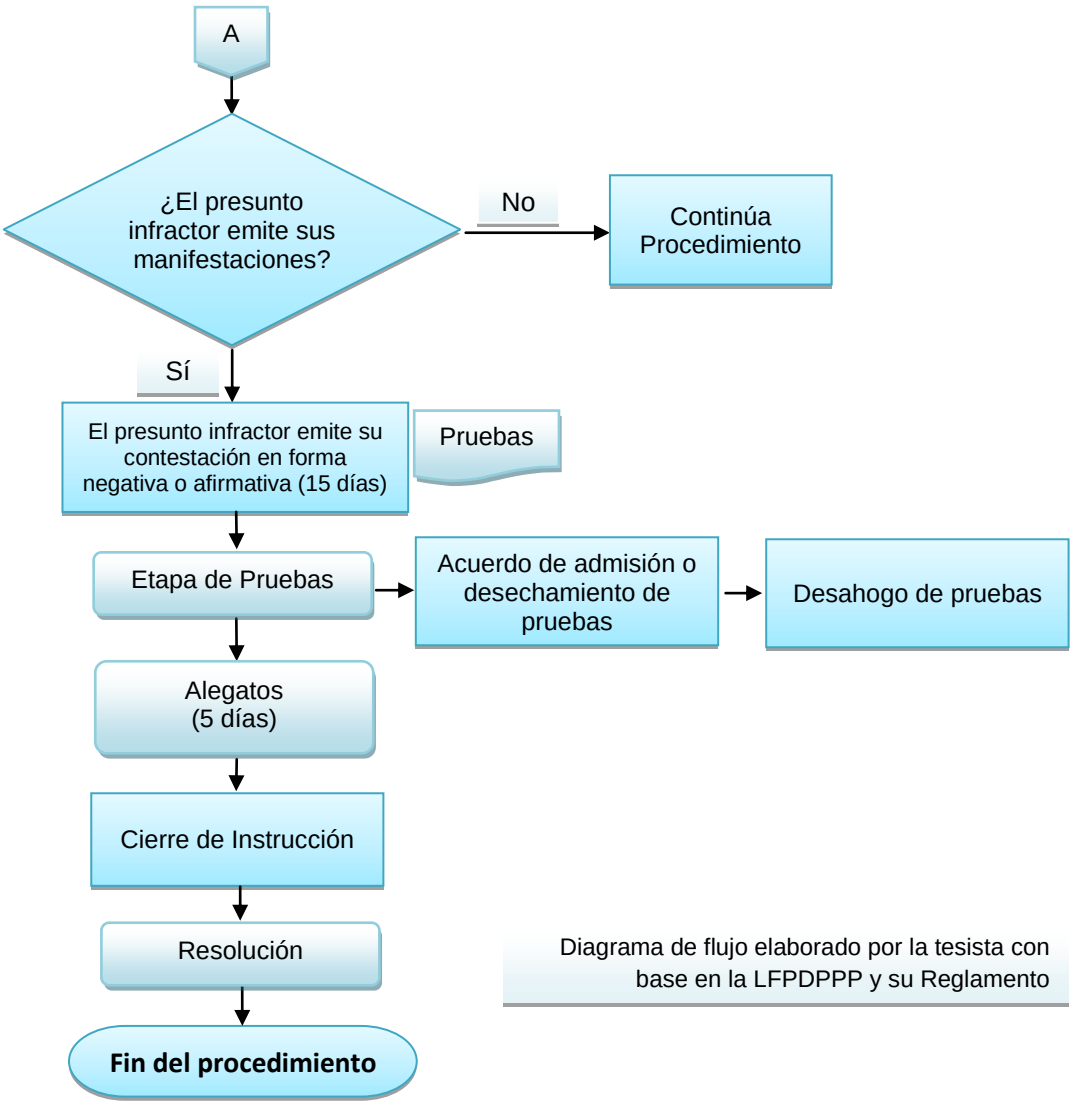


Diagrama de flujo elaborado por la tesista con base en la LFPDPPP y su Reglamento

En dicho acuerdo se emplazará al presunto infractor para que en un plazo de 15 días hábiles, contados a partir de que surte efectos la notificación, manifieste lo que a su derecho convenga y rinda las pruebas. En caso de no presentar pruebas, el IFAI resolverá conforme a los elementos de convicción de que disponga, sin embargo cuenta con la facultad para solicitar del presunto infractor, las pruebas que estime necesarias para el procedimiento.

La contestación del presunto infractor debe versar sobre cada uno de los hechos que se le imputan, ya sea afirmándolos o negándolos, en donde deberá señalar cómo ocurrieron o que los ignora por no ser propios. Asimismo debe exponer sus argumentos para desvirtuar la presunta infracción, y presentar las pruebas correspondientes.

Las pruebas serán ofrecidas, admitidas o desechadas y desahogadas en los mismos términos que en el procedimiento de protección de derechos, en donde también son aplicadas de manera supletoria las disposiciones del CFPC y la LFPA.

Concluido el desahogo de pruebas se notificará al presunto infractor que cuenta con un plazo de 5 días hábiles siguientes a su notificación, para presentar alegatos y vencido dicho plazo se ordenará el cierre de instrucción para la emisión de la resolución.

En relación con el plazo para emitir la resolución de no mayor de 50 días hábiles, cabe hacer la siguiente precisión, toda vez que no queda muy claro a partir de cuándo empezará a correr. Al respecto el artículo 62, tercer párrafo de la LFPDPPP indica: “El Instituto … resolverá en definitiva dentro de los cincuenta días siguientes a la fecha en que inició el procedimiento sancionador”. Por su parte ese mismo artículo de la LFPDPPP, en su párrafo primero señala: “El procedimiento de imposición de sanciones dará comienzo con la notificación que efectúe el Instituto al presunto infractor …”.

En ese sentido el plazo máximo de 50 días hábiles para emitir la resolución, se computará a partir de la fecha de notificación al presunto infractor del acuerdo de inicio del procedimiento. Este plazo al igual que en los procedimientos antes aludidos, podrá ser ampliado por una sola vez y hasta por un periodo igual, en este caso hasta 100 días hábiles.

Ahora bien, el artículo 63 de la LFPDPPP señala 19 supuestos de infracción a la LFPDPPP, a las que le corresponden sus debidas sanciones, establecidas en el artículo 64 de la LFPDPPP, las cuales pueden consistir en apercibimiento, aplicable para el primer supuesto, y las multas para los demás casos. Las resoluciones del IFAI deben ir como toda resolución o acto de autoridad debidamente fundada y motivada, para lo cual deberá tomar en consideración los siguientes elementos o criterios señalados en el artículo 65 de la LFPDPPP para la imposición de sanciones:

- La naturaleza del dato. Se debe tomar en cuenta si los datos se refieren a datos sensibles, pues de ser el caso, las sanciones se duplicarán.
- La notoria improcedencia de la negativa del Responsable, para realizar los actos solicitados por el titular, en términos de la LFPDPPP. Al respecto consideramos que la expresión “improcedencia de la negativa” no es muy adecuada y puede ser incluso confusa en su interpretación, por lo cual sugerimos entender este supuesto simplemente como aquella negativa injustificada por parte del Responsable, para realizar los actos solicitados por el titular. Por otra parte, este supuesto puede aplicarse para el caso de resoluciones no observadas por el Responsable, emitidas en los procedimientos de protección de derechos, en donde se ordenó el cumplimiento de la solicitud del titular, como consecuencia de la revocación o modificación de su respuesta.

- El carácter intencional o no, de la acción u omisión constitutiva de la infracción. Este es un elemento subjetivo relacionado con la determinación de voluntad del sujeto para realizar o no cierta conducta, en este caso alguna de las señaladas en la LFPDPPP como infracción, el cual será acreditado conforme a cada caso en particular.
- La capacidad económica del Responsable. Es de advertirse que en el procedimiento de imposición de sanciones no se otorga alguna facultad expresa al IFAI para solicitar del Responsable, aquellos documentos con los cuales acredite su solvencia económica, la cual evidentemente es indispensable para fijar la multa. De esta manera, se considera indispensable que el IFAI, en atención a sus facultades genéricas para solicitar cualquier elemento de convicción o prueba que estime necesario, requiera al Responsable desde el inicio del procedimiento, para presentar la documentación que acredite su capacidad económica.
- La reincidencia. Implica la existencia previa de una misma infracción sancionada por la autoridad. Las conductas reiteradas en infracciones serán sancionadas a través de una multa adicional.

Un punto importante a considerar para la imposición de sanciones es el artículo 63 de la LFPDPPP, donde en su primer párrafo se observa que las infracciones serán conductas llevadas a cabo por el Responsable, entonces ¿es posible sancionar a otros sujetos que también tratan datos personales y realizan conductas violatorias a la ley?

De acuerdo con lo dispuesto en el artículo 53, segundo párrafo del Reglamento de la LFPDPPP, el Encargado[136] tendrá el carácter de Responsable y las mismas obligaciones propias de éste, cuando destine o utilice los datos personales con una finalidad distinta a la autorizada por el Responsable, o cuando efectúe una transferencia, incumpliendo sus instrucciones. Asimismo, conforme al artículo 72 del Reglamento de la LFPDPPP, el receptor de los datos personales será un sujeto regulado por la LFPDPPP y su Reglamento, en su carácter de Responsable, y deberá tratar los datos personales conforme a lo convenido en el aviso de privacidad que le comunique el Responsable transferente. En consecuencia existen dos sujetos, el Encargado y el receptor, que también son considerados por la LFPDPPP como Responsables, por lo cual en nuestra opinión, aquéllos pueden ser sancionados de la misma manera, en caso de realizar una infracción a la ley de la materia.

[136] De conformidad con el artículo 3, fracción IX de la LFPDPPP, el Encargado es la persona física o jurídica que sola, o conjuntamente con otras, trate datos personales por cuenta del Responsable.

Es importante considerar para efectos de la debida fundamentación y motivación de la resolución emitida en el procedimiento de imposición de sanciones, la estrecha relación que hay entre una infracción y la vulneración a los principios establecidos en la LFPDPPP y su Reglamento, los cuales como ya fue comentado, también son obligaciones para el Responsable. De esta forma, consideramos que en la revisión de las infracciones a la LFPDPPP, el IFAI deberá analizar si el infractor vulneró igualmente alguno de los ocho principios rectores,[137] como se presenta a continuación:

ARTÍCULO 63 DE LA LFPDPPP		PRINCIPIOS VULNERADOS
I.	No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;	Licitud
II.	Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;	Calidad, Lealtad y Responsabilidad
III.	Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;	Lealtad y Responsabilidad
IV.	Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;	Los ocho Principios Rectores de la Protección de Datos Personales y el Criterio de minimización
V.	Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;	Consentimiento, Información, Finalidad y Proporcionalidad
VI.	Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;	Calidad
VII.	No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;	Licitud
VIII.	Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;	Lealtad y Responsabilidad
IX.	Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto en el artículo 12;	Consentimiento, Finalidad, Proporcionalidad y Criterio de minimización
X.	Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó a la divulgación de los mismos;	Responsabilidad
XI.	Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;	Responsabilidad
XII.	Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;	Licitud, Consentimiento y Responsabilidad
XIII.	Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;	Consentimiento

[137] De acuerdo con el artículo 6 de la LFPDPPP y el 9 de su Reglamento, los ocho principios rectores de la protección de datos personales son: Licitud, Consentimiento, Información, Calidad, Finalidad, Lealtad, Proporcionalidad y Responsabilidad.

XIV.	Obstruir los actos de verificación de la autoridad;	No se considera que se vulnere alguno de los principios rectores, en razón de que esta conducta se da entre el presunto infractor y el IFAI.
XV.	Recabar datos en forma engañosa y fraudulenta;	Lealtad
XVI.	Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;	Consentimiento y Calidad
XVII.	Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;	Los ocho Principios Rectores de la Protección de Datos Personales
XVIII.	Crear bases de datos en contravención a lo dispuesto en el artículo 9, segundo párrafo de esta Ley, y	Licitud, Finalidad, Proporcionalidad y el Criterio de minimización
XIX.	Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.	Los ocho Principios de Protección de Datos y el Criterio de minimización

En cuanto a las sanciones que se aplicarán a estas infracciones, éstas se encuentran en el artículo 64 de la LFPDPPP, en donde no se señalan expresamente cuáles infracciones serán consideradas como leves y cuáles como graves; sin embargo al revisar la sanción (apercibimiento o multas) que corresponde a cada uno de los supuestos de infracción antes vistos, podemos determinar la gravedad de la conducta realizada, especialmente por el incremento de los montos de las multas. Así las conductas más graves en materia de protección de datos serán aquellas que involucren el tratamiento de datos sensibles, así como los casos de reincidencia y las más leves serán aquellas cuya sanción a aplicar sea el apercibimiento.

De acuerdo con el artículo 64, fracción I, en relación con el 63, fracción I, ambos de la LFPDPPP, el apercibimiento únicamente se dará cuando el Responsable no cumpla con la solicitud del titular para el acceso, rectificación cancelación y oposición al tratamiento de sus datos personales, sin razón fundada, en los términos de la LFPDPPP. Pero si el Responsable no cumple con dicho apercibimiento, es decir insiste en su negativa por cumplir la solicitud del titular, de conformidad con el artículo 64, fracción II, en relación con el 63, fracción VII, ambos de la LFPDPPP, se le podrá aplicar una multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal.[138]

[138] La referencia de “salario mínimo vigente en el Distrito Federal” es como se encuentra en el artículo 64 de la LFPDPPP, sin embargo se considera imprecisa, ya que de conformidad con el artículo 123, apartado A, fracción VI de la Constitución Política de los Estados Unidos Mexicanos y la “Resolución del H. Consejo de Representantes de la Comisión Nacional de los Salarios Mínimos que fija los salarios mínimos generales y profesionales vigentes a partir del 1 de enero de 2013”, publicada en el Diario Oficial de la Federación el 21 de diciembre de 2012, existen dos tipos de salarios mínimos: generales y profesionales, por lo cual para efectos de la LFPDPPP lo correcto es señalar “salario mínimo general vigente en el Distrito Federal” (SMGVDF), mención que se hará en adelante en el presente trabajo. Asimismo, de acuerdo con la referida Resolución, el

En relación con la infracción señalada en la fracción XIX del artículo 63 de la LFPDPPP, relativa a cualquier incumplimiento del Responsable a las obligaciones a su cargo, en términos de lo previsto en la ley, además de ser muy general, se encuentra desprovista de sanción, pues el artículo 64 no la incluye en alguna de sus fracciones, lo cual la convierte en una norma imperfecta.

De acuerdo con García Máynez, las leyes imperfectas son las que no se encuentran provistas de sanción, las no sancionadas jurídicamente. Dicho autor explica la existencia de este tipo de normas, ante la imposibilidad de sancionar todas las normas, de la siguiente manera: "… cada norma sancionadora tendría que hallarse garantizada por una nueva norma, y ésta por otra, y así sucesivamente. Pero como el número de los preceptos que pertenecen a un sistema de derechos es siempre limitado, hay que admitir, *a fortiori*, la existencia de normas jurídicas desprovistas de sanción".[139]

Bajo dicho argumento podemos entender la existencia de normas desprovistas sin sanción, sin embargo en el caso que nos ocupa es incomprensible, en razón de tratarse de un apartado de la ley dedicado exclusivamente al señalamiento de infracciones y sus correspondientes sanciones, por lo cual es inexcusable dicha omisión, pues aun y cuando la autoridad acredite dicho incumplimiento por parte del Responsable, estará en todo momento imposibilitada para imponer alguna sanción de las señaladas en la LFPDPPP y como consecuencia quedar impune.

En estos casos si la conducta no va a ser sancionada, por lo menos se debe establecer una recomendación al Responsable y quedar dicha conducta como un antecedente negativo a considerar en la aplicación de sanciones, para posteriores infracciones a la LFPDPPP o tal vez ordenar la verificación correspondiente para dar seguimiento al caso en concreto, y evitar con ello otro incumplimiento.

Para una mejor comprensión en las multas que corresponden a cada uno de los supuestos de infracción señalados en el artículo 63, fracciones de la II al XVIII de la LFPDPPP y a fin de observar los montos que pueden ser aplicados por el IFAI conforme a lo dispuesto en el artículo 64, fracciones de la II a la IV de la LFPDPPP, se presenta el siguiente cuadro:

SMGVDF para el año 2013 es de $64.76. Entonces la multa puede ir de $6,476.00 a $20,723,200.00.

[139] GARCÍA MÁYNEZ, Eduardo, *Introducción al estudio del Derecho*, Porrúa, quincuagésima séptima edición, México, 2004, pp. 90 y 91.

Artículo 63 Fracciones:	Multa en días de SMGVDF	Monto en pesos	Monto en pesos calculando los montos adicionales mínimos y máximos por reincidencia
II a la VII	De 100 a 160,000	De $6,476 a $10,361,600	De $12,952 a $31,084,800
VIII a la XVIII	De 200 a 320,000	De $12,952 a $20,723,200	De $19,428 a $41,446,400
IV (Reincidencia)	Multa adicional De 100 a 320,000	De $6,476 a $20,723,200	
IV (Datos sensibles)	Hasta por dos veces los montos establecidos.	De $12,952 a $20,723,200	
		De $25,904 a $41,446,400	

De lo anterior observamos que una infracción mínima puede ser sancionada con multa de $6,476.00 (seis mil cuatrocientos setenta y seis pesos 00/100 M.N.) y una infracción mayor con multa hasta de $20’723,200.00 (veinte millones setecientos veintitrés mil doscientos pesos 00/100 M.N.). Y si a este último monto máximo se le agregara el monto máximo adicional por reincidencia daría como resultado una multa por $41’446,400.00 (cuarenta y un millones cuatrocientos cuarenta y seis mil cuatrocientos pesos 00/100 M.N.).

Ahora bien, si tenemos una multa incrementada por datos sensibles en su monto máximo ($41’446,400.00) más la multa máxima adicional ($41’446,400.00) daría como resultado una multa por un importe total de $82’892,800.00 (ochenta y dos millones ochocientos noventa y dos mil ochocientos pesos 00/100 M.N.).

La intención de realizar el anterior ejercicio fue precisamente para obtener aquellos montos máximos con los cuales puede ser sancionado un Responsable por cometer infracciones a la LFPDPPP, y observar como la intención del legislador fue establecer sanciones ejemplares que inhiban el incumplimiento a la ley de la materia, por parte de los Responsables.

Lo anterior se confirma cuando además de las sanciones, en la LFPDPPP se establecen también delitos en materia del tratamiento indebido de datos personales, cuyas penas pueden ir de 3 meses a 5 años de prisión, y para datos sensibles podrán duplicarse. En los artículos 67 y 68 de la LFPDPPP se establecen dos tipos penales:

1) Al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a la base de datos bajo su custodia.
2) 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.

No obstante los delitos contemplados en la LFPDPPP sería conveniente considerar otros tipos de delitos que se encuentran estrechamente relacionados con

la materia como lo son los llamados delitos informáticos, entre los cuales se encuentran los delitos de fraude y fraude informático; falsificación informática; robo de identidad; y utilización indebida de dispositivos, mismos que hasta la fecha no se encuentran completamente regulados en el sistema jurídico mexicano, por lo menos a nivel federal,[140] al considerar únicamente la obtención de información y no el apoderamiento sin autorización, de la identidad o de datos personales. Situación de tal trascendencia y actualidad que merece un especial estudio para su consideración en el marco jurídico vigente.

Ahora bien, independientemente de las sanciones aplicadas y los delitos cometidos, los titulares también podrán iniciar un procedimiento por responsabilidad civil de conformidad con la legislación aplicable.

Finalmente y en relación al procedimiento de imposición de sanciones, cabe mencionar que la LFPDPPP no establece la forma cómo se llevará a cabo la ejecución de la resolución en la cual se imponga una multa, especialmente en caso de no ser cubierta por parte del Responsable, por lo cual será necesario que el IFAI lleve a cabo convenios con la autoridad fiscal, a fin de estar en posibilidad de exigir el cumplimiento de la sanción, de lo contrario, al igual que sucede en otros procedimientos administrativos, sus resoluciones no podrán hacerse válidas y por tanto, no se logrará cumplir el objeto de la ley, que es salvaguardar el derecho a la protección de datos en posesión de los particulares.

V. Medios de impugnación.

Los medios de impugnación que proceden en contra de las resoluciones emitidas en los procedimientos establecidos en la LFTAIPG y en la LFPDPPP, en materia de protección de datos personales, en posesión de entes públicos y privados, respectivamente, son distintos como se explica a continuación:

En la LFTAIPG se contempla el recurso de revisión, el cual procederá en los términos de los artículos 49 y 50 de dicha ley y no como se establece en el artículo 83 de la LFPA. De acuerdo con el artículo 50 de la LFTAIPG podrá ser interpuesto en cualquiera de los siguientes casos:

1) La dependencia o entidad no entregue al solicitante los datos personales solicitados, o lo haga en un formato incomprensible.

[140] En el Título Noveno del Código Penal Federal, se contemplan los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática, sin embargo aún no se considera el delito de robo de identidad. Sin embargo es importante mencionar que este último ha sido objeto de algunas iniciativas de reforma a dicho código, ante la Cámara de Diputados. Ver Gaceta Parlamentaria número 2904-II del jueves 3 de diciembre de 2009 y Gaceta Parlamentaria número 3401-V del martes29 de noviembre de 2011.

2) La dependencia o entidad se niegue a efectuar modificaciones o correcciones a los datos personales.
3) El solicitante no esté conforme con el tiempo, el costo o la modalidad de entrega.
4) El solicitante considere que la información entregada es incompleta o no corresponda a la información requerida en la solicitud.

Como se podrá observar, los anteriores supuestos son similares a las casuales de procedencia del procedimiento de protección de derechos, establecidas en el artículo 115 del Reglamento de la LFPDPPP y tanto el recurso de revisión como dicho procedimiento son interpuestos ante el IFAI, ello nos lleva a la posibilidad de establecer un sólo procedimiento para la protección de datos personales, como se pretende llegar con el presente trabajo, el cual pueda ser sustanciado por la misma autoridad y regulado bajo los mismos criterios y principios, aunque por supuesto, con ciertos bemoles de acuerdo a las particularidades del caso y según sea la naturaleza del sujeto Responsable (pública o privada).

El recurso de revisión será turnado al Comisionado ponente a fin de que integre el expediente y elabore un proyecto de resolución para presentar al Pleno del IFAI en un plazo de 30 días hábiles siguientes a la interposición del recurso. Durante dicho plazo el Pleno podrá determinar la celebración de audiencias con las partes. Una vez que el Pleno reciba el proyecto de resolución tendrá 20 días hábiles para resolver en definitiva el recurso. Dichos plazos podrán ser ampliados por una sola vez y por el mismo periodo. El plazo total para resolver el recurso de revisión será de 50 días hábiles, plazo similar al del procedimiento de protección de derechos contemplado en la LFPDPPP.

La resolución emitida por el IFAI podrá desechar o sobreseer el recurso; confirmar la decisión del Comité de Información o; revocar o modificar las decisiones del Comité de Información y ordenar a la dependencia o entidad el acceso al particular a sus datos personales, la reclasificación de la información o la modificación de los datos. En la resolución se establecerán los plazos para su cumplimiento y procedimientos para asegurar su ejecución. Asimismo de observar alguna responsabilidad por parte del servidor público, el IFAI dará vista al órgano interno de control de la dependencia o entidad, a fin de iniciar con el procedimiento de responsabilidad correspondiente.

El artículo 59 de la LFTAIPG señala que las resoluciones emitidas por el IFAI en los recursos de revisión, serán definitivas para las dependencias y entidades, pero los particulares podrán impugnarlas ante el Poder Judicial de la Federación. En términos del artículo 114, fracción II de la Ley de Amparo, los Jueces de Distrito son competentes para conocer del juicio de amparo indirecto en contra de actos que no

provengan de tribunales judiciales, administrativos o del trabajo, cuando el acto reclamado emane de un procedimiento seguido en forma de juicio, en cuyo caso el amparo sólo podrá promoverse contra la resolución definitiva por violaciones cometidas en la misma resolución o durante el procedimiento, si por virtud de estas últimas hubiere quedado sin defensa el quejoso o privado de los derechos que la ley de la materia le conceda.

Otro medio de impugnación administrativo contemplado en la LFTAIPG es la reconsideración, el cual puede ser presentado por el particular después de un año de haberse emitido la resolución, en contra de la resolución que confirme la decisión del Comité de Información, por lo que sólo podrá referirse a la misma solicitud. El plazo máximo para resolver la reconsideración será de 60 días hábiles. A pesar de ser la reconsideración otro medio con el cual cuenta el particular para impugnar una resolución, lo consideramos infructuoso porque al resolverlo la misma autoridad, es más probable que sea nuevamente confirmado. Además el lapso de un año es excesivo e inoportuno, más aún cuando se trata de proteger un derecho fundamental que requiere de su pronta atención mediante la impartición de una justicia expedita.

En cuanto al medio de impugnación contemplado en la LFPDPPP, éste se encuentra señalado en su artículo 56: “Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa”.

Por su parte, el artículo 1o. de la Ley Federal de Procedimiento Contencioso Administrativo (LFPCA) señala: “Los juicios que se promuevan ante el Tribunal Federal de Justicia Fiscal y Administrativa, se regirán por las disposiciones de esta Ley, sin perjuicio de lo dispuesto por los tratados internacionales de que México sea parte. A falta de disposición expresa se aplicará supletoriamente el Código Federal de Procedimientos Civiles, siempre que la disposición de este último ordenamiento no contravenga las que regulan el juicio contencioso administrativo federal que establece esta Ley”.

De lo anterior se infiere que el juicio que regula la LFPCA y se lleva ante el Tribunal Federal de Justicia Fiscal y Administrativa (TFJFA) es el contencioso administrativo federal y no el juicio de nulidad como se señala en la LFPDPPP; y si bien, en la práctica también es conocido con esta última denominación, lo correcto es señalarlo en términos de la LFPCA. De esta manera, el juicio que procede en contra de las resoluciones emitidas en materia de protección de datos personales en posesión de los particulares, y al cual debió referirse la LFPDPPP, es el contencioso administrativo federal.

Por otro lado, se advierte que este juicio se encuentra únicamente contemplado en la LFPDPPP para el procedimiento de protección de derechos y no así para el de verificación e imposición de sanciones; situación que es convalidada en los artículos 138 y 144 del Reglamento de la LFPDPPP, cuando establece la procedencia del "juicio de nulidad" en contra de las resoluciones emitidas en los procedimientos de verificación y de imposición de sanciones. Sin embargo, consideramos que los medios de impugnación para todos los procedimientos debieron haber sido señalados en la ley de la materia y no en su reglamento.

Por lo anterior, se propone señalar de manera clara y precisa en cada uno de los procedimientos contemplados en la LFPDPPP que las resoluciones emitidas en éstos podrán ser impugnadas ante el TFJFA, a través del juicio contencioso administrativo.

De conformidad con lo establecido en el artículo 2o. de la LFPCA: "El juicio contencioso administrativo federal procede contra las resoluciones administrativas definitivas que establece la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa" (LOTFJFA). Luego entonces los supuestos que resultan aplicables a la materia de protección de datos personales, se establecen en el artículo 14, fracciones III, XI y XVI de la LOTFJFA, de la siguiente manera:

> "El Tribunal Federal de Justicia Fiscal y Administrativa conocerá de los juicios que se promuevan contra las resoluciones definitivas, actos administrativos y procedimientos que se indican a continuación:
> I a II …
> III. Las que impongan multas por infracción a las normas administrativas federales;
> IV a X …
> XI. Las dictadas por las autoridades administrativas que pongan fin a un procedimiento administrativo, a una instancia o resuelvan un expediente, en los términos de la Ley Federal de Procedimiento Administrativo;
> XII a XV …
> XVI. Las señaladas en las demás leyes como competencia del Tribunal …"

La demanda del juicio contencioso administrativo federal deberá ser presentada dentro de los 45 días[141] siguientes a aquel en que surtió efectos la notificación de la resolución impugnada. Las partes en el juicio contencioso administrativo federal serán el demandante (el titular o el Responsable); el demandado, quienes podrán ser la autoridad que dictó la resolución impugnada (en este caso sería el IFAI) y el particular a quien favorezca la resolución (el titular o el Responsable); el jefe del Servicio de Administración Tributaria o cuando se controvierte el interés fiscal de la Federación podrá apersonarse la Secretaría de Hacienda y Crédito Público (como puede suceder para los procedimientos de imposición de sanciones) y; el tercero que tenga un derecho incompatible con la pretensión del demandante (puede ser el mismo tercero que participó en el procedimiento de protección de derechos).

Es importante mencionar que los magistrados deberán contemplar por vez primera en la sustanciación y resolución del juicio contencioso administrativo, la presencia del derecho fundamental a la protección de datos personales y de sus principios, materia no antes vista por el TFJFA, por lo cual será de gran interés revisar los primeros asuntos que se ventilen ante dicho tribunal, toda vez que forjarán los precedentes y primeros criterios en la materia.

En términos generales los procedimientos regulados en la LFTAIPG y la LFPDPPP en materia de protección de datos personales son similares además de que ambos son sustanciados por la misma autoridad, el IFAI. Dicha convergencia permitiría estudiar la conveniencia de establecer en un único ordenamiento legal de aplicación general en toda la República Mexicana y bajo los mismos principios y criterios, la regulación del derecho a la protección de datos personales, con las peculiaridades procedentes, según se trate la naturaleza del sujeto Responsable.

Esta propuesta nos llevaría a revisar igualmente, la viabilidad para establecer un órgano constitucional autónomo con facultades suficientes para lograr la adecuada salvaguarda de este derecho fundamental, en las cuales se incluirían desde luego, las necesarias para establecer medidas cautelares o precautorias durante los procedimientos que sustancie y especialmente para asegurar la ejecución de sus resoluciones, todo lo cual se analizará en el siguiente capítulo.

---

[141] De conformidad con el artículo 74, fracción II de la LFPCA los plazos que se fijen en días deben ser entendidos como hábiles, entendiéndose por estos aquellos en que se encuentren abiertas al público las oficinas de las Salas del Tribunal durante el horario normal de labores.

CAPÍTULO CUARTO
ALTERNATIVAS DE MEJORAMIENTO AL MARCO JURÍDICO Y ACCIONES DE GOBIERNO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA JURÍDICO MEXICANO

I. Examen de las disposiciones constitucionales y propuesta de reforma.

Como resultado del análisis realizado en los capítulos anteriores, observamos la existencia de una diversidad de ordenamientos legales, reglamentarios y normativos que regulan, en todos los niveles de gobierno, el derecho a la protección de datos personales en México en poder de entes públicos, además de la existencia de la LFPDPPP y su Reglamento, aplicable a entes privados, y a pesar de existir principios básicos para su aplicación, es ineludible que debido a dicha variedad, exista a su vez, una pluralidad de procedimientos, términos, criterios e instituciones que, en la mayoría de los casos, sólo provoca confusión en los titulares de los datos personales o la complicación del ejercicio y protección de su derecho fundamental, así como un trato desigual a los datos personales en poder de entes públicos y privados.

Por otra parte, como ya se mencionó en el caso de entes públicos, el derecho a la protección de datos personales se regula de manera conjunta con el derecho de acceso a la información, lo cual amplía aún más dicha complejidad, al impedir la distinción de ambos derechos de manera clara.

Ante dicha problemática, y como lo hemos señalado en reiteradas ocasiones a lo largo del presente trabajo, es necesario contar con procedimientos y criterios uniformes, a fin de lograr la adecuada salvaguarda del derecho a la protección de datos personales. Por ello, y en aras del perfeccionamiento y evolución que inevitablemente tendrá este derecho de reciente reconocimiento en México, proponemos la emisión de una Ley General de Protección de Datos Personales, de orden público y de observancia general en la República mexicana, así como la creación de un órgano constitucional, autónomo y especializado, encargado de garantizar este derecho fundamental.[142]

---

[142] Como se mencionó en el Capítulo Segundo del presente trabajo, la Comisionada Sigrid Arzt, se ha pronunciado a favor de esta iniciativa, según comunicado IFAI/081/12, del 18 de junio de 2012, donde propone promover una Ley General de Transparencia y Acceso a la Información, lo cual tendría un inevitable impacto en la protección de datos personales en posesión de entes públicos, al poder ser recurribles las resoluciones de los institutos estatales ante el IFAI. La propuesta de autonomía también fue expuesta en la IX Semana Nacional de Transparencia 2012, llevada a cabo los días 19, 20 y 21 de septiembre de 2012 en la ciudad de México, en la cual el Ministro de la Suprema Corte de Justicia de la Nación, José Ramón Cossío Díaz, señaló la importancia que el IFAI cuente con autonomía constitucional, al tener una función doblemente protectora de

Lo anterior, parte de la premisa que al ser el derecho a la protección de datos personales un derecho fundamental, se vuelve una necesidad básica a satisfacer por todo individuo, por lo que al estar reconocido en la Carta Magna y tratados internacionales suscritos por México, el Estado como garante del derecho debe proveer las bases legales e institucionales idóneas para permitir a los individuos el ejercicio efectivo de su derecho, en respeto a su dignidad humana, así como garantizarlo en caso de verse vulnerado, mediante mecanismos e instituciones adecuadas.

En ese sentido y parafraseando a Emilio Álvarez Icaza Longoria, los derechos fundamentales se convierten en una exigencia primordial de todo ser humano, la cual debe ser satisfecha como una necesidad básica para su desarrollo, pues como el referido autor alude, estos derechos son: "… derechos tan básicos que sin ellos resulta difícil llevar una vida digna. Son universales, prioritarios e innegociables".[143]

Luego entonces, al ser el derecho a la protección de datos personales un derecho fundamental, se presenta como una necesidad básica de todo individuo que debe ser satisfecha, especialmente ante la amenaza o intromisión en su vida privada, prácticas cada vez más frecuentes y agresivas en áreas como en la mercadotecnia, el comercio y con los avances tecnológicos. Así las cosas, los individuos tendrán que adquirir una mayor cultura en el conocimiento de su derecho, para controlarlo y hacerlo valer en los términos y bajo las condiciones que las leyes de la materia estipulen, sin embargo, si éstas son complejas y diversas, pueden convertirse en un verdadero obstáculo de su derecho e impedir con ello la satisfacción de esta necesidad prioritaria de todo ser humano.

Por lo anterior, y a fin de facilitar a los individuos el ejercicio de su derecho, consideramos necesaria la existencia de una ley general aplicable para todos los entes, sean públicos o privados, que recolecten y traten datos personales, además permita una mayor y más accesible protección al derecho de los titulares, incluso cuando sus datos son transmitidos a otros países; pues como hemos visto en los anteriores capítulos, el manejo de datos personales se caracteriza por no tener

---

derechos humanos, es decir del derecho de acceso a la información y el de protección de datos personales, lo cual justifica tenga un estatus similar al del IFE, Banco de México, INEGI y la Comisión Nacional de Derechos Humanos.

143 ESTRADA CORONA, Adrián, "El ejercicio de los derechos humanos en México, fruto de una lucha constante de la sociedad civil. Entrevista con el Mtro. Emilio Álvarez Icaza Longoria", *Revista Digital Universitaria*, 1 de julio 2010, Vol. 11, número 7, ISSN: 1607-6079, formato pdf, disponible en http://www.revista.unam.mx/vol.11/num7/art72/art72.pdf p. 3, consultada el 18 de agosto de 2012.

límites territoriales, debido a la facilidad de transmitirlos de un lugar a otro, incluso fuera de nuestras fronteras, a través del uso de la tecnología, lo cual justifica aún más la importancia de contar con una regulación de aplicación en todo el país, que propicie la homogeneidad y congruencia en la materia, así como contar con una autoridad autónoma y especializada, que promueva y proteja este derecho en México.

Esta propuesta continuará bajo un modelo híbrido, porque a pesar de tener las características del modelo general o de leyes integrales (adoptado por la Unión Europea), éste se seguirá en una forma más flexible, al permitir la participación activa por parte de los Responsables a través del esquema de la autorregulación, en la cual la autoridad solo intervendrá como mero orientador en la materia.

Ahora bien, dentro de esta evolución del derecho a la protección de datos personales, es importante resaltar la tendencia actual hacia la elaboración de documentos internacionales vinculantes, [144] que contribuyan a una mayor y homogénea protección de este derecho; lo anterior, ante el inevitable y constante flujo de datos personales que se da en todo el mundo. En ese contexto, el contar con principios, procedimientos, términos y autoridades comunes que garanticen la efectiva y uniforme protección de datos personales en el territorio nacional, facilitará el cumplimiento de dichos documentos, en caso de que México se adhiera a los mismos, y en la medida que favorezcan y amplíen la protección de los derechos de los titulares de datos personales. Por otro lado, bajo esas circunstancias y de acuerdo con el principio de reciprocidad del derecho internacional, se podrá exigir como mínimo a otros países, contar con las mismas o similares condiciones y medidas de seguridad que México tiene, previo a la realización de cualquier transferencia internacional de datos personales.

Después de señalar algunos de los beneficios que traería esta propuesta, ahora revisemos la viabilidad de llevarla a cabo, a través de la modificación de aquellos preceptos legales que darán sustento a la misma, siendo en primer término,

---

144 Como ejemplo podemos citar los “Estándares Internacionales sobre Protección de Datos Personales y Privacidad”, adoptados en la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009, en Madrid, España, en la que participan cerca de 50 países, bajo la coordinación de la Agencia Española de Protección de Datos. Este documento según su nota de presentación, pretende: “… promover internacionalmente el derecho a la protección de datos y la privacidad, ofreciendo un modelo de regulación que garantiza un alto nivel de protección y que, al mismo tiempo, puede ser asumido en cualquier país, con las mínimas adaptaciones que puedan ser necesarias según las culturas jurídicas, sociales o económicas propias de cada región”. Disponible en http://www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/common/Estandares_Nota_Presentacion.pdf, consultada el 1 de septiembre de 2012.

los relativos a la Constitución Política de los Estados Unidos Mexicanos. En el Capítulo Segundo de este trabajo fueron ya examinados los artículos 6o., 16 segundo párrafo y 73 fracción XXIX-O de la Carta Magna, por ser estos los preceptos constitucionales que regulan expresamente el derecho a la protección de datos personales. Sin embargo, ahora abordaremos la posibilidad de establecer las propuestas de reforma a dichos artículos, en el orden que fueron mencionados, como a continuación se señala:

Previo a presentar la propuesta de reforma al artículo 6o. constitucional, es importante mencionar que esa disposición es un claro ejemplo de cómo a pesar de haberse estipulado las bases mínimas a considerar en las diversas leyes en materia de acceso a la información, ello no ha sido suficiente para alcanzar la homogeneidad pretendida, y no obstante de haber logrado grandes avances en la materia, aún no es posible afirmar que se ha alcanzado el tan anhelado objetivo de una completa y verdadera transparencia de la información pública gubernamental y la rendición de cuentas por parte de cualquier ente que recibe recursos del erario público, independientemente del nivel de gobierno al que pertenezca, sea autónomo o no, dado que cada uno emite, aplica e interpreta a su modo sus propias leyes o disposiciones normativas de la manera como le sea más conveniente y sin que en algunos casos, los ciudadanos puedan acceder, sin justificación alguna, a la información que requieren.

Ante dicho escenario es que actualmente existen diversas propuestas para emitir una Ley General de Transparencia y Acceso a la Información Pública Gubernamental,[145] a la que se sujetarían todos los entes públicos, sean federales, estatales o municipales en el derecho de acceso a la información pública, así como se otorgaría autonomía constitucional al IFAI, propuestas que de llevarse a cabo, serían acordes con la planteada en el presente trabajo, y lo cual permitiría concretar la regulación del derecho de acceso a la información y la de protección de datos personales, de manera independiente a través de sus leyes generales respectivas.

---

[145] Al 16 de octubre de 2012 se han presentado en la Cámara de Diputados y Senadores, ocho propuestas de reforma a la Constitución y la Ley Federal de Transparencia y Acceso a la Información, por parte de los partidos del PAN, PRD, PRI, PT y Nueva Alianza. El 19 de diciembre de 2012, las Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos Primera; de Gobernación y de Anticorrupción y Participación Ciudadana en Materia de Transparencia de la Cámara de Senadores, emitieron un dictamen para analizar tres iniciativas de reformas constitucionales en materia de transparencia, presentadas el 6 y 13 de septiembre de 2012 y el 4 de octubre de 2012, por senadores de los Grupos Parlamentarios del PRD, PRI-PVEM y PAN, respectivamente, en las cuales se propone principalmente la autonomía constitucional del IFAI y la emisión de dos leyes generales en materia de acceso a la información y de protección de datos personales.

Ahora bien, como ya fue señalado en anteriores capítulos, las fracciones II y III del artículo 6o. constitucional establecen el derecho a la protección de datos personales, como uno de los principios del derecho de acceso a la información, lo cual se mantendría con ese mismo carácter de mandatos. Para efectos de la propuesta planteada en el presente trabajo, y debido al innegable vínculo que tienen ambos derechos, la fracción II del referido artículo constitucional, se conservaría en los mismos términos como actualmente se encuentra, es decir:

> "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".

Como se observa, esta fracción refiere a dos derechos, el de la vida privada y el de los datos personales, por lo cual la palabra "leyes" no se modifica a singular para referirla a una ley en particular, pues como se analizó en el Capítulo Segundo de este trabajo, existen otras disposiciones que regulan lo relativo a estos derechos, ya sea a través de disposiciones para su protección o su excepción en una materia particular, motivo por el cual decidimos conservar de esta forma la redacción, a fin de no limitar la protección de estos derechos a una sola disposición legal.

Así a través de dicha fracción, se mantiene el mandato general para los entes públicos de sujetarse, en lo relativo a la vida privada y datos personales, a lo señalado por otras leyes, entre las que se encontraría desde luego, la propuesta Ley General de Protección de Datos Personales, pero también aquéllas que dada su materia particular (telecomunicaciones, protección al consumidor, derechos de autor, derechos del contribuyente, usuarios de servicios financieros, seguridad nacional, salud, entre otras) regulan en el ámbito de su competencia, la protección de datos personales y, en su caso, establecen sus excepciones.

Por lo que se refiere a la fracción III del artículo 6o. constitucional, consideramos debe ser modificada la parte relativa a los derechos de acceso y rectificación de los datos personales por dos motivos, en primer lugar porque limita su ejercicio sólo a esos dos derechos, sin considerar los de cancelación y oposición también reconocidos por el artículo 16 constitucional y, en segundo lugar, para establecer que el ejercicio de los derechos ARCO será regulado por la ley de la materia. Así la fracción III del artículo 6o. constitucional quedaría de la siguiente manera:

> "Artículo 6o. …
> 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 a la II. …

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~~. **En cuanto al acceso, rectificación, cancelación y oposición de los datos personales de los individuos, se estará a lo dispuesto por el artículo 16, segundo párrafo de esta Constitución y la ley de la materia**.

IV a la VII. …"

[Texto en negrita es añadido]

En cuanto al segundo párrafo del artículo 16 de la Carta Magna, el cual es el origen y fundamento del derecho a la protección de datos personales, será indudablemente la base constitucional de la ley general propuesta. Como se ha comentado en otras ocasiones, este artículo contiene expresamente los derechos que podrán ser ejercidos por cualquier persona en la protección de sus datos (derechos ARCO), sin hacer distinción alguna entre la protección de datos personales en posesión de entes públicos y la de entes privados, por lo cual es posible hablar de una la "ley" como en dicha disposición se señala en singular, que establezca los términos en que podrá ejercerse este derecho, así como sus excepciones; por lo cual sólo se hará énfasis que se trata de la ley de la materia.

Por otro lado, este precepto será también el sustento para la creación del propuesto órgano constitucional autónomo y especializado en materia de protección de datos, encargado de garantizar este derecho fundamental, a fin de dotarlo de personalidad jurídica y patrimonio propio, así como de autonomía en el ejercicio de sus funciones y en su administración.

De esta manera, el texto del segundo párrafo del artículo 16 constitucional sería el siguiente:

"Artículo 16. …

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley **de la materia**, 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. **La protección de los datos personales será garantizada a través de un**

órgano público autónomo en el ejercicio de sus funciones y en su administración, dotado de personalidad jurídica y patrimonio propios".

[Texto en negrita es añadido]

Ahora bien, por lo que se refiere al artículo 73 fracción XXIX-O constitucional, será necesario modificarlo a fin de conferir facultades al Congreso de la Unión para legislar en materia de protección de datos personales, en todos los niveles de gobierno y ámbitos, público y privado. De esta forma, con la mención expresa de la facultad conferida al Congreso, la protección de datos personales sería una materia exclusiva de la Federación, no reservada a los Estados, tal y como lo dispone el artículo 124 constitucional, el cual señala: "Las facultades que no están expresamente concedidas por esta Constitución a los funcionarios federales, se entienden reservadas a los Estados".

Previo a presentar la propuesta de modificación a la citada disposición, es necesario recordar los dos motivos principales que tuvieron los legisladores para separar la protección de datos personales en posesión de particulares de la de entes públicos; el primero fue debido a que el derecho a la protección de datos en posesión de estos últimos entes, ya se encontraba regulado en la LFTAIPG a nivel federal y por cada una de las entidades federativas y el Distrito Federal a nivel local, y el segundo motivo fue porque el tratamiento de datos personales en poder de entes privados está estrechamente relacionado con el comercio, materia de exclusiva regulación por parte del Congreso de la Unión, de conformidad con lo dispuesto en el artículo 73 fracción X de la Constitución Política de los Estados Unidos Mexicanos.

En relación con el primer motivo, hemos señalado en repetidas ocasiones que a pesar del indiscutible vínculo existente entre el derecho de acceso a la información y el de protección de datos personales, por ser este último una limitante o excepción del primero (sólo para el caso de entes públicos), estos derechos evidentemente no son iguales, en razón de que cada uno cuenta con sus propios objetivos, procedimientos y principios.

Para entender el por qué estos derechos fueron regulados en la misma ley, debemos recordar lo señalado en el Capítulo Segundo del presente trabajo, donde analizamos la exposición de motivos de la iniciativa de la LFTAIPG, presentada por el Ejecutivo Federal el 30 de noviembre de 2001. En ésta se expuso la trascendencia cada vez mayor que tenía, en la sociedad actual, la protección de datos personales, lo cual ameritaba su inclusión necesaria en la LFTAIPG, por lo menos a través de principios mínimos y de manera provisional, en tanto se emitiera la ley de la materia.

Bajo ese contexto y circunstancias fue justificable la inserción del derecho a la protección de datos personales en la LFTAIPG, al no existir ninguna otra disposición que lo regulara hasta ese momento y de manera expresa, lo cual representó un gran avance en la materia, aun y cuando se regulaba como parte de otro derecho (el de acceso a la información); sin embargo, actualmente no es posible mantenerlo dentro de la LFTAIPG, cuando ya existe su reconocimiento constitucional y la emisión de la LFPDPPP, condiciones por demás suficientes para integrar el derecho a la protección de datos personales en una legislación exclusiva de esta materia.

Aunado a lo anterior, debemos recordar que el Artículo Segundo Transitorio del Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, publicado en el DOF el 20 de julio de 2007, señala que: “La Federación, los Estados y el Distrito Federal, en sus respectivos ámbitos de competencia, deberán expedir las leyes en materia de acceso a la información pública y transparencia, o en su caso, realizar las modificaciones necesarias, a más tardar un año después de la entrada en vigor de este Decreto”; de lo cual no se infiere de modo alguno, la emisión de leyes relativas al derecho a la protección de datos personales, motivo por el cual no consideramos se afecte la competencia de los Estados con la emisión de una ley en esta materia, toda vez que se mantendría su facultad para legislar en cuanto al derecho de acceso a la información y transparencia.

En cuanto al segundo motivo para regular de manera independiente la protección de datos personales por los fines diversos que persiguen los entes públicos y privados; al respecto señalamos como cierto que estos últimos tienen generalmente fines preponderantemente comerciales para tratar los datos personales de los individuos, sin embargo ello no siempre es así, como sucede con algunas asociaciones civiles. Por otra parte, los entes públicos también pueden llegar a comercializar los datos personales (contando con el consentimiento expreso de su titular, tal y como se prevé en los artículos 18 fracción II y 21 de la LFTAIPG), aun y cuando no sea su fin principal.

De esta manera, el argumento de dividir la protección de datos personales por la naturaleza de los entes que poseen dichos datos, basado en los fines que persiguen, no tiene sustento, toda vez que no se puede señalar como exclusivo de los particulares los fines comerciales, ni tampoco suponer que los entes públicos no los pueden llegar a realizar. Además no puede negarse que tanto las bases de datos públicas como privadas relativas a datos personales, pueden presentar los mismos riesgos, en caso de no estar debidamente protegidas, bajo mecanismos y medidas

de seguridad adecuadas, así como la confidencialidad que deben guardar todos aquellos quienes las tienen bajo su resguardo.

Al respecto, podemos citar como ejemplo, la venta indebida del padrón electoral, lo cual evidentemente se debió a la falta de medidas de seguridad idóneas para su resguardo y el quebrantamiento, por parte del Responsable y sus Encargados, a diversos principios rectores de la protección de datos personales como son: licitud, finalidad, lealtad y responsabilidad en el cuidado de los datos, hecho que independientemente de la infracción o delito que pudiera haberse dado en otra materia, debió ser investigado en lo referente a la protección de datos personales. En esta situación y bajo una misma ley, se exigiría la aplicación con el mismo rigor de sanciones o la persecución de delitos en la materia, según sea el caso, tanto para entes públicos como privados, pues en todo momento debe prevalecer la salvaguarda del derecho fundamental.

La Constitución Política de los Estados Unidos Mexicanos reconoce en el párrafo segundo de su artículo 16, un derecho fundamental y una ley, por lo cual el derecho a la protección de datos personales debe ser regulado de manera uniforme, sin dejar por ello de reconocer que habrán diferencias necesarias al aplicar la ley de la materia para entes públicos o privados, debido a su propia naturaleza, especialmente al momento de ser sancionados. Es importante señalar que la ley de la materia será reglamentaria del párrafo segundo del artículo 16 constitucional, y en consecuencia deberá encontrarse acorde con las bases mínimas señaladas en dicho precepto.

Asimismo como derecho fundamental regulado también a nivel internacional, la ley que se emita en esta materia deberá estar de acuerdo con lo dispuesto en los tratados internacionales suscritos y aprobados por México, a fin de ser congruente con lo establecido en el segundo párrafo del artículo 1o. constitucional y el principio *pro homine*,[146] con lo cual se brindará a favor de los titulares de los datos, una protección más amplia de su derecho.

Por lo anterior, se propone que el texto del artículo 73 fracción XXIX-O quede de la siguiente manera:

> “Artículo 73. El Congreso tiene facultad:
> I a XXIX-Ñ. …
> XXIX-O. Para **expedir una ley general** ~~legislar~~ en materia de protección de datos personales **con objeto de cumplir lo**

[146] Véase la explicación de este principio, en el punto II. Tratados internacionales en materia de protección de datos personales, aprobados por el Senado de la República del Capítulo Segundo del presente trabajo, páginas 73 y 74.

> **previsto en el artículo 16, segundo párrafo de esta Constitución, y en los tratados internacionales de la materia, de los que México sea parte**.
> XXIX-P. …
> XXIX-Q. …
> XXX. …”
> [Texto en formato de negrita añadido]

Con la reforma de la fracción XXIX-O del artículo 73 constitucional, en uno de los artículos transitorios del decreto por el cual se emita, se establecería el plazo que tendría el Congreso de la Unión para expedir la ley general, así como el término de vigencia de las leyes estatales sobre la materia. Esto podría llevarse a cabo, en la misma forma como se indicó en el Decreto por el que se adicionó la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el DOF el 30 de abril de 2009, en cuyo Artículo Tercero Transitorio se estableció lo relativo a la vigencia de las leyes estatales, y que retomando su texto, para los efectos pretendidos, sólo se adaptaría en su parte final, para quedar de la siguiente manera:

> “**Tercero.-** En tanto el Congreso de la Unión expide la ley **general** respectiva a la facultad que se otorga en este Decreto, continuarán vigentes las disposiciones que sobre la materia hayan dictado las legislaturas de las entidades federativas, en tratándose de datos personales en posesión de **entes públicos**”.
> [Texto en negrita es añadido]

Con la realización de las reformas propuestas a los artículos 6o., 16, segundo párrafo y 73 fracción XXIX-O de la Constitución Política de los Estados Unidos Mexicanos, contaremos entonces con la base constitucional para llevar a cabo la propuesta de la Ley General de Protección de Datos Personales y la creación del órgano autónomo especializado en esta materia, como se analizará a continuación en los siguientes apartados del presente capítulo.

II. Estudio sobre la conveniencia de reformar las leyes y reglamentos en materia de protección de datos personales en el sistema jurídico mexicano.

Como se expuso en el punto anterior, a fin de lograr la coherencia y uniformidad en la protección de datos personales, en favor de procedimientos más claros, sencillos y accesibles, lo cual redundará en una mayor certeza y seguridad para los titulares de dichos datos, proponemos la emisión de una Ley General de Protección de Datos Personales. Con la aplicación de una sola ley relativa a la materia, también se logrará una mayor congruencia con los tratados internacionales

suscritos y aprobados por México sobre protección de datos personales, así como una mayor compatibilidad con las medidas de protección emitidas por otros países, tema de especial interés para las transferencias internacionales.

Como consecuencia de la emisión de la Ley General de Protección de Datos Personales, se dará la abrogación de todas las disposiciones locales existentes sobre protección de datos personales en posesión de entes públicos,[147] así como la derogación de las disposiciones que sobre esta materia se encuentren en sus leyes de transparencia. La abrogación se daría en los mismos términos que se expusieron en el Artículo Quinto Transitorio del Decreto por el cual se expidió la LFPDPPP,[148] publicado en el DOF el 5 de julio de 2010, para que, en el caso en concreto, su texto quede de la siguiente manera:

> "~~**QUINTO.-**~~ [numeral que corresponda] En cumplimiento a lo dispuesto por el artículo tercero transitorio del Decreto por el que se ~~adiciona~~ **reforma** la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el ~~30 de abril de 2009~~ [fecha en que se publique la ley], las disposiciones locales en materia de protección de datos personales en posesión de los ~~particulares~~ **entes públicos** se abrogan, y se derogan las demás disposiciones que se opongan a la presente Ley.
>
> [Texto en negrita es añadido]

La abrogación de las leyes y derogación de las disposiciones locales emitidas en materia de protección de datos personales en posesión de entes públicos no implicará, como más adelante explicamos, la eliminación de aquellas disposiciones que regulen la forma cómo se podrán ejercer los derechos ARCO, pues al igual que sucede con los entes privados, esto le corresponde establecer a los Responsables, sujetándose por supuesto a las bases mínimas establecidas en la ley de la materia.

En ese contexto, y como resultado del perfeccionamiento que también tendrá el derecho a la protección de datos personales, basado en la realidad de la

---

147 Como se analizó en el Capítulo Segundo, los Estados que actualmente cuentan con una ley de protección de datos personales son: Campeche, Colima, Guanajuato, Oaxaca, Tlaxcala y el Distrito Federal.

148 La denominación completa del decreto referido es Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

sociedad mexicana y en la propia experiencia vivida por el derecho al acceso a la información, con el cual ha sido identificado estrechamente en cuanto a los datos tratados por entes públicos, es que se propone la emisión de una ley general de protección de datos personales con la posterior emisión de su respectivo reglamento.

Para esta propuesta resulta de interés conocer lo que se entiende por ley general, al respecto el Pleno de la Suprema Corte de Justicia de la Nación, en la tesis jurisprudencial con número de registro 165224, señala lo siguiente:

> "**LEYES LOCALES EN MATERIAS CONCURRENTES. EN ELLAS SE PUEDEN AUMENTAR LAS PROHIBICIONES O LOS DEBERES IMPUESTOS POR LAS LEYES GENERALES.** Las leyes generales son normas expedidas por el Congreso de la Unión que distribuyen competencias entre los distintos niveles de gobierno en las materias concurrentes y sientan las bases para su regulación, de ahí que no pretenden agotar la regulación de la materia respectiva, sino que buscan ser la plataforma mínima desde la que las entidades puedan darse sus propias normas tomando en cuenta su realidad social. Por tanto, cumpliendo el mínimo normativo que marca la ley general, las leyes locales pueden tener su propio ámbito de regulación, poniendo mayor énfasis en determinados aspectos que sean preocupantes en una región específica. Si no fuera así, las leyes locales en las materias concurrentes no tendrían razón de ser, pues se limitarían a repetir lo establecido por el legislador federal, lo que resulta carente de sentido, pues se vaciaría el concepto mismo de concurrencia. En este sentido, las entidades federativas pueden aumentar las obligaciones o las prohibiciones que contiene una ley general, pero no reducirlas, pues ello haría nugatoria a ésta".[149]

De esta forma una ley general implica la posibilidad de que las entidades federativas puedan actuar respecto de la protección de datos personales, pero en la forma y términos como lo determine el Congreso de la Unión en la ley, en la cual se sentarían las bases mínimas para su regulación. En este sentido, además de

[149] Tesis Jurisprudencial P./J.5/2010, Novena Época, emitida por el Pleno de la Suprema Corte de Justicia de la Nación y publicada en el Semanario Judicial de la Federación y su Gaceta XXXI, febrero de 2010, página 2322, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 165224. El 15 de febrero de 2010, con la Acción de inconstitucionalidad 119/2008, el Tribunal del Pleno aprobó, con el número 5/2010, la tesis jurisprudencial.

respetar la soberanía de los Estados, también se fomentaría el principio de la autorregulación que rige en el modelo de protección de datos personales acogido en México, y por el cual se permite a los Responsables emitir su propia regulación por sectores, para ampliar la protección y facilitar el ejercicio efectivo de los derechos ARCO por parte de sus titulares, a través de esquemas de autorregulación como son los códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos. Así las entidades federativas podrán emitir su propia regulación para la atención de las solicitudes presentadas por los titulares, por las cuales ejercen sus derechos ARCO, en las que establezcan plazos, procedimientos internos para dar trámite a las mismas, mecanismos de seguridad, entre otros elementos relevantes para salvaguardar este derecho, sujetándose a las bases mínimas establecidas en la ley general.

Es de destacar que en la protección de datos personales es de suma importancia la coordinación que existirá entre el órgano garante de este derecho y las autoridades federales y locales, quienes en el ámbito de sus atribuciones, coadyuvarán en la vigilancia y aplicación de la ley de la materia, así como en la difusión de este derecho. De igual forma, dentro del ámbito de su competencia y de acuerdo al sector o actividad que regulen, las autoridades podrán emitir o modificar la disposición que tenga un impacto en la protección de datos personales, a fin de atender las necesidades que surjan de ese sector o actividad.

Para enriquecer el proyecto propuesto, se considerarán todos aquellos valiosos trabajos realizados previamente en esta materia, los cuales fueron expuestos ampliamente en los capítulos anteriores. Uno de esos precedentes retomados en el proyecto es precisamente la idea de regular en un mismo ordenamiento la protección de datos personales en posesión tanto de entes públicos como privados, supuesto contemplado ya desde la primera iniciativa de la LFPDPPP del 6 de septiembre de 2001 y en la segunda del 1 de diciembre de 2005,[150] en las cuales se señalaba la aplicación de la ley a bases de datos públicas y privadas. En ese mismo sentido se encuentran algunos documentos internacionales los cuales consideran como Responsable, a la persona física o jurídica, de naturaleza pública o privada.

Por lo anterior, para estructurar el proyecto de la ley general de protección de datos personales, partiremos de aquella legislación de reciente emisión, considerada como la más avanzada y completa en la protección de datos personales, es decir la LFPDPPP, de la cual se tomará su estructura y contenido como la base para la elaboración de la ley general propuesta, a fin de incluir

[150] Véase análisis de la primera y segunda iniciativa a la LFPDPPP en el Capítulo Segundo del presente trabajo, pp. 91 y 92.

únicamente en la misma, las adecuaciones y propuestas pertinentes, como a continuación se detalla:

CAPÍTULO I
Disposiciones Generales

- El objeto de la ley sería el siguiente: Artículo 1.- La presente Ley reglamenta el derecho a la protección de datos personales, en términos del segundo párrafo del artículo 16 constitucional y los Tratados Internacionales celebrados y ratificados por el Estado Mexicano en la materia; la ley es de orden público y de observancia general en todo el territorio nacional, y tiene como objeto garantizar y regular el tratamiento legítimo, controlado e informado de los datos personales, a fin de salvaguardar el derecho a la autodeterminación informativa de las personas.
- Los sujetos regulados por la ley serán las personas físicas o morales de carácter público o privado que lleven a cabo el tratamiento de datos personales. Dentro de las personas de carácter público se encontrarán los poderes Ejecutivo, Legislativo y Judicial de la Federación, los estados y el Distrito Federal; los ayuntamientos de los municipios; los órganos político-administrativos de las demarcaciones territoriales del Distrito Federal; las entidades de la administración pública paraestatal, ya sean federales, central y paraestatal, estatales o municipales y los órganos autónomos federales y estatales.
- En cuanto al glosario, se incluirá el término de “ente público”, entendido como la persona de carácter público que obtenga, use, divulgue o almacene datos personales. En el caso de “Encargados” de entes públicos, se establecerá que serán aquellos servidores públicos facultados por disposición o autorización expresa del Responsable, para obtener, usar, divulgar o almacenar datos personales. También se adicionará el de “Instituto” para referir al que denominaremos Instituto Nacional de Protección de Datos Personales. Y finalmente se precisará que el Responsable es la persona física o moral de carácter público o privado que decide sobre el tratamiento de los datos personales.
- Por lo que se refiere a las excepciones a los principios y derechos previstos en la ley, en cuanto a su observancia y ejercicio, se establecerán los relativos al orden público, seguridad nacional y pública, salud pública y derechos de terceros, en los casos y con los alcances previstos en esta ley y otras aplicables en la materia.
- Se propone eliminar de las excepciones a las sociedades de información crediticia, e incluir únicamente la precisión que para el ejercicio de los derechos ARCO ante dichas sociedades, se seguirá el

procedimiento establecido en la Ley para Regular las Sociedades de Información Crediticia, y en caso de negarse alguno de los derechos o estar inconforme con la respuesta, se podrá presenta la solicitud de protección de derechos, en los términos que establezca la ley general.

CAPÍTULO II
De los Principios de Protección de Datos Personales

- Dentro de las excepciones al consentimiento para el tratamiento de datos personales se agregaría el supuesto de la transmisión de datos personales entre entes públicos, siempre y cuando los mismos se utilicen para el ejercicio de sus facultades.
- Será obligación del Responsable el cerciorarse que el titular conozca el aviso de privacidad previo al tratamiento de sus datos personales, por lo que, en caso de controversia, le corresponderá al primero acreditar que el titular efectivamente tuvo conocimiento del mismo.

CAPÍTULO III
De los Derechos de los Titulares de Datos Personales

- Por lo que se refiere al derecho de cancelación, se añadiría el supuesto para cancelar datos personales de manera inmediata, en aquellos casos donde no surja ningún tipo de relación jurídica, como puede ser en la presentación de solicitudes de empleo, créditos, incorporación a escuelas, clubes o asociaciones, cotizaciones, entre otras. En estos casos la cancelación y la inmediata eliminación de los datos, sin un periodo de bloqueo previo, la hará el Responsable sin necesidad de mediar solicitud alguna, sin embargo el titular en cualquier momento podrá solicitar su cancelación o que le acrediten su realización.
- En caso de cancelaciones, el titular podrá solicitar al Instituto su intervención a fin de verificar la eliminación definitiva de sus datos, a través de personal especializado en la materia. De observar que el Responsable no eliminó los datos personales, no obstante de haber transcurrido el plazo para ello, el Instituto podrá iniciar el procedimiento de infracciones, a fin de determinar la probable sanción. Lo anterior, a fin de proteger el derecho al olvido de los titulares.
- En cuanto a la posibilidad de que los sucesores puedan solicitar el acceso, rectificación o cancelación de los datos de un titular fallecido, se podrán solicitar al Responsable, siempre y cuando ello sea necesario para que ejerzan algún derecho relacionado con la sucesión o previsto en alguna otra ley. Por lo cual ésta será la única excepción a que la solicitud sea presentada por el titular o su representante.

CAPÍTULO IV
Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición

- Los medios para ejercer los derechos ARCO deberán estar expresamente señalados en el aviso de privacidad, debiendo ser de fácil acceso para toda persona.
- El plazo de los veinte días hábiles para dar respuesta a la solicitud de ejercicio de derechos ARCO, se contará a partir del día siguiente a su recepción.
- En cuanto a la negativa para ejercer algún derecho ARCO, se precisará que para el caso de entes públicos, ésta deberá estar debidamente fundada y motivada. Y se agregarán como supuestos los relativos a información reservada o confidencial, así como si se trata de trámites o servicios, en cuyo caso se deberá agotar previamente, el procedimiento específico señalado en sus manuales y con los formatos requeridos.

CAPÍTULO V
De la Transferencia de Datos

- Se eliminará de los supuestos que no requieren del consentimiento del titular, los casos de transferencias de datos personales entre sociedades del mismo grupo comercial, y se hará el señalamiento que previo a cualquier tratamiento de datos personales, el Responsable deberá advertir directamente al titular de la posible transferencia de sus datos, a fin de contar con su consentimiento expreso o manifestar en su caso su oposición. Sin dicho requisito el Responsable no podrá hacer transferencia alguna, aun y cuando se trate de sujetos integrantes de su misma cadena comercial.

CAPÍTULO VI
De las Autoridades

Sección I
Del Instituto

- En este capítulo se establecerán las atribuciones del órgano garante del derecho a la protección de datos personales, así como la coordinación que tendrá con otras autoridades tanto federales como locales en la materia, con el objeto de difundir, promover y vigilar el cumplimiento de la ley general.
- Se adicionará como atribución del Instituto, imponer medidas de apremio a fin de hacer cumplir sus requerimientos.

- En cuanto a su estructura se establecerá que para el adecuado cumplimiento de sus atribuciones y objeto de la ley general, el Instituto contará con delegaciones estatales en el territorio nacional, las cuales se establecerán como órganos desconcentrados de dicho Instituto y estarán encargados de recibir las solicitudes de protección de derechos y auxiliar en la difusión y promoción de este derecho.

Sección II
De las Autoridades Reguladoras

- En cuanto a las autoridades reguladoras continuará la participación a nivel federal de la Secretaría de Economía, la cual se encargará de coordinarse con el IFAI y las dependencias locales, especialmente por lo que se refiere a los esquemas de autorregulación vinculantes por sectores o actividades.

CAPÍTULO VII
Del Procedimiento de Protección de Derechos

- Por la inconformidad con la respuesta recibida o la falta de ella por parte del Responsable, el titular podrá presentar una solicitud de protección de derechos, ante el Instituto.
- La solicitud será presentada dentro de los 15 días siguientes a la fecha en que se comunique la respuesta al titular por parte del Responsable o en caso de falta de respuesta, será a partir en que venza el plazo de los 20 días con los que contaba el Responsable para emitir la misma.
- Para el desempeño de las funciones que la ley le atribuye al Instituto, éste podrá aplicar medidas de apremio como son el apercibimiento, multas y solicitar el auxilio de la fuerza pública.
- En caso de falta de respuesta, si después de haber hecho el Instituto el requerimiento al Responsable para que acredite la misma o la emita, y éste no lo atiende, el Instituto aplicará por una sola vez las medidas de apremio correspondientes y ante la insistente negativa, reconducirá el procedimiento al de verificación y, en su caso, al de imposición de sanciones, pues se considerará la falta de respuesta como una infracción a la ley. Si no existen elementos que justifiquen la reconducción, el Instituto podrá resolver el sobreseimiento por falta de materia.
- Si la solicitud de ejercicio de derechos ARCO no fuere recibida por el Responsable o se negare a emitir acuse de recibo, el titular podrá presentar un escrito ante el Instituto en el que exprese tal situación y acredite haber presentado la solicitud en el lugar o a través de los medios señalados en el aviso de privacidad, a fin de investigar el motivo

de su negativa, y en su caso, iniciar con el procedimiento de verificación correspondiente.

- Cuando se presenten diversas solicitudes por el mismo titular en contra de supuestos Responsables que posteriormente acrediten ser Encargados de los datos personales, se podrán acumular las solicitudes, siempre y cuando los Encargados señalen quien es el Responsable y éste se identifique como tal. Lo anterior por economía procesal y a fin de emitir una única resolución.
- El Instituto podrá solicitar la suspensión del tratamiento de los datos en los casos donde se observe una notoria violación a la ley, a fin de salvaguardar el derecho del titular.
- El Instituto podrá allegarse de cualquier elemento de convicción que estime necesario, por lo cual podrán valerse de cualquier persona, sea parte o tercero, y de cualquier documento u objeto, siempre que tengan relación inmediata con los hechos controvertidos, a fin de conocer la verdad de los hechos.
- Contra las resoluciones del Instituto, se interpondrá el juicio contencioso administrativo ante el Tribunal Federal de Justicia Fiscal y Administrativa.[151]

CAPÍTULO VIII
Del Procedimiento de Verificación

- Para efecto de llevar a cabo las verificaciones en todo el territorio nacional, el Instituto contará con personal técnico y especializado para realizar las mismas en las delegaciones estatales.
- Si durante la visita de verificación se observare alguna violación a la ley, se podrán imponer las medidas precautorias necesarias a fin de salvaguardar los datos personales. Dentro de las medidas precautorias se encontrará la suspensión temporal del tratamiento de datos personales o el no uso de la base de datos hasta en tanto pueda ser revisada.
- Cuando derivado de una verificación, se observen violaciones a la ley, se podrá comunicar a los titulares sobre dicha situación, a fin de que en su caso, ejerzan los derechos o acciones procedentes, independientemente de las aplicables por la ley de la materia.

[151] La competencia del Tribunal referido se daría de conformidad con lo dispuesto en el artículo 14, fracciones XI y XVI de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa. Las Salas Regionales del Tribunal Federal de Justicia Fiscal y Administrativa conocen de los juicios por razón del territorio respecto del lugar donde se encuentra la sede de la autoridad demandada; si son varias las autoridades demandadas, donde se encuentre la que dictó la resolución impugnada. Cuando el demandado sea un particular, se atenderá a su domicilio.

- Será motivo de inicio del procedimiento de verificación, la falta de respuesta del Responsable ante una solicitud de ejercicio de derecho ARCO.
- Contra las resoluciones del Instituto, se interpondrá el juicio contencioso administrativo ante el Tribunal Federal de Justicia Fiscal y Administrativa.

CAPÍTULO IX
Del Procedimiento de Infracciones

- En cuanto a este capítulo se modificará su denominación de "Procedimiento de Imposición de Sanciones", a fin de no sólo delimitarlo a las sanciones sino a cualquier tipo de infracción, por lo cual se propone "Del Procedimiento de Infracciones".
- Para la sustanciación de este procedimiento se hará una división entre los entes públicos y los entes privados.
- Para los entes públicos se aplicará lo dispuesto en las leyes de responsabilidades administrativas, en cuyo caso el Instituto turnará el asunto a las autoridades federales o locales competentes, según sea el caso, para la aplicación de las sanciones administrativas que correspondan al servidor público infractor. No obstante ello, si derivado del procedimiento se observare alguna conducta que pudiera constituir un probable delito, se hará del conocimiento del Ministerio Público Federal.
- Si derivado de la investigación se observare que el ente público violó las disposiciones de la ley, como lo es el no mantener las medidas de seguridad adecuadas y causar por ello, un daño grave al titular o a diversos titulares, el Instituto podrá también imponer multa a dicho ente, independientemente de las responsabilidades en las que incurran los servidores públicos involucrados.
- En cuanto a los entes privados, la determinación de infracciones se hará en los términos que establezca la ley general, como actualmente lo prevé la LFPDPPP.
- Con el escrito que presente el presunto infractor para atender la vista del Instituto, deberá anexar un comprobante de sus ingresos anuales, para efecto de determinar la capacidad económica del presunto infractor.

CAPÍTULO X
De las Infracciones y Sanciones

- Se adicionará como infracción la insistente negativa a emitir una respuesta a la solicitud de ejercicio de derechos ARCO, sin causa

justificada, misma que se ubicaría en el segundo grupo de multas (mayor gravedad).

- Se incluirá como infracción el tratamiento de datos personales, no obstante de haberse decretado su suspensión como medida preventiva, la cual se contendrá en el grupo dos de multas.
- Cualquier incumplimiento por parte del Responsable a las obligaciones establecidas en la ley, serán sancionadas conforme al grupo uno de multas (menor gravedad).
- Se establecerán importes de multas específicas para cada infracción de acuerdo a su gravedad e impacto en los derechos de los titulares.
- Los Encargados también podrán ser sancionados cuando actúen con el carácter de Responsables sin su autorización.
- Para el cobro de multas impuestas por el Instituto se llevará a cabo la coordinación con las entidades federativas.
- Contra las resoluciones del Instituto, se interpondrá el juicio contencioso administrativo ante el Tribunal Federal de Justicia Fiscal y Administrativa [152]

CAPÍTULO XI
De los Delitos en Materia del Tratamiento Indebido de Datos Personales

- Los delitos en esta materia serán de orden federal.
- El Instituto coadyuvará con el Ministerio Público Federal en la aportación de cualquier elemento necesario para la integración de la averiguación previa.

La propuesta que se hace en el presente trabajo se realizará en una forma integral, por lo cual junto con la ley general se propone el establecimiento de un órgano de control, garante del derecho a la protección de datos personales, el cual se expone en el siguiente apartado.

III. Análisis sobre la viabilidad de crear un órgano autónomo especializado.

De conformidad con lo dispuesto en la LFPDPPP y la LFTAIPG, la autoridad garante de la protección de datos personales en posesión de los particulares y de las dependencias y entidades federales es el IFAI, organismo descentralizado de la Administración Pública Federal no sectorizado, con personalidad jurídica y patrimonio propios, institución que no obstante su reconocida

[152] La competencia del Tribunal referido se daría de conformidad con lo dispuesto por el artículo 14 fracciones III y XVI de la Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa.

experiencia en el tema de transparencia y acceso a la información pública gubernamental, debido a los importantes logros alcanzados y reconocimiento nacional e incluso internacional en esa materia, éstos han quedado restringidos exclusivamente a las dependencias y entidades de la Administración Pública Federal, sin tener un mayor alcance dado la limitación establecida por la propia LFTAIPG, pero también debido a su naturaleza jurídica, la cual le impide tener presencia como autoridad de la materia ante otros entes públicos federales y locales.

Por lo anterior, la forma como está actualmente estructurado el IFAI no permite alcanzar los propósitos que aquí se pretenden, conforme se ha expuesto a lo largo del presente trabajo. De esta manera, es necesaria ya sea la modificación de este Instituto o la creación de uno nuevo que esté dotado de ciertas características para garantizar el efectivo ejercicio del derecho a la protección de datos personales por parte de sus titulares y su adecuada salvaguarda.

En caso de llevarse a cabo la reestructuración del IFAI, habrá que considerar la viabilidad para salvaguardar dos derechos fundamentales y trascendentales en la sociedad mexicana, que son el de acceso a la información y el de protección de datos personales, en las dimensiones que se proponen, en virtud de que requerirá de una estructura, capacidad económica y humana mayor, a fin de tener presencia y autoridad en todo el territorio nacional. No obstante que ello podría ser factible, en nuestra opinión lo importante es que la sociedad mexicana pueda identificar perfectamente a la autoridad garante de cada derecho fundamental, en este caso el de la protección de datos personales, por lo cual consideramos más viable la creación de un órgano autónomo y especializado en esta materia, a fin de evitar cualquier confusión. Porque habrá que recordar que mientras el derecho de acceso a la información se encuentra basado en el principio de máxima publicidad, el derecho a la protección de datos personales refiere a un principio de autodeterminación informativa, donde el titular es el único que decide cómo, a quién y para qué proporciona sus datos personales; principios que resultan por demás contrarios.

Ahora bien, es importante mencionar que la creación de un nuevo órgano autónomo especializado no afectaría o interrumpiría de modo alguno, la existencia y operación de otros órganos u organismos autónomos creados de conformidad con lo establecido en la fracción IV del artículo 6o. constitucional, que a la letra dice:

> “**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.”

Lo anterior, en razón de que los órganos u organismos referidos en esta disposición son exclusivamente garantes del derecho de acceso a la información y no del derecho a la protección de datos personales como se desprende del texto antes citado.

Con las reformas constitucionales y una Ley General de Protección de Datos Personales como se propone en el presente trabajo, sólo nos restaría contar con un órgano autónomo especializado, el cual se instituya como aquella autoridad garante del derecho a la protección de datos personales a nivel nacional, dotada de autonomía suficiente en la emisión y aplicación de sus resoluciones, así como para ser el principal promotor y difusor de este derecho.

En este orden de ideas, a continuación se analizará la viabilidad de crear el órgano autónomo especializado en la protección de datos personales, mediante la revisión de las características y posibles beneficios que su constitución traería en la salvaguarda de este derecho.

La creación de este órgano a través de la Constitución Política de los Estados Unidos Mexicanos, implicaría dotarlo de una autonomía constitucional de carácter administrativa, financiera y jurídica, para organizarse y administrarse por sí mismo, así como para crear las normas jurídicas que lo regulen, pero sobre todo, ello significaría que no estuviera sujeto a ninguno de los Poderes de la Unión o cualquier autoridad sea federal o local, lo cual garantizaría la efectividad, neutralidad e imparcialidad de sus resoluciones ante cualquier ente, sea público o privado, así como ante cualquier órgano de gobierno, federal, estatal o municipal.

Si bien para la creación de este órgano, en inicio se requerirá de recursos públicos suficientes para su conformación, es posible que para su posterior desarrollo, sean utilizados aquellos ingresos que se obtengan de la aplicación de multas a los infractores de la ley y su reglamento, a fin de solventar sus propios gastos, lo cual le otorgaría una verdadera autonomía financiera. Evidentemente de estos ingresos y gastos, se hará la correspondiente rendición de cuentas, conforme se establezca en la ley de la materia.

Ahora bien, debido a lo innovadora que resulta la materia de protección de datos personales, es indispensable que este órgano sea especializado en la misma, y cuente con amplio conocimiento e información actualizada de este derecho y de todo aquello con lo cual se pueda relacionar, especialmente lo relativo a ciertos sectores específicos como son el tecnológico, financiero, telecomunicaciones, seguridad y salud, para lo cual deberá contar con personal técnico calificado.

Contar con un órgano técnico y de amplio conocimiento en la materia, garantizará la exacta observancia y aplicación de los principios rectores del derecho a la protección de datos personales y de la ley de la materia, con lo cual se logrará el objetivo principal de salvaguardar los derechos de los titulares de datos personales. Asimismo, contar con personal debidamente capacitado en el tema, permitirá brindar una adecuada orientación a los titulares en el ejercicio de sus derechos ARCO y en la cultura del autocontrol y protección de su derecho, consideradas como acciones preventivas; así como la posibilidad de otorgar una oportuna asesoría y capacitación en la protección de datos personales a los Responsables, relacionados con temas de su particular interés, al estar vinculados con el sector donde se desenvuelven, lo cual favorecerá indudablemente en la autorregulación y la aplicación de mejores prácticas por sectores específicos, todo ello para la ampliación de beneficios y medidas de seguridad en el tratamiento de los datos personales.

Se propone que el referido órgano sea denominado Instituto Nacional de Protección de Datos Personales (Instituto) y para garantizar la objetividad, legalidad, imparcialidad y profesionalismo de sus decisiones, se encontrará dirigido por un órgano colegiado, integrado por siete miembros, quienes se propone sean nombrados por el Senado de la República, a fin de incrementar la eficacia de sus resoluciones, al no depender su nombramiento directamente del Ejecutivo Federal. Dichas personas deberán contar con reconocido prestigio y experiencia en la materia y no desempañar ningún otro cargo o función.

Los comisionados durarán en su encargo siete años, sin posibilidad de relección y sin poder tener otro empleo, cargo o comisión. El Instituto será presidido por un Comisionado, quien fungirá como su representante legal. El Comisionado Presidente durará en su cargo un periodo de dos años y será elegido por los otros comisionados.

A fin de dar mayor transparencia y certeza en las tareas encomendadas al Instituto, se recomienda la creación de un órgano asesor del Instituto integrado por diversos sectores públicos y privados de la sociedad, como pueden ser representantes del Congreso de la Unión, autoridades reguladoras en esta materia, federales y locales, universidades, así como cámaras del comercio y la industria.

Este órgano sería denominado Consejo Consultivo del Instituto, el cual se desarrollaría a través de sesiones ordinarias, mismas que se llevarían a cabo, cuando menos cada tres meses, sin menoscabo que se pudieren celebrar sesiones extraordinarias, con causa justificada y mediante solicitud de algunos de los miembros del Consejo Consultivo o de los Comisionados del Instituto.

Las decisiones se tomarían por mayoría de votos y sus atribuciones serían:

- Ofrecer alternativas de solución a los diversos casos, que por su relevancia, el Pleno del Instituto considere sean revisados por el Consejo Consultivo.
- Emitir opiniones en relación con las diversas consultas que se sometan al Consejo.
- Brindar asesoría especializada a los Comisionados del Instituto en temas relacionados con la protección de datos personales.
- Proporcionar información actualizada sobre la materia de protección de datos personales, tanto a nivel nacional como internacional.
- Realizar estudios pormenorizados de los principales problemas en la materia para brindar soluciones adecuadas, conforme a las necesidades vigentes.
- Auxiliar al Pleno del Instituto en la conformación de criterios para la aplicación de la ley y su reglamento, así como verificar que se encuentren publicados en su página de Internet para conocimiento del público.
- Revisar y aprobar los informes trimestrales que le remita el Pleno del Instituto con relación a las actividades realizadas en el mes inmediato interior. Los informes deberán contener datos como: número de asuntos (solicitudes, quejas o resoluciones) recibidos en cada procedimiento (Protección de Derechos, Verificación e Infracciones) en el trimestre que se informa, asuntos pendientes y atendidos, resoluciones emitidas y el sentido de las mismas. En caso de infracciones, montos impuestos a los infractores y datos de los reincidentes.

Al considerar la aplicación de una sola ley para entes públicos y privados, no se puede desconocer su particular naturaleza, por lo cual se requerirá de dos áreas distintas que se encarguen de desahogar las solicitudes y cualquier requerimiento relacionados con cada uno de ellos, es decir dos secretarías de protección de datos, una para entes públicos y otra para entes privados.

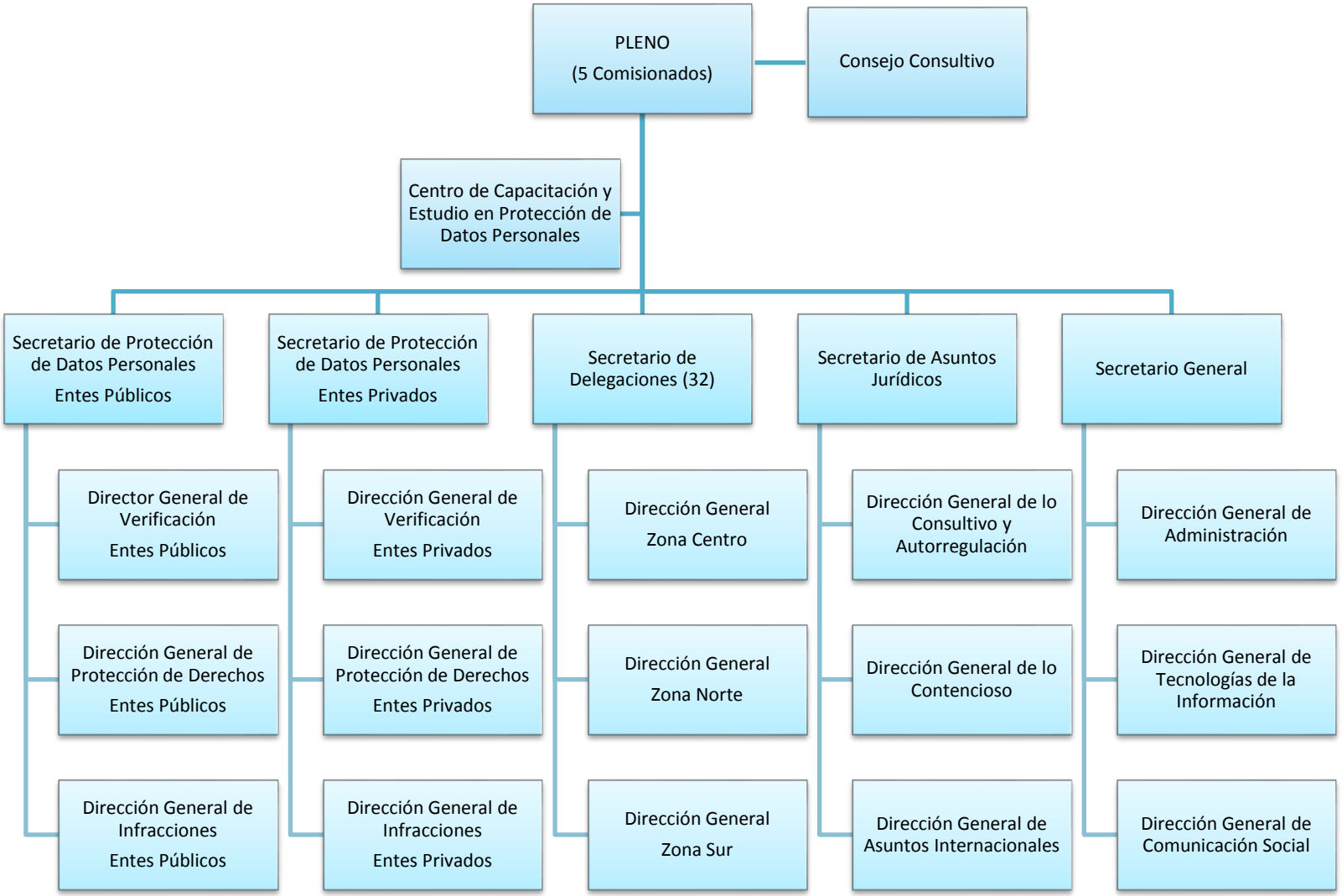
Las atribuciones del Instituto serán las mismas que ya establece el artículo 39 de la LFPDPPP, con la adición de unas, para quedar de la siguiente manera:

- Vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;
- Interpretar en el ámbito administrativo la presente Ley;
- Brindar asesoría a los titulares de los datos personales en el ejercicio de sus derechos ARCO y en la presentación de solicitudes de protección de derechos.

- Proporcionar apoyo técnico a los Responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;
- Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de la Ley, para efectos de su funcionamiento y operación;
- Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;
- Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en la Ley e imponer las sanciones según corresponda;
- Cooperar con otras autoridades de supervisión federales o locales y con organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos;
- Rendir al Congreso de la Unión un informe anual de sus actividades;
- Acudir a foros internacionales en el ámbito de la Ley;
- Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes;
- Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales y brindar capacitación a los Responsables, y
- Las demás que le confieran esta Ley y demás ordenamientos aplicables.

Para el ejercicio de las atribuciones y el despacho de los asuntos que le competen al Instituto contará con la siguiente estructura, conforme al siguiente organigrama:

ESTRUCTURA ORGÁNICA
DEL INSTITUTO NACIONAL DE PROTECCIÓN DE DATOS PERSONALES



Los secretarios de protección de datos tendrán facultades para coordinar y supervisar la sustanciación de los tres procedimientos a su cargo, es decir, el de protección de derechos, de verificación y de infracciones. A sus directores generales se les darán las facultades necesarias para sustanciar directamente los procedimientos, entre las que se encontrarán desde luego, la posibilidad de imponer medidas de apremio y precautorias como se señaló en el apartado de la ley general.

Es importante mencionar que el personal encargado de realizar las verificaciones deberá contar con conocimientos especializados en sistemas y tecnologías de la información, a fin de llevar a cabo las revisiones a las bases de datos de los Responsables de manera adecuada, por lo cual deberá contar con conocimientos técnicos especializados. Al respecto, sería importante que por la versatilidad de la materia, dicho personal esté en constante capacitación, para su actualización, por lo cual se sugiere que el Instituto cuente con un Centro de Capacitación y Estudio en Protección de Datos Personales.

En dicho centro se impartirían cursos de capacitación y actualización en materia de protección de datos personales, técnica y especializada, en beneficio del personal que labore en el Instituto o, incluso, de los propios titulares y Responsables que así lo requieran. Además podría contar con una biblioteca encargada de la adquisición, conservación, estudio y exposición de libros y documentos en esta materia, tanto a nivel nacional como internacional. También podrían organizarse intercambios con otros países como retroalimentación en información, material y mecanismos para garantizar este derecho.

El secretario de delegaciones se encargará de coordinar y supervisar las tareas encomendadas a los delegados estatales del Instituto, siendo el enlace con las oficinas centrales. Esta secretaría llevará un reporte estadístico de las consultas y solicitudes presentadas en las delegaciones. Asimismo se encargará de la atención que se brinde en las mismas. En coordinación con las áreas competentes organizará los cursos de capacitación y eventos que se realicen en las delegaciones. Además podrá proponer la celebración de convenios, acuerdos y demás instrumentos jurídicos para la colaboración y participación de gobiernos estatales, dependencias gubernamentales u organizaciones locales, para la promoción y protección de datos personales.

En cuanto al secretario de asuntos jurídicos se encargará de atender las consultas jurídico administrativas que se presenten respecto de la materia, así como llevar los juicios administrativos y judiciales en los que el Instituto sea parte. Asimismo participará en eventos y foros internacionales relativos a la materia, así como promoverá la cooperación internacional para la efectiva tutela de la protección de datos personales y la difusión de mejores prácticas.

Finalmente, por lo que se refiere al secretario general, tendrá las atribuciones necesarias para la administración del personal, así como de los recursos financieros y tecnológicos necesarios para el cumplimiento de las funciones encomendadas al Instituto.

Asimismo se suman a esta propuesta integral las acciones de gobierno que pudieran emprenderse en la materia, las cuales requerirán definitivamente de la participación de la sociedad por ser un fenómeno común y presente en todos los sectores y actividades de nuestra vida diaria, por lo cual se proponen las siguientes:

- Fomentar a nivel nacional la cultura del derecho a la protección de datos personales, a través de información actualizada relativa al control de datos personales, difundida en los distintos medios de comunicación.
- Mayor concientización en los titulares de los datos, respecto de los principales problemas y posible afectación a su privacidad, derivado de su falta de conocimiento y control de los datos personales que proporcionan diariamente a través de diversos medios. Al respecto, se deberá dar especial atención a los niños y adolescentes en el uso de las diversas herramientas tecnológicas.
- Establecer medidas preventivas para la protección de datos personales, a fin de evitar futuros conflictos, mediante la revisión constante de las medidas de seguridad y establecimiento de avisos de privacidad actualizados y accesibles para los titulares.
- Fomentar la aplicación de niveles apropiados de confidencialidad de acuerdo con la información que se trate, y especialmente cuando sea transferida.
- Realización de estudios e investigaciones relativas a la protección de datos personales, a nivel nacional e internacional, a fin de detectar los fenómenos que requieren de mayor atención y establecer las posibles alternativas de solución.
- Mantener una constante coordinación con las autoridades reguladoras de la materia a nivel federal y local, así como con todo organismo o asociación relacionado con la materia.

Con esta propuesta planteada en el presente trabajo se logrará la debida salvaguarda del derecho fundamental a la protección de datos personales, que por su reconocimiento en la Constitución Política de los Estados Unidos Mexicanos y la reciente emisión de la LFPDPPP, hacen necesaria su evaluación no sólo en la actualidad, sino también en un futuro inmediato, donde se visualiza como un derecho

bien consolidado sobre bases constitucionales, legales e institucionales que permitirán garantizar no sólo este derecho sino también aquellos derechos básicos relacionados con el mismo, como son vida privada, privacidad e intimidad de todo individuo, a fin de lograr su más amplia y total protección.

Como se comentó al inicio del presente trabajo, el derecho a la protección de datos personales es un derecho relativamente reciente en México, pues a tres años de haberse incluido expresamente en la Constitución Política de los Estados Unidos Mexicanos, y a dos años de contar con una ley de la materia, todavía falta camino por recorrer; por ello, este gran avance por reconocerlo como derecho fundamental, deberá tomarse como el inicio y no como el fin de esta enorme tarea para garantizarlo, pues además de establecerse en nuestra Carta Magna, como ésta lo ordena, deberán establecerse los mecanismos adecuados para alcanzar su óptima salvaguarda, lo cual finalmente determinará si efectivamente se logra con este objetivo.

De esta manera, y considerando una visión a corto y largo plazo del desarrollo y evolución de este derecho, después de realizar el presente trabajo de investigación, podemos concluir que en la forma como actualmente se encuentra regulado el derecho a la protección de datos personales en el sistema jurídico mexicano, no se garantiza de manera plena este derecho a sus titulares, motivo por el cual será necesario realizar las adecuaciones necesarias, tanto legales como institucionales, como se propone en este capítulo. No obstante, es relevante tener en cuenta que esta tarea requerirá no sólo de la intervención de las autoridades sino de todos aquellos sujetos involucrados en el ejercicio de este derecho, sean entes públicos, privados, personas jurídicas o físicas, a fin de lograr tanto el tratamiento como la protección de datos personales de manera responsable e informada, toda vez que lo más importante en este derecho es la protección, no de datos aislados y sus bases donde consten, sino de todos los individuos que requieren y exigen de los demás, un mínimo de respeto a su vida privada y a su dignidad humana.

CONCLUSIONES

Primera. Del análisis realizado a los diversos ordenamientos que regulan el derecho a la protección de datos personales, confirmamos la hipótesis planteada al inicio del trabajo, consistente en afirmar que actualmente en el sistema jurídico mexicano no se brindan las condiciones legales e institucionales adecuadas para la salvaguarda plena de este derecho, en los términos establecidos en la Constitución Política de los Estados Unidos Mexicanos y los tratados internacionales suscritos y aprobados por México, no obstante de su reconocimiento expreso en el artículo 16 constitucional y la existencia de una ley de la materia, pero limitada a la aplicación de entes privados. Ante dicha situación, la presente investigación culmina con la presentación de una propuesta integral consistente en la emisión de una Ley General de Protección de Datos Personales y la creación de un órgano autónomo constitucional, que permita garantizar el ejercicio efectivo del derecho a la autodeterminación informativa de los titulares, de manera plena y siempre a favor de los individuos.

Segunda. Es innegable que el tratamiento de los datos personales trae importantes beneficios económicos y, por lo tanto, es visto como un bien valioso y necesario en la actualidad. Sin embargo, los meros datos aislados no tendrán dicho carácter hasta en tanto se vinculen con sus titulares y puedan crearse perfiles bien definidos que, convertidos en clientes potenciales, se traducirán en ingresos económicos. Así, la transferencia de datos personales se vuelve una importante actividad comercial, que requiere de una regulación especial, pues en este caso, no se dispone de mercancías fácilmente manipulables y trasladables sino de datos personales que requieren del consentimiento de sus dueños. Por ello y a fin de garantizar adecuadamente este derecho, es necesario a nivel internacional, contar con la cooperación de los Estados en el establecimiento de estándares mínimos de protección de los datos personales, a través de documentos internacionales vinculantes, para lograr la armonización de los diversos modelos de protección existentes, así como el equilibrio entre la salvaguarda de este derecho y el progreso económico.

Tercera. Actualmente, compartir cualquier tipo de información, incluyendo la personal, es una actividad común que se facilita en gran medida con el uso de las TIC’s, por lo que uno de los principales desafíos a enfrentar en México, es la adquisición de una amplia cultura en la protección de datos personales, por parte de titulares, Responsables, Encargados y

autoridades. Esto se podrá realizar a través de acciones de gobierno orientadas a cada uno de los sujetos involucrados, consistente en difundir información completa y actualizada en la materia, así como de las disposiciones aplicables, que permitan conocer y distinguir de manera clara y accesible, las características y los alcances de este derecho, para prevenir y concientizar, principalmente a la población, de las consecuencias negativas que trae una entrega irresponsable y desinformada de los datos personales, sin tomar la más mínima medida de seguridad, porque es innegable que, en primer instancia, sólo corresponde a los titulares, el deber de ejercer su derecho a la autodeterminación informativa de manera responsable e informada, previo a cualquier tratamiento de sus datos personales.

Cuarta. Si bien existen contradicciones, ambigüedades y lagunas en las leyes de la materia, al ser el derecho a la protección de datos personales un derecho humano reconocido en la Carta Magna y en tratados internacionales suscritos y aprobados por México, este derecho deberá ser garantizado en la forma como se establece en el artículo 1o. constitucional, es decir, con una interpretación de la Ley Suprema que favorezca, en todo momento a las personas, la protección más amplia. Bajo este principio *pro homine* y el de convencionalidad, es que la autoridad garante llevará a cabo la protección de los derechos ARCO de los titulares, especialmente al momento de sustanciar los procedimientos contemplados en la ley de la materia, considerados como los principales mecanismos de defensa que tienen los titulares ante la vulneración de sus derechos.

Quinta. Los ordenamientos mexicanos que regulan el derecho a la protección de datos personales, se encuentran divididos en razón de la naturaleza jurídica de los sujetos que llevan a cabo el tratamiento de los datos personales, es decir pública o privada; lo cual trae como consecuencia, una protección segmentada, como si se tratare de dos derechos distintos, a lo cual se adiciona la confusa relación entre el derecho de acceso a la información y el derecho a la protección de datos personales en poder de entes públicos, cuando son regulados en una misma ley, no obstante de sus indiscutibles diferencias. De esta manera, y al tomar en cuenta que lo primordial es la protección amplia de los derechos de los titulares, independientemente de los sujetos quienes tratan los datos personales (sean entes públicos o privados sus obligaciones serán las mismas al momento de llevar cabo el tratamiento de los datos), se propone que el derecho a la protección de datos personales sea regulado de manera

uniforme, a través de una única ley, denominada Ley General de Protección de Datos Personales.

Sexta. En términos generales el Reglamento de la LFPDPPP es técnico y complejo, lo cual dificulta su entendimiento en inicio y, por lo tanto, su aplicación en casos concretos, lo cual puede repercutir en perjuicio del ejercicio de los derechos del titular. Por ejemplo, resulta confuso y va más allá de la ley, cuando establece excepciones sólo para la aplicación del propio Reglamento, más no así para la aplicación de la ley de la materia, lo que resulta incongruente. Para el caso del plazo para presentar solicitudes por falta de respuesta, es omiso en establecer un plazo específico, limitándose a remitir al establecido en el artículo 45 de la LFPDPPP, el cual no es preciso para este supuesto. Por lo que se refiere al procedimiento, contempla el supuesto cuando el Responsable no acuse de recibo la solicitud del titular o se niegue a recibirla, pero no establece la forma como la autoridad intervendrá si el Responsable no remite su respuesta. Por eso se propone su revisión integral o, en su caso, la emisión de uno nuevo que sea acorde con la Ley General de Protección de Datos Personales propuesta.

Séptima. La LFPDPPP no considera en el ejercicio de los derechos ARCO, algunos supuestos relevantes y comunes en la actualidad, como son la obtención de datos personales en solicitudes de empleo, de crédito, de ingreso a escuelas o clubes, entre otros, sin llegar a concretar algún tipo de relación entre el titular y el Responsable, por lo cual se propone la cancelación inmediata de datos, después de haberse emitido la negativa, sin necesidad de entrar a un periodo de bloqueo, para su eliminación definitiva. Otra situación es el tratamiento de datos personales por parte de terceros que forman parte de los grupos comerciales de los Responsables, quienes por el sólo hecho de estar señalados de manera general en el aviso de privacidad, llevan a cabo el tratamiento de datos personales, sin necesidad de obtener de manera directa y previa, el consentimiento de su titular, lo cual se considera violatorio del derecho a la autodeterminación informativa de los individuos para decidir a quién y para qué proporcionan sus datos personales, motivo por el cual se debe contemplar en la ley general propuesta, la obtención previa del consentimiento del titular en estos casos.

Octava. Dentro de las excepciones a la LFPDPPP se encuentran las sociedades de información crediticia, encargadas de recopilar, manejar y entregar o enviar información relativa al historial crediticio de personas físicas o morales, de acuerdo con lo dispuesto en la Ley para Regular las

Sociedades de Información Crediticia, la cual no obstante de prever de manera especial la protección de datos personales, bajo la figura del Secreto Financiero y la aplicación de sanciones administrativas y penales con el delito de revelación de secretos; al no contemplar intervención alguna de la autoridad garante del derecho a la protección de datos personales, limita el ejercicio de los derechos ARCO de los titulares ante estos entes, dejándolos en total desventaja y desprotección, pues no es posible aplicar en caso de vulneración en esta materia específica, la legislación de la materia. Debido a ello, se propone eliminar esta excepción de la ley general, sin que ello impida continuar con la aplicación de la Ley para Regular las Sociedades de Información Crediticia, pero sin limitar el ejercicio del derecho fundamental de los titulares. Es por eso que previo a la emisión de la ley general se debe realizar la revisión exhaustiva de ésta y otras leyes regulatorias de materias específicas, como son salud, finanzas, protección al consumidor, telecomunicaciones, entre otras, relacionadas con la protección de datos personales, a fin de aplicarlas de una manera armónica y congruente.

Novena. De acuerdo con el artículo 73 fracción XXIX-O constitucional, legislar en materia de protección de datos personales en posesión de los particulares, es facultad exclusiva del Congreso de la Unión. En consecuencia, los Estados y el Distrito Federal, con fundamento en los artículos 6o. y 124 constitucional, regulan actualmente el derecho a la protección de datos personales en poder de entes públicos, como un principio del derecho al acceso a la información, dentro de sus leyes de transparencia, aunque estados como Campeche, Colima, Guanajuato, Oaxaca, Tlaxcala y el Distrito Federal, cuentan ya con una ley específica en esta materia, todo lo cual ha provocado la emisión de diferentes ordenamientos regulatorios de un mismo derecho. Por lo anterior, y como propuesta integral, se propone modificar el artículo 73 fracción XXIX-O, a fin de otorgar facultades exclusivas al Congreso de la Unión en materia de protección de datos personales, pero sin distinguir entre los sujetos que los poseen, así como al artículo 6o. constitucional para remitir a la ley de la materia, en información relativa a datos personales. De esta manera, con la emisión de la nueva ley general se ordenaría la derogación o abrogación, según sea el caso, de todas aquellas disposiciones secundarias y locales que regulan este derecho, bajo un esquema transitorio de vigencia de las leyes existentes, hasta en tanto se emita la ley general.

Décima. En el sistema jurídico mexicano existen diversos ordenamientos que regulan la protección de datos personales, tanto a nivel federal como local, los cuales establecen diferentes procedimientos, derechos, plazos, criterios, principios y mecanismos de protección, que pueden ir desde los más completos hasta los más limitados, todo lo cual propicia una salvaguarda disímil en desventaja de los titulares y, en consecuencia, en contra de lo establecido en el párrafo segundo del artículo 16 constitucional. De esta manera, y a fin de lograr la homogeneidad a favor de los derechos de los titulares, se propone emitir la Ley General de Protección de Datos Personales, la cual al ser reglamentaria de dicho precepto constitucional, regulará de manera armónica y uniforme, la protección de datos personales en todo el territorio nacional. Lo anterior, no será impedimento para que las autoridades federales y locales, en su carácter de Responsables, puedan a través de la autorregulación, como sucede con los particulares, emitir su propia normatividad para regular sus procedimientos internos, plazos, mecanismos de seguridad y todo aquello que facilite el ejercicio de los derechos ARCO de los titulares.

Décima Primera. De la diversidad de ordenamientos mexicanos que regulan el derecho a la protección de datos personales, también observamos una pluralidad de autoridades garantes de este derecho, federales y locales, lo cual trae como consecuencia la emisión de igual número de criterios para interpretar y aplicar las leyes de la materia, y con ello una protección desigual del derecho. De esta manera, proponemos la existencia de un único órgano garante, cuya creación devenga de la propia Carta Magna, establecido como órgano autónomo especializado, en el segundo párrafo de su artículo 16. La autonomía sería en su administración, organización y dirección, sin sujeción a ninguna autoridad federal o local, que obstaculice o limite la protección plena y efectiva de este derecho y garantice la imparcialidad y objetividad de sus resoluciones. Por otra parte, el órgano será especializado, por lo técnico, complejo y versátil que puede resultar esta materia, lo cual garantizará la adecuada aplicación de la ley general, al contar con la dirección de un Órgano Colegiado, auxiliado por un Consejo Consultivo, todos expertos y conocedores de los diversos temas relacionados con la protección de datos personales, así como con personal capacitado y actualizado en la materia.

MESOGRAFÍA

Bibliografía

ÁLVAREZ, Clara Luz, *Internet y derechos fundamentales,* Porrúa y Universidad Panamericana, México, 2011, pp. 283.

BASTERRA, Marcela I., *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados Derecho Constitucional Provincial Iberoamérica y México*, Buenos Aires, Ediar, México, Universidad Nacional Autónoma de México, 2008, pp. 624.

CUADRA, Héctor, *La Proyección Internacional de los Derechos Humanos*, Instituto de Investigaciones Jurídicas, Serie B. Estudios comparativos, b) Estudios especiales, número 10, México, 1970, pp. 308.

FERRAJOLI, Luigi, *Derechos y garantías. La ley del más débil,* Capítulo 2. Derechos Fundamentales, Madrid, Trotta, 2004, pp. 37-72.

GARCÍA MÁYNEZ, Eduardo, *Introducción al estudio del Derecho*, Porrúa, quincuagésima séptima edición, México, 2004, pp. 444.

LEÓN, Leysser L., *El problema jurídico de la manipulación de información personal*, Colección Derecho PUCP, número 2, Ed. Palestra, Perú, 2007, pp. 431.

OVILLA Bueno, Rocío, *La protección de los datos personales en México*, Porrúa, México, 2005, pp. 72.

Libros electrónicos

GÓMEZ-ROBLEDO, Alonso y Lina, Ornelas Núñez, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal,* Instituto de Investigaciones Jurídicas, Serie Estudios Jurídicos, número 97, México, 2006, ISBN 970-32-3913-7, formato pdf, disponible en http://biblio.juridicas.unam.mx/libros/5/2299/3.pdf, pp. 74.

GREGORIO, Carlos G., "Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina", *Transparentar al Estado: la experiencia mexicana de acceso a la información*, Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, número 193, México, 2004, primera reimpresión 2005, ISBN 970-32-1836-9, formato pdf, disponible en http://biblio.juridicas.unam.mx/libros/3/1407/12.pdf, pp. 299-325.

MUÑOZ DE ALBA MEDRANO, Marcia, "Los nuevos derechos humanos en la era tecnológica: ¿El Habeas Data… la solución?"*, V Congreso Iberoamericano de Derecho Constitucional*, Instituto de Investigaciones Jurídicas, México, 1998, Serie G: Estudios Jurídicos, número 193, ISBN 968-36-6786-4, formato pdf, disponible en: http://biblio.juridicas.unam.mx/libros/1/113/28.pdf, pp. 583-599.

REBOLLO DELGADO, Lucrecio, *El derecho fundamental a la intimidad*, segunda edición actualizada, Dykinson, S.L., Madrid, 2005, ISBN 84-9772-698-7, disponible en http://books.google.com.mx/books?hl=es&id=S9_loNaIDyUC&q=intimidad#v=snippet&q=intimidad&f=false, pp. 468.

Hemerografía

Impresos

ESCALANTE GONZALBO, Fernando. *El Derecho a la privacidad*, 02 Cuadernos de transparencia del Instituto Federal de Acceso a la Información y Protección de Datos, México, marzo 2004, octava reimpresión, octubre 2010, pp. 43.

FIRMA DAVARA ABOGADOS, S.C., "¿Y sus datos están protegidos?", *IDC Asesor Jurídico y Fiscal*, Ediciones Especiales IDC 2012, Boletín quincenal, Año 25, cuarta época, Grupo Expansión, México, enero 2012, pp. 81.

Electrónicos

AGENCE FRANCE-PRESSE, "Datos personales, mina de oro para los gigantes de internet", Periódico Organización Editorial Mexicana, Sección Ciencia y Tecnología, 24 de enero de 2012, disponible en http://www.oem.com.mx/laprensa/notas/n2398578.htm

AGENCIA ID, "Promueven tecnología para eliminar en su totalidad archivos digitales", Periódico Vanguardia de Saltillo, Sección Tecnología, Fuente Agencia Id, 28 de agosto de 2012, disponible en http://www.vanguardia.com.mx/promueventecnologiaparaeliminar ensutotalidadarchivosdigitales-1361370.html

BAZÁN, Víctor, "El *habeas data* y el derecho de autodeterminación informativa en perspectiva de derecho comparado", *Estudios Constitucionales*, Vol. 3, número 002, Centro de Estudios Constitucionales, Santiago, Chile, Red de Revistas Científicas de América Latina y el Caribe, España y Portugal, Universidad Autónoma del Estado de México, 2005, ISSN 0718-0195, formato pdf, disponible en http://redalyc.uaemex.mx/pdf/820/820 30204.pdf, pp. 85-139.

COMUNICADO IFAI/081/12, Oaxaca, Oaxaca, 18 de junio de 2012, "Propone Sigrid Arzt promover una Ley General de Transparencia y Acceso a la Información", Foro Regional *Los órganos autónomos en las propuestas para una política de rendición de cuentas ¿Centralismo, federalismo o cooperación?*, disponible en http://www.ifai.org.mx/Publicaci ones/comunicados.

DE DIENHEIM BARRIGUETE, Cuauhtémoc Manuel, "El Derecho a la intimidad, al honor y a la propia imagen", *Derechos Humanos*, Órgano Informativo de la Comisión de Derechos Humanos del Estado de México, Número 57, septiembre-octubre 2002, ISSN 1405-5627, formato pdf, disponible en http://www.juridicas.unam.mx/publica/librev/rev/derhum/ cont/57/pr/pr28.pdf, pp. 59-65.

EL SOL DE MÉXICO, "Preparan lineamientos para exhibir a presuntos delincuentes", Sección Ciudad, 19 de junio de 2012, disponible en http://www.tedf.org.mx/sala_prensa/sintesis/ sm2012/jun/120619/120619_cdhdf_preparan_lineamientos.pdf.

ESTRADA CORONA, Adrián, "El ejercicio de los derechos humanos en México, fruto de una lucha constante de la sociedad civil. Entrevista con el Mtro. Emilio Álvarez Icaza Longoria", *Revista Digital Universitaria*, 1 de julio 2010, Vol. 11, número 7, ISSN: 1607-6079, formato pdf, disponible en http://www.revista.unam.mx/vol.11/num7/art72/art72.pdf pp. 1-6.

GARCÍA GONZÁLEZ, Aristeo, "La protección de datos en la administración electrónica. Aspectos generales", *Derecho comparado de la información*, número 14, julio-diciembre

2009, obra del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, ISSN 1870-0594, formato pdf, disponible en http://www.juridicas.unam.mx/publica/librev/rev/decoin/cont/14/art/art3.pdf, pp. 81-110.

GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado", *Boletín Mexicano de Derecho Comparado*, número 120, septiembre-diciembre 2007, obra del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM, ISSN 0041 8633, formato pdf, disponible en: http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/120/art/art3.pdf, pp. 743-778.

DEPARTAMENTO DE ESTADO DE LOS ESTADOS UNIDOS DE AMÉRICA, Oficina de Programas y Servicios de Información, "Guía de acceso a la información", 17 de abril de 2012, versión en español, disponible en http://www.state.gov/documents/organization/145341.pdf, pp. 1-29.

MARTÍ DE GIDI, Luz del Carmen, "Vida privada, honor, intimidad y propia imagen como derechos humanos"*, Letras jurídicas*, Volumen 8, Año 4, julio-diciembre 2003, Revista del Centro de Estudios sobre Derecho, Globalización y Seguridad de la Universidad Veracruzana, ISSN 1665 1529, formato pdf, disponible en http://www.letrasjuridicas.com/Volumenes/8/luz8.pdf, pp. 115-126. [El artículo en formato pdf no se encuentra numerado].

OFICINA DEL COMISIONADO PARA LA PROTECCIÓN DE DATOS DE IRLANDA, *Registrarse, entrar, darse de baja. Proteger tu privacidad y controlar tus datos. Un recurso para el profesorado*, redacción, edición adaptada y publicación a cargo de la Agencia Española de Protección de Datos y de las Comunidades Autónomas de Madrid, Cataluña y Euskadi, 2007, ISBN 978-0-9557 187-0-0, formato pdf, disponible en http://www.avpd.euskadi.net/s04-5273/es/contenidos/informacion/documentos_difusion/es_difusion/adjuntos/guia-educativa.pdf, pp. 1-119.

SIERRA CABALLERO, Francisco, "La guerra en la era de la información: propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación"*, Sphera Pública*, revista de Ciencias Sociales y de la Comunicación, publicación anual, número 003, Universidad Católica San Antonio de Murcia, España, 2003, ISSN: 1180-9210, Red de revistas científicas de América Latina y El Caribe, España y Portugal, formato pdf, disponible en http://redalyc.uaemex.mx/pdf/297/29700314.pdf, pp. 253-267.

TREJO DELARBRE, Raúl, "Vivir en la sociedad de la información. Orden global y dimensiones locales en el universo digital", *La Sociedad de la Información,* Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación, Organización de Estados Iberoamericanos para la Educación, la Ciencia y la Cultura (OEI), España, Número 1, septiembre-diciembre 2001, ISSN: 1681-5645, [en línea], disponible en http://www.oei.es/revistactsi/numero1/trejo.htm.

VÁZQUEZ BOTE, Eduardo, "Los denominados derechos de la personalidad", *Boletín Mexicano de Derecho Comparado*, número 18, septiembre – diciembre 1973, Nueva Serie Año VI, ISSN 0041 8633, formato pdf, disponible en http://biblio.juridicas.unam.mx/revista/pdf/DerechoComparado/18/art/art3.pdf, pp. 403-439.

VELASCO SAN MARTÍN, Cristos, *Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?,* Boletín de Política

Informática, Instituto Nacional de Estadística, Geografía e Información, número 1, 2003, formato pdf, disponible en http://www.inegi.gob.mx/inegi/contenidos/espanol/prensa/contenidos/Articulos/tecnologia/libertad.pdf, pp. 1-12.

Legislación

Legislación federal mexicana

Constitución Política de los Estados Unidos Mexicanos.

Tratados Internacionales suscritos por México y aprobados por el Senado

Convención de la Organización de Cooperación y el Desarrollo Económicos.
Lugar y fecha de adopción: París, 14 de diciembre de 1960.
Firma ad referéndum México: 14 de abril de 1994.
Aprobación Senado: 10 de mayo de 1994 (DOF 13 de mayo de 1994).
Publicación DOF promulgación: 5 de julio de 1994.
Entrada en vigor para México: 18 de mayo de 1994.
Nota: Al momento de firmar la Convención, el Gobierno de México suscribió la **Declaración sobre la Aplicación de sus Obligaciones como Miembro de la OCDE**, adoptada en París, el 14 de abril de 1994, aprobada simultáneamente por el Senado de la República.

Pacto Internacional de Derechos Civiles y Políticos.
Lugar y fecha de adopción: Asamblea General de las ONU, Nueva York, 16 de diciembre de 1966. Resolución 2200 A (XXI).
Aprobación Senado: 18 de diciembre de 1980 (DOF 9 de enero de 1981).
Publicación DOF promulgación: 20 de mayo de 1981 (Fe de erratas 22 de junio de 1981).
Entrada en vigor para México: 23 de junio de 1981.

Convención de Viena sobre el Derecho de los Tratados.
Lugar y fecha de adopción: Viena, Austria, 23 de mayo de 1969.
Firma ad referéndum México: 23 de mayo de 1969.
Aprobación Senado: 29 de diciembre de 1972 (DOF 28 de marzo de 1973).
Publicación DOF promulgación: 14 de febrero de 1975.
Entrada en vigor para México: 27 de enero de 1980.

Convención Americana sobre Derechos Humanos.
Lugar y fecha de adopción: San José, Costa Rica, el 22 de noviembre de 1969.
Aprobación Senado: 18 de diciembre de 1980 (DOF 9 de enero de 1981).
Publicación DOF promulgación: 7 de mayo de 1981.
Entrada en vigor para México: 24 de marzo de 1981.

Convención de Viena sobre el Derecho de los Tratados entre Estados y Organizaciones Internacionales o entre Organizaciones Internacionales.
Lugar y fecha de adopción: Viena, Austria, 21 de marzo de 1986.
Firma ad referéndum México: 21 de marzo de 1986.
Aprobación Senado: 11 de diciembre de 1987 (DOF 11 de enero de 1988).
Publicación DOF promulgación: 28 de abril de 1988.
Entrada en vigor para México: No ha entrado en vigor general.

Convención sobre los Derechos del Niño.
Lugar y fecha de adopción: Nueva York, 20 de noviembre de 1989.
Firma ad referéndum México: 26 de enero de 1990.
Aprobación Senado: 19 de junio de 1990 (DOF 31 de julio de 1990).
Publicación DOF promulgación: 25 de enero de 1991.
Entrada en vigor para México: 21 de octubre de 1990.

Acta Final de la Ronda de Uruguay de Negociaciones Económicas Multilaterales y, por lo tanto, el Acuerdo por el que se Establece la Organización Mundial del Comercio.
Lugar y fecha de adopción: Marrakech, Marruecos, 15 de abril de 1994.
Firma ad referéndum México: 15 de abril de 1994.
Aprobación Senado: 13 de julio de 1994 (DOF 4 de agosto de 1994).

Publicación DOF promulgación: 30 de diciembre de 1994.
Entrada en vigor para México: 1 de enero de 1995.

Convención sobre los derechos de las personas con discapacidad.
Lugar y fecha de adopción: Asamblea General de la ONU, Nueva York, 13 de diciembre de 2006.
Firma ad referéndum México: 30 de marzo de 2007.
Aprobación Senado: 27 de septiembre de 2007 (DOF 24 de octubre de 2007).
Publicación DOF promulgación: 2 de mayo de 2008.
Entrada en vigor para México: 3 de mayo de 2008.

Legislación federal

Código Civil Federal.
Código Fiscal de la Federación.
Código Penal Federal.
Código Federal de Procedimientos Civiles.

Ley de Amparo, Reglamentaria de los artículos 103 y 107 de la Constitución Política de los Estados Unidos Mexicanos.
Ley de Protección y Defensa al Usuario de Servicios Financieros.
Ley de Seguridad Nacional.
Ley de Vías Generales de Comunicación.
Ley del Sistema Nacional de Información Estadística y Geográfica.
Ley Federal de los Derechos del Contribuyente.
Ley Federal de Procedimiento Contencioso Administrativo.
Ley Federal de Protección al Consumidor.
Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
Ley Federal de Telecomunicaciones.
Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
Ley Federal del Derecho de Autor.
Ley Orgánica del Tribunal Federal de Justicia Fiscal y Administrativa.
Ley para regular las Sociedades de Información Crediticia.
Ley sobre la Celebración de Tratados.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicado en el Diario Oficial de la Federación el 2 de abril de 2004.
Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de la Cámara de Diputados, publicado en el Diario Oficial de la Federación el 6 de abril de 2009
Reglamento Interior del IFAI, publicado en el Diario Oficial de la Federación el 29 de octubre de 2012.

Acuerdo General de la Comisión para la Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales de la Suprema Corte de Justicia de la Nación, del nueve [diez] de julio de dos mil ocho, relativo a los órganos y procedimientos

para tutelar en el ámbito de este Tribunal los derechos de acceso a la información, a la privacidad y a la protección de datos personales garantizados en el artículo 6o. constitucional, publicado en el Diario Oficial de la Federación el 15 de julio de 2008.

Lineamientos de Protección de Datos Personales emitidos por el Instituto Federal de Acceso a la Información y Protección de Datos, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005, modificados el 17 de julio de 2006.

Lineamientos del Aviso de privacidad, publicados en el Diario Oficial de la Federación el 17 de enero de 2013.

Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicados en el Diario Oficial de la Federación el 17 de enero de 2013

Resolución del H. Consejo de Representantes de la Comisión Nacional de los Salarios Mínimos que fija los salarios mínimos generales y profesionales vigentes a partir del 1 de enero de 2012, publicada en el Diario Oficial de la Federación el 19 de diciembre de 2011.

Legislación estatal

Ley de Acceso a la Información Pública del Estado de Sinaloa, Decreto N° 84, publicado en el Periódico Oficial "El Estado de Sinaloa" N° 051 del 26 de abril de 2002, visible en http://www.transparenciasinaloa.gob.mx/images/stories/ARCHIVOS%20PUBLICOS/Leyes%20Estatales%20Actuales/ley%20acceso%20informacion.pdf

Ley de Acceso a la Información Pública del Estado de Sonora, Ley número 156, publicado en el Boletín Oficial, N° 16, Sección II, de fecha 25 de febrero de 2005, visible http://www.congresoson.gob.mx/Leyes_Archivos/doc_21.pdf

Ley de Acceso a la Información Pública para el Estado de Tlaxcala, Decreto N° 100, publicado en el Periódico Oficial del Gobierno del Estado en el Tomo XCI, Segunda época, N° Extraordinario, el 22 de mayo de 2012, visible en http://www.caip-tlax.org.mx/pdf/LAIP.pdf

Ley de Acceso a la Información Pública para el Estado y los Municipios de Guanajuato, Decreto número 198, publicado en el Periódico Oficial, 120 Segunda Parte, del 29 de julio de 2003, visible en http://transparencia.guanajuato.gob.mx/archivos/laip.pdf

Ley de Acceso a la Información Pública para el Estado y los Municipios de Yucatán, Decreto número 515, publicado en el Diario Oficial del Gobierno del Estado de Yucatán, el 31 de mayo de 2004, visible en http://www.archivogeneral.yucatan.gob.mx/MarcoNormativo/LEY_ACCESOINFO_YUC.pdf

Ley de Acceso a la Información Pública y Protección de Datos Personales para el Estado de Coahuila, publicada en el Periódico Oficial el martes 2 de septiembre de 2008, visible en http://200.57.142.114/archivos/filemanager/leyes//Leyes_Estatales_Vigentes/Ley_de_Acceso_a_la_Información_Pública_y_Protección_de_Datos_Personales_para_el_Estado_de_Coahuila.pdf

Ley de Información Pública del Estado de Jalisco y sus Municipios, Decreto número 23936/LIX/11, publicada en el Periódico Oficial el 22 de diciembre de 2011, Sección XXXIV, visible en http://portal.guadalajara.gob.mx/sites/default/files/LeyInformacionPublicaEstadoJaliscoMunicipios2012.pdf

Ley de Información Pública, Estadística y Protección de Datos Personales del Estado de Morelos, publicada en 27 de marzo de 2003, en el Periódico Oficial “Tierra y Libertad” en la Publicación Oficial 4274, visible en http://www.morelos.gob.mx/10consejeria/files/Leyes/Ley00100.pdf

Ley de Protección de Datos Personales del Estado de Campeche y sus Municipios, Decreto Núm. 231, publicado en el Periódico Oficial No. 5034 de fecha 9 de julio de 2012, visible en http://congresocam.gob.mx/LX/index.php?option=com_jdownloads&Itemid=0&task=finish&cid=2633&catid=4

Ley de Protección de Datos Personales del Estado de Colima, Decreto No. 356, publicado en el Suplemento No. 1 del Periódico Oficial “El Estado de Colima” No. 27, el sábado 21 de junio de 2003, disponible en la página del Congreso del Estado de Colima http://www.congresocol.gob.mx/legislacion.html

Ley de Protección de Datos Personales del Estado de Oaxaca, Decreto Nº 672, publicado en el Periódico Oficial Órgano del Gobierno Constitucional del Estado Libre y Soberano de Oaxaca, el 23 de Agosto de 2008, visible en http://www.congresooaxaca.gob.mx/lxi/legislacion/leyes/056.pdf

Ley de Protección de Datos Personales para el Distrito Federal, publicada en la Gaceta Oficial del Distrito Federal el 3 de octubre de 2008, disponible en la página de Internet de la Asamblea Legislativa http://www.aldf.gob.mx/leyes-107-2.html

Ley de Protección de Datos Personales para el Estado de Tlaxcala, Decreto Número 91, publicado en el Periódico Oficial del Gobierno del Estado en el Tomo XCI Segunda época, No. extraordinario el 14 de mayo de 2012, visible en http://www.caip-tlax.org.mx/pdf/LPDPTLAX.pdf

Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato, Decreto Número 266, publicado en el Periódico Oficial número 80, segunda parte del 19 de mayo de 2006, visible en http://transparencia.guanajuato.gob.mx/archivos/leydp.pdf

Ley de Transparencia y Acceso a la Información del Estado de Nuevo León, Decreto número 256, publicado en el Periódico Oficial No. 96, del sábado 19 de julio de 2008, visible en http://sg.nl.gob.mx/Transparencia_2009/Archivos/AC_0001_0002_0089416-0000001.pdf

Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, publicada en la Gaceta Oficial del Distrito Federal el 28 de marzo de 2008, disponible en la página de Internet de la Asamblea Legislativa http://www.aldf.gob.mx/leyes-107-2.html

Ley de Transparencia y Acceso a la Información Pública del Estado de Colima, Decreto No. 318, disponible en la página del Congreso del Estado de Colima http://www.congresocol.gob.mx/legislacion.html

Ley de Transparencia y Acceso a la Información Pública del Estado de Aguascalientes, Decreto número 169, publicado en el Periódico Oficial del Estado de Aguascalientes, el lunes 22 de mayo de 2006, visible en http://www.congresoags.gob.mx/lxilegislatura/legislacionestatal/074.%20LEY%20DE%20TRANSPARENCIA%20Y%20ACCESO%20A%20LA%20INFORMACION%20PUBLICA%20DEL%20ESTADO%20DE%20AGUASCALIENTES/LEY%20DE%20TRANSPARENCIA%20Y%20ACCESO%20A%20LA%20INFORMACION%20PUBLICA%20DEL%20ESTADO%20DE%20AGUASCALIENTES.pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Campeche, Decreto Núm. 162, publicado en el Periódico Oficial 3370, el 21 de julio de 2005, visible en http://congresocam.gob.mx/LX/index.php?option=com_jdownloads&Itemid=0&task=finish&cid=2493&catid=4

Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua, Decreto 278-05, publicado en el Periódico Oficial del Estado No. 83 del 15 de octubre de 2005, visible en http://www.congresochihuahua.gob.mx/biblioteca/leyes/archivosLeyes/115.pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Durango, Decreto 157, publicado en el Periódico Oficial No. 4, de fecha 13 de julio de 2008, visible en http://congresodurango.gob.mx/Leyes/transparencia.pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Michoacán de Ocampo, Decreto Número 29, publicado en el Periódico Oficial del Estado, el 7 de noviembre de 2008, Tomo CXLV, Núm. 14, visible en http://www.congresomich.gob.mx/Modulos/mod_Biblioteca/archivos/373_bib.pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Nayarit, publicada en la Sección Cuarta del Periódico Oficial del Estado de Nayarit, el sábado 22 de diciembre de 2007, visible en http://congresonay.gob.mx/Portals/1/Archivos/compilacion/leyes/Transparencia_y_Acceso_a_la_Informacion_Publica_del_Estado_de_Nayarit_%28Ley_de%29.pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Puebla, publicada en el Periódico Oficial el 31 de diciembre de 2011, disponible en la página de Internet del Congreso del Estado de Puebla en http://www.congresopuebla.gob.mx/index.php?option=com_docman&task=cat_view&gid=25&Itemid=111

Ley de Transparencia y Acceso a la Información Pública del Estado de Quintana Roo, del 13 de mayo de 2004, disponible en la página de Internet del Poder Legislativo del Estado de Quintana Roo en http://www.congresoqroo.gob.mx/

Ley de Transparencia y Acceso a la Información Pública del Estado de San Luis Potosí, Decreto 234, publicado en el Periódico Oficial, el jueves 18 octubre de 2007, visible en http://148.235.65.21/LIX/documentos/leyes/75_Ley_Transparencia.pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Tabasco, Decreto 229, publicado en el Suplemento “C” al Periódico Oficial 6723 de fecha 10 de febrero de 2007, visible en http://www.congresotabasco.gob.mx/60legislatura/trabajo_legislativo/pdfs/leyes/Ley%20de%20Transparencia%20y%20Acceso%20a%20la%20Informacion%20Publica%20del%20Edo%20de%20Tabasco..pdf

Ley de Transparencia y Acceso a la Información Pública del Estado de Tamaulipas, Decreto No. LIX-958, del 29 de junio de 2007, publicado en el Periódico Oficial No. 81 del 5 de julio de 2007, visible en http://www.congresotamaulipas.gob.mx/Legislacion/archivolegislacion.asp?idasunto=94

Ley de Transparencia y Acceso a la Información Pública del Estado de Zacatecas, Decreto número 149, publicado en el Periódico Oficial, Órgano del Gobierno del Estado de Zacatecas, el 29 de junio de 2011, Tomo CXXI, Periódico 52, disponible en la página de Internet del Poder Legislativo del Estado de Zacatecas en http://www.congresozac.gob.mx/cgi-bin/coz2/mods/secciones/index.cgi?action=todojuridico&cual=162

Ley de Transparencia y Acceso a la Información Pública del Estado de México y Municipios, publicada en el Periódico Oficial “Gaceta del Gobierno del Estado de México”, el 30 de abril de 2004, visible en http://www.infosap.gob.mx/leyes_y_codigos.html

Ley de Transparencia y Acceso a la Información Pública Gubernamental para el Estado de Hidalgo, Decreto Núm. 217, publicado en el Periódico Oficial, el viernes 29 de diciembre de 2006, disponible en la página de Internet del Congreso del Estado de Hidalgo en http://www.congreso-hidalgo.gob.mx/index.php?Biblioteca-Legislativa

Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California Sur, Decreto 1838, publicado en el Boletín Oficial del Estado de Baja California Sur, el 12 de marzo de 2010, disponible en la página de Internet del H. Congreso del Estado de Baja California Sur en http://www.cbcs.gob.mx/index.php?option=com_content&view=article&id=1979&Itemid=154

Ley de Transparencia y Acceso a la Información Pública para el Estado de Oaxaca, Decreto Nº 221, publicado en el Periódico Oficial del Estado de Oaxaca el sábado 15 de marzo de 2008, visible http://www.congresooaxaca.gob.mx/lxi/legislacion/leyes/061.pdf

Ley de Transparencia y Acceso a la Información Pública para el Estado de Veracruz de Ignacio de la Llave, Ley Número 848, publicada en la Gaceta Oficial, Órgano del Gobierno del Estado de Veracruz de Ignacio de la Llave, el 27 de febrero de 2007, disponible en la página de Internet del H. Congreso del Estado de Veracruz en http://www.legisver.gob.mx/index.php?p=ley

Ley de Transparencia y Acceso a la Información Pública para el Estado de Baja California, publicada en el Periódico Oficial No. 36, de fecha 12 de Agosto de 2005, Tomo CXII, visible en http://www.congresobc.gob.mx/contenido2/Transparencia2/img/LeyAccesoInformacionPublica.pdf

Ley Estatal de Acceso a la Información Gubernamental en el Estado de Querétaro, publicada en el Periódico Oficial del Estado de Querétaro “La Sombre de Arteaga”, el 27 de septiembre de 2002 (No. 44), visible en http://www.legislaturaqro.gob.mx/files/leyes/Ley%20Estatal%20de%20Acceso%20a%20la%20Informacion%20Gubernamentalen%20el%20Estado%20de%20Queretaro.pdf

Ley Número 374 de Transparencia y Acceso a la Información Pública del Estado de Guerrero, publicada en el Periódico Oficial No. 48, de fecha martes 15 de junio de 2010, visible en http://guerrero.gob.mx/wp-content/uploads/leyesyreglamentos/1036/L374TAIPEG.pdf

Ley que Garantiza la Transparencia y el Derecho a la Información Pública del Estado de Chiapas, Decreto Número 412, publicado en el Tomo II del Periódico Oficial No. 388, el jueves 12 de octubre de 2006, visible en http://www.consejeriajuridica.chiapas.gob.mx/marcojuridico/ley/default/Ley%20que%20Garantiza%20la%20Transparencia%20y%20el%20Derecho%20a%20la%20Informacion%20publica%20Edo%20Chis%2016nov2011.pdf

Ley Reguladora de la Base de Datos Genéticos para el Estado de Chihuahua, Decreto No. 583/09 IV P.E., publicado en el Periódico Oficial del Estado No. 26 del 01 de abril de 2009, visible en http://www.congresochihuahua.gob.mx/biblioteca/leyes/archivosLeyes/179.pdf

Otros instrumentos internacionales

Declaración Americana de los derechos y deberes del hombre, adoptada en la IX Conferencia Internacional Americana, Bogotá, Colombia, el 2 de mayo de 1948, disponible en http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/INST%2004.pdf

Declaración Universal de los Derechos Humanos, adoptada y proclamada por la Asamblea General de la ONU en su Resolución 217 A (III) del 10 de diciembre de 1948, disponible en http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/INST%2000.pdf

Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad, adoptada por la Asamblea General de la ONU, en su Resolución 3384 (XXX) del 10 de noviembre de 1975, disponible en http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/INST%2024.pdf

Directrices de la OCDE que regulan la protección de la privacidad y el flujo transfronterizo de datos personales del 23 de septiembre de 1980, NIPO: 326-04-034-7, Catálogo general de publicaciones oficiales, para la edición en español, Copyright 2004, *Organisation for Economic Co-operation and Development* (OECD), París y Ministerio de Administraciones Públicas, Secretaría General Técnica, España, publicada con la autorización de la OCDE, disponible en la página del Portal de Administración Electrónica del Gobierno de España, con derechos 2004, en http://administracionelectronica.gob.es/recursos/pae_000001422.pdf

Principios rectores para la reglamentación de los ficheros computarizados de datos, adoptados por la Asamblea General de la ONU, en su Resolución 45/95 del 14 de diciembre de 1990, que establece siete, en la 68a. sesión plenaria de la Asamblea General de la ONU, disponible en http://www.ordenjuridico.gob.mx/TratInt/Derechos%20 Humanos/OTROS%2015.pdf

Repertorio de recomendaciones prácticas sobre la protección de los datos personales de los trabajadores, emitido por la OIT, en su Reunión de Expertos sobre la vida privada de los trabajadores, realizada en Ginebra el 7 de octubre de 1996, Copyright Organización Internacional del Trabajo 1997, ISBN 92-2-310329-0, Ginebra, Oficina Internacional del Trabajo, 1997, disponible en http://www.avpd.euskadi.net/s04-5249/es/contenidos/inform acion/documentos_otros/es_docum/adjuntos/OIT_recomendaciones.pdf

Recomendación del Consejo de la OCDE relativa a las directrices sobre política criptográfica del 27 de marzo de 1997, traducción no oficial en español por el Ministerio de Política Territorial y Administración Pública del Gobierno de España, disponible en el Portal de Administración Electrónica del Gobierno de España http://administracionelectronica.gob. es/recursos/pae_000005909.pdf

Declaración Universal sobre el genoma humano y los derechos humanos, adoptada por la UNESCO, el 11 de noviembre de 1997, disponible en http://www.ordenjuridico.gob.mx/ TratInt/Derechos%20Humanos/INST%2031.pdf

Declaración sobre la protección de la privacidad de las redes globales, adoptada en la Conferencia Ministerial de la OCDE, denominada “Un mundo sin fronteras: comprender el potencial del comercio electrónico global”, celebrada del 7 al 9 de octubre de 1998 en Ottawa, Canadá, DSTI/ICCP/REG(98)10/FINAL, disponible en español en la página de Internet de la Agencia Española de Protección de Datos Personales, con Derechos de reproducción OCDE, 1998 en http://www.agpd.es/portalwebAGPD/canaldocumentacion/

legislacion/organismos_internacionales/ocde/common/pdfs/C.10-cp--Declaraci-oo-n-ministerial-Ottawa.pdf

Recomendación del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico, aprobada el 9 de diciembre de 1999, traducción realizada en México por la entonces Secretaría de Comercio y Fomento Industrial y la Procuraduría Federal del Consumidor, disponible en http://www.oecd.org/sti/consumerpolicy/34023784.pdf

Marco de Privacidad del APEC, adoptado en 2004 por los Ministros de las economías APEC, documento traducido y reproducido con permiso de la Secretaría de APEC. Traducido del inglés, el idioma original del documento, por la Secretaría de Economía del Gobierno de México. Información tomada de "APEC Privacy Framework" ISBN981-05-4471-5, APEC#205-SO-01.2. Número de publicación de APEC asignado a la traducción: APEC#206-TC-06.2, 2005 Secretariado de APEC, disponible en la página del Observatorio “Ciro Angarita Barón”, Sobre la protección de datos personales en Colombia”, el cual forma parte de la Red Académica Internacional habeasdata.org en http://habeasdatacolombia.uniandes.edu.co/?page_id=11

Legislación de otros países

Legislación de América Latina

Constitución de Argentina, disponible en http://www3.hcdn.gov.ar/folio-cgi-bin/om_isapi.dll?clientID=1185577405&advquery=habeas&hitsperheading=on&infobase=constra.nfo&record={7FF67B87}&softpage=Doc_Frame_Pg42&x=15&y=19&zz=

Constitución de Brasil, disponible en http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm

Constitución de Chile, disponible en http://www.leychile.cl/Navegar?idNorma=242302

Constitución de Colombia, disponible en http://wsp.presidencia.gov.co/Normativa/Documents/ConstitucionPoliticaColombia_20100810.pdf

Constitución de Costa Rica, disponible en http://www.pgr.go.cr/SCIJ/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=871&nValor3=74424&strTipM=TC

Constitución de Ecuador, disponible en http://www.asambleanacional.gov.ec/documentos/Constitucion-2008.pdf

Constitución de El Salvador, disponible en http://www.asamblea.gob.sv/eparlamento/indice-legislativo/buscador-de-documentos-legislativos/constitucion-de-la-republica

Constitución de Guatemala, disponible en http://www.congreso.gob.gt/manager/images/1188FE6B-B453-3B8C-0D00-549DA12F72CB.pdf

Constitución de Nicaragua, disponible en http://www.bcn.gob.ni/banco/legislacion/constitucion.pdf

Constitución de Panamá, disponible en http://www.asamblea.gob.pa/asamblea/constitucion/index.htm

Constitución de Paraguay, disponible en http://pdba.georgetown.edu/constitutions/paraguay/para1992.html

Constitución de Perú, disponible en http://www2.congreso.gob.pe/sicr/relatagenda/constitucion.nsf/constitucion/439F1D9B3CEB1E805256729006BC62C?opendocument

Constitución de Venezuela, disponible en la página de la Red Iberoamericana de Datos Personales en http://pdba.georgetown.edu/constitutions/venezuela/ven1999.html

Constitución del Estado de Bolivia, disponible en http://www.diputados.bo/images/docs/cpe.pdf

Ley 25.326, Ley de Protección de los Datos Personales de Argentina, disponible en http://www1.hcdn.gov.ar/BO/boletin00/2000-11/BO02-11-00leg.pdf y su Reglamento emitido por Decreto 1558, disponible en http://www1.hcdn.gov.ar/BO/boletin01/2001-12/BO03-12-01leg.pdf

Ley de Acceso a la Información Pública de Guatemala, disponible en http://200.12.63.122/archivos/decretos/2008/gtdcx57-0008.pdf

Ley de Control Constitucional de Ecuador, disponible en http://docs.ecuador.justia.com/nacionales/leyes/ley-de-control-constitucional.pdf

Ley de Protección de Datos Personales de Nicaragua, disponible en http://www.asamblea.gob.ni/trabajo-legislativo/agenda-legislativa/ultimas-iniciativas-presentadas/ y http://legislacion.asamblea.gob.ni/normaweb.nsf/9e314815a08d4a6206257265005d21f9/e5d37e9b4827fc06062579ed0076ce1d?OpenDocument

Ley N° 19628 de Chile, disponible en http://www.leychile.cl/Navegar?idNorma=141599&buscar=19628

Ley N° 8968 de Costa Rica, disponible en http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC

Ley Nº 17.838 de Uruguay, disponible en http://www0.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17838&Anchor=

Ley Nº 6 de Panamá, que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones, disponible en http://www.presidencia.gob.pa/ley_n6_2002.pdf

Leyes números 1682 y 1969 de Paraguay, disponibles en la página de la red iberoamericana de datos personales en http://www.redipd.org/documentacion/legislacion/common/legislacion/paraguay/Ley_1682_de_2001.pdf y http://www.redipd.org/documentacion/legislacion/common/legislacion/paraguay/Ley_1969_de_2002.pdf

Reglamento General de la Ley Penitenciaria de El Salvador, disponible en http://www.ute.gob.sv/cpp/index.php?option=com_docman&Itemid=102&task=doc_download&gid=53

Legislación de Europa

Convenio del Consejo de Europa para la protección de los derechos humanos y libertades fundamentales del 4 de noviembre de 1950, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.31-cp--CONVENIO-EUROPEO-DERECHOS-HUMANOS.pdf

Convenio N° 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del 28 de enero de 1981, modificado el 15 de junio de 1999, disponible en https://www.agpd.es/portalwebAGPD/

canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

Convenio de Dublín relativo a la determinación del Estado responsable del examen de las solicitudes de asilo presentadas en los Estados miembros de las Comunidades Europeas, del 15 de junio de 1990, disponible http://www.acnur.org/biblioteca/pdf/1798.pdf?view=1

Convenio de Asturias de Bioética del Consejo de Europa, convenio para la protección de los Derechos Humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina, convenio sobre los Derechos Humanos y la Biomedicina, del 4 de abril de 1997, disponible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.33-cp--CONVENIO-SOBRE-BIO-EE-TICA-DE-OVIEDO.pdf

Modificación del Convenio N° 108 para la protección de las personas en relación con el tratamiento automatizado de sus datos personales del 15 de junio de 1999, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.30-cp--MODIFICACI-OO-N-CONVENIO-N-1o--108.pdf

Carta de los Derechos Fundamentales de la Unión Europea del 7 de diciembre de 2000, publicada en español en el Diario Oficial de las Comunidades Europeas, el 18 de diciembre de 2000, pp. C 364/1-21, disponible en http://www.europarl.europa.eu/charter/pdf/text_es.pdf

Protocolo adicional del Convenio N° 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos, del 8 de noviembre de 2001, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.29-cp--PROTOCOLO-ADICIONAL-CONVENIO-N-1o-108.pdf

Convenio del Consejo de Europa sobre la Ciberdelincuencia del 23 de noviembre de 2001, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Directiva 95/46/CE del 24 de octubre de 1995, para la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, publicada en español en el Diario Oficial de las Comunidades Europeas, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp--Directiva-95-46-CE.pdf

Directiva 97/66/CE del 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.5-cp--Directiva-97-66-CE-.pdf

Directiva 1999/93/CE del 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, publicada en español en el Diario Oficial de las Comunidades Europeas, el 19 de enero de 2000, pp. L 13/12-13/20, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.7-cp--Directiva-1999-93-sobre-firma-electr-oo-nica.pdf

Directiva 2000/31/CE del 8 de junio de 2000, relacionada a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), publicada en español en el Diario Oficial de las Comunidades Europeas, el 17 de julio de 2000, pp. L 178/1-178-16, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.8-cp--Directiva-2000-31-CE---Comercio-Electr-oo-nico.pdf

Directiva 2002/19/CE del 7 de marzo de 2002, concerniente al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a si interconexión (Directiva acceso), publicada en español en el Diario Oficial de las Comunidades Europeas, el 24 de abril de 2002, pp. L 108/7-108/20, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/Directiva-2002-19.pdf

Directiva 2002/20/CE del 7 de marzo de 2002, referente a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización), publicada en español en el Diario Oficial de las Comunidades Europeas, el 24 de abril de 2002, pp. L 108/21-108/32, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/Directiva-2002-20.pdf

Directiva 2002/21/CE del 7 de marzo de 2002, hacia un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), publicada en español en el Diario Oficial de las Comunidades Europeas, el 24 de abril de 2002, pp. L 108/33-108/50, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/Directiva-2002-21.pdf

Directiva 2002/22/CE del 7 de marzo de 2002, del servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal). Modificada por la Directiva 2009/136/CE del 25 de noviembre de 2009, publicada en español en el Diario Oficial de las Comunidades Europeas, el 24 de abril de 2002, pp. L 108/51-108/77, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.9-cp--Directiva-2002-22--ap-servicio-universal-cp-.pdf

Directiva 2002/58/CE del 12 de julio de 2002, referente al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Modificada por las Directivas 2006/24/CE del 15 de marzo de 2006 y 2009/136/CE del 25 de noviembre de 2009, publicada en español en el Diario Oficial de las Comunidades Europeas, el 31 de julio de 2002, pp. L 201/37-201/47, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.6-cp--Directiva-2002-58-CE-protecci-oo-n-e-intimidad-en-comunicaciones-electronicas.pdf

Directiva 2004/82/CE del 29 de abril de 2004, sobre la obligación de los transportistas de comunicar los datos de las personas transportadas, publicada en español en el Diario Oficial de las Comunidades Europeas, el 6 de agosto de 2004, pp. L 261/24-261/27, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/Directiva-2004-82.pdf

Directiva 2006/24/CE del 15 de marzo de 2006 para la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de

acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, publicada en español en el Diario Oficial de las Comunidades Europeas, el 13 de abril de 2006, pp. L 105/54-105/63, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/DIRECTIVA-24-de-15-marzo-2006.pdf

Estándares Internacionales sobre Protección de Datos Personales y Privacidad, adoptados en la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009, en Madrid, España, disponible en http://www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/common/Estandares_Nota_Presentacion.pdf

Normas de desarrollo, adoptadas por decisión del Consejo de Europa el 13 de septiembre de 2004, del Reglamento N° 45/2001 del Parlamento Europeo y del Consejo de Europa, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, publicado en el Diario Oficial de las Comunidades Europeas el 21 de septiembre de 2004, pp. L 296/16-296/, disponible en https://www.agpd.es/portalwebAGPD/internacional/common/Decisin_prote_dat_en_las_Instits_europeas.pdf

Reglamento N° 2725/2000 del Consejo de Europa del 11 de diciembre de 2000, relativo a la creación del sistema “Eurodac” para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, publicado en el Diario Oficial de las Comunidades Europeas el 15 de diciembre de 2000, pp. L 316/1-316/10, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/B.19-cp--REGLAMENTO-EURODAC.pdf

Reglamento N° 45/2001 del Parlamento Europeo y del Consejo de Europa del 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, publicado en el Diario Oficial de las Comunidades Europeas el 12 de enero de 2001, pp. L 8/1-8/22, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/B.21-cp--REGLAMENTO-PROTECCI-OO-N-DATOS-EN-INSTITUCIONES-DE-LA-U.E..pdf

Reglamento N° 407/2002 del Consejo de Europa del 28 de febrero de 2002, por el que se establecen determinadas normas de desarrollo del Reglamento N° 2725/2000, relativo a la creación del sistema “Eurodac” para la comparación de las impresiones dactilares para la aplicación efectiva del Convenio de Dublín, publicado en el Diario Oficial de las Comunidades Europeas el 5 de marzo de 2002, pp. L 62/1-62/5, disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/B.20-cp--DESARROLLO-REGLAMENTO-EURODAC.pdf

Legislación de Estados Unidos y Canadá

Estados Unidos

The Freedom of Information Act, 5 U.S.C. § 552*, As Amended by Public Law* No. 110-175, 121 Stat. 2524, *and Public Law* No. 111-83, § 564, 123 Stat. 2142, 2184, de 1966, disponible en http://www.justice.gov/oip/amended-foia-redlined-2010.pdf

Privacy Act del 31 de diciembre de 1974, *5 U.S.C. § 552ª,* disponible en http://www.archives.gov/about/laws/privacy-act-1974.html

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, 115 Stat. 272-402, Public Law 107-56, Oct. 26, 2001, *Approved* Oct. 26, 2001, *Legislative History* – H.R. 3162, *Congressional Record,* Vol. 147 (2001), *Weekly Compilation of Presidential Documents,* Vol. 37 (2001), disponible en http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf

Canadá

Personal Information Protection and Electronic Documents Act, conocida como PIPED *Act*, emitida el 13 de abril de 2000, S.C. 2000, c. 5, *Current to September* 19, 2012, *Last amended on April* 1, 2011, *Published by the Minister of Justice*, disponible en http://laws-lois.justice.gc.ca/PDF/P-8.6.pdf

Jurisprudencia

Tesis aislada 1a. XXVI/2012, Décima Época, Primera Sala, Semanario Judicial de la Federación y su Gaceta, Libro V, Febrero de 2012, Tomo 1, página 659, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 200 0263.

Tesis aislada P. LXVIII/2011, Décima Época, Pleno, Semanario Judicial de la Federación y su Gaceta, Libro III, Diciembre de 2011, Tomo 1, página 551, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 160526.

Tesis aislada XI.1o.A.T.45 K, Novena Época, Primer Tribunal Colegiado en Materias Administrativa y de Trabajo del Décimo Primer Circuito, Semanario Judicial de la Federación y su Gaceta, Tomo XXXI, mayo de 2010, p. 2079, materia común, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 164509.

Tesis Jurisprudencial P./J.5/2010, Novena Época, Pleno de la Suprema Corte de Justicia de la Nación y publicada en el Semanario Judicial de la Federación y su Gaceta XXXI, febrero de 2010, p. 2322, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 165224.

Tesis aislada P. LXVII/2009, Novena Época, Instancia Pleno, Semanario Judicial de la Federación y su Gaceta XXX, Diciembre de 2009, p. 7, materias civil y constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 165821.

Tesis aislada 1a.CCXIV/2009, Novena Época, Instancia Primera Sala, Semanario Judicial de la Federación y su Gaceta XXX, Diciembre de 2009, p. 277, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 165823.

Tesis aislada 2a. XCIX/2008, Novena Época, Instancia Segunda Sala, Semanario Judicial de la Federación y su Gaceta XXVIII, Julio de 2008, p. 549, materia constitucional, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 169167.

Tesis aislada I.3º.C.79 K, Novena Época, Tercer Tribunal Colegiado en Materia Civil del Primer Circuito, Semanario Judicial de la Federación y su Gaceta, Tomo XXVI, julio de 2007, p. 2725, materia civil y común, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 171888.

Tesis aislada 1a.CXLIX/2007, Novena Época, Instancia Primera Sala, Semanario Judicial de la Federación y su Gaceta XXVI, Julio de 2007, p. 272, materia penal, Jurisprudencia y tesis aisladas IUS de la Suprema Corte de Justicia de la Nación, registro 171883.

Sitios de Internet

Agencia Española de Protección de Datos, http://www.agpd.es/portalwebAGPD/index-ides-idphp.php

Declaraciones y Convenciones que figuran en las Resoluciones de la Asamblea General de la Organización de las Naciones Unidas, http://www.un.org/spanish/documents/instruments/docs_subj_sp.asp?subj=45

Diario Oficial de la Federación, http://www.dof.gob.mx/

Diccionario de la Lengua Española, vigésima segunda edición, Real Academia Española, http://www.rae.es/rae.html.

Gaceta Parlamentaria de la Cámara de Diputados, http://gaceta.diputados.gob.mx/

Gaceta Parlamentaria de la Cámara de Senadores, http://www.senado.gob.mx/index.php?ver=sp&mn=2

Instituto Federal de Acceso a la Información y Protección de Datos, http://www.ifai.org.mx/

Jurisprudencias y Tesis Aisladas IUS de la Suprema Corte de Justicia de la Nación, http://ius.scjn.gob.mx/paginas/tesis.aspx

Leyes Federales de México de la página de Internet de la Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/index.htm

Leyes y Poderes Estatales de la página de Internet de la Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/gobiernos.htm

Orden Jurídico Nacional de la Secretaría de Gobernación, http://www.ordenjuridico.gob.mx/index.php

Organización de las Naciones Unidas (ONU), http://www.un.org/es/

Organización de los Estados Americanos (OEA), http://www.oas.org/es/

Organización para la Cooperación y Desarrollo Económicos (OCDE), http://www.oecd.org/mexico/

Protección Datos México, http://protecciondatos.mx/information/

Reformas a la Constitución de la página de Internet de la Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm

Reglamentos de Leyes Federales de la página de Internet de la Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/regla.htm

Sistema de Consulta de la Normativa del Consejo de la Judicatura Federal y su actualización, http://w3.cjf.gob.mx/sevie_page/normativa/Default.asp

Tratados Internacionales celebrados por México de la página de Internet de la Secretaría de Relaciones Exteriores, http://www.sre.gob.mx/tratados/

Tribunal Federal de Justicia Fiscal y Administrativa, http://www.tfjfa.gob.mx/

United States Holocaust Memorial Museum, Washington, D.C., http://www.ushmm.org/outreach/es/article.php?ModuleId=10007703.

Ponencias de cursos, seminarios o congresos

LUNA PLA, Issa, curso “Los Derechos de Acceso a la Información y Protección de Datos Personales”, realizado del 20 de octubre al 17 de noviembre de 2011, coordinado por la Dirección de Capacitación del Instituto Federal de Acceso a la Información y Protección de Datos, dirigido al personal de dicho Instituto.

MONCAYO GONZÁLEZ, Sergio A., *Protección de Datos Personales en México. Garantías Primarias y Secundarias / Avances Constitucionales,* ponencia presentada en el Seminario HabeasData2010, celebrado en Buenos Aires, Argentina el 26 y 27 de noviembre de 2010, formato pdf, disponible en http://www.habeasdata2010.com.ar/pdf/moncayo2.pdf, pp. 1-25.

PUENTE DE LA MORA, Ximena, “Protección de datos personales en posesión de los particulares en México: Avances y Desafíos”*,* ponencia presentada en la Mesa 10: Protección de Datos Personales del XIV Congreso Iberoamericano de Derecho e Informática, Universidad Autónoma de Nuevo León, Facultad de Derecho y Criminología T, Federación Iberoamericana de Asociaciones de Derecho e Informática, realizado del 25 al 30 de octubre de 2010, formato pdf, disponible en http://biblio.juridicas.unam.mx/libros/6/2941/26.pdf, pp. 911-925.