

Martes, 27 de Abril de 2010

No. Gaceta: 127

#### Dictámenes a Discusión

De las Comisiones Unidas de Gobernación; y de Estudios Legislativos, el que contiene proyecto de 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.

#### INTERVINIERON LOS SENADORES:

RICARDO MONREAL ÁVILA, PT.

SILVANO AUREOLES CONEJO, PRD.

JESÚS MURILLO KARAM, PRI.

ALEJANDRO ZAPATA PEROGORDO, PAN.

FUE APROBADO POR 85 VOTOS. SE TURNÓ AL EJECUTIVO FEDERAL.

Documento Aprobado

#### Sinopsis:

La Ley que se expide tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Establece que los responsables en el tratamiento de datos personales, deben observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Señala que tratándose de datos personales sensibles (aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual) el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento.

Se establece como obligación de los responsables en el tratamiento de datos personales, de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

Se dispone que el titular de datos o su representante legal podrán solicitar al responsable de datos personales, el acceso, rectificación, cancelación u oposición respecto de los datos personales que le conciernen.

Establece que el Instituto Federal de Acceso a la Información y Protección de Datos, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia.

#### Documentos Relacionados:

Cámara de Diputados

Oficio con el que remite Minuta:

Proyecto de 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. 2010-04-15

Dictámenes de Primera Lectura

De las Comisiones Unidas de Gobernación; y de Estudios Legislativos, el que contiene proyecto de 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. 2010-04-22

COMISIONES UNIDAS DE GOBERNACIÓN Y DE ESTUDIOS LEGISLATIVOS.

DICTAMEN DE LAS COMISIONES UNIDAS DE GOBERNACIÓN Y DE ESTUDIOS LEGISLATIVOS, A LA MINUTA CON PROYECTO DE 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.

HONORABLE ASAMBLEA:

A las Comisiones Unidas de Gobernación y de Estudios Legislativos de la LXI Legislatura de la Cámara de Senadores, les fue turnada para su estudio y dictamen, la MINUTA CON PROYECTO DE 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.

Con fundamento en lo dispuesto por los artículos 72 de la Constitución Política de los Estados Unidos Mexicanos; 39, apartados 1 y 2, fracción XXIX y 45 numeral 6, incisos e) y f) numeral 7 y demás relativos y aplicables de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; así como por lo dispuesto en los artículos 56, 60, 65, 87, 88, 93 y 94 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, y habiendo analizado el contenido de la Minuta de referencia, someten a la consideración de esta Honorable Asamblea, el presente dictamen al tenor de los siguientes:

## I. ANTECEDENTES

1. En sesión ordinaria celebrada en la Cámara de Diputados el día 6 de septiembre de 2001, el Diputado Federal Miguel Barbosa Huerta, integrante del Grupo Parlamentario del Partido de la Revolución Democrática, presentó la Iniciativa con Proyecto de Decreto que expide la Ley de Protección de Datos Personales.

En esa misma fecha, la Presidencia de la Mesa Directiva determinó que la iniciativa señalada en el numeral anterior, fuera turnada a la Comisión de Gobernación y de Seguridad Pública de la Cámara de Diputados para su estudio y dictamen.

2. Con fecha 12 de enero de 2005, el Diputado Federal Jesús Martínez Álvarez, del Grupo Parlamentario del Partido Convergencia, presentó la Iniciativa con Proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales.

En esa misma fecha, la Presidencia de la Mesa Directiva dispuso que la iniciativa citada en el numeral anterior, fuera turnada a la Comisión de Gobernación para su estudio y elaboración del dictamen correspondiente.

3. En sesión ordinaria celebrada en la Cámara de Diputados el día 23 de febrero de 2006, el Diputado Federal David Hernández Pérez, del Grupo Parlamentario del Partido Revolucionario Institucional, presentó la Iniciativa con Proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales.

En esa misma fecha, la Presidencia de la Mesa Directiva determinó que la iniciativa referida en el numeral anterior, fuera turnada a la Comisión de Gobernación para su estudio y dictamen.

4. En sesión ordinaria celebrada en la Cámara de Diputados el día 22 de marzo de 2006, la Diputada Federal Sheyla Fabiola Aragón Cortés, del Grupo Parlamentario del Partido Acción Nacional, presentó la Iniciativa con Proyecto de Decreto que expide la Ley Federal de Protección de Datos Personales.

En esa misma fecha, la Presidencia de la Mesa Directiva dispuso que la iniciativa señalada en el numeral anterior, fuera turnada a la Comisión de Gobernación para su estudio y elaboración del dictamen correspondiente.

5. En sesión ordinaria celebrada en la Cámara de Diputados el día 4 de noviembre de 2008, el Diputado Federal Luis Gustavo Parra Noriega, integrante del Grupo Parlamentario del Partido Acción Nacional, presentó Iniciativa con Proyecto de Decreto, por la que se expide la Ley de Protección de Datos Personales en Posesión de los Particulares.

En esa misma fecha, la Presidencia de la Mesa Directiva determinó que la iniciativa referida en el numeral anterior, fuera turnada a la Comisión de Gobernación de la Cámara de Diputados para su estudio y dictamen, y a la Comisión de Presupuesto y Cuenta Pública, para su opinión.

6. El 3 de marzo de 2009, la Comisión de Presupuesto y Cuenta Pública, emitió opinión del impacto presupuestario de la Iniciativa con Proyecto de Decreto que expide la Ley de Protección de Datos Personales en Posesión de los Particulares, considerando que la misma genera un impacto presupuestario en razón de que se propone la creación de un organismo descentralizado de la Administración Pública Federal llamado "Comisión Nacional de Protección de Datos Personales", en la que se contempla la creación de una estructura orgánica integrada por cuatro comisionados, un Comisionado Presidente, una secretaría ejecutiva, una Secretaría Técnica del pleno, una Secretaría de Acuerdos y el titular del órgano interno de control por lo que la Comisión mencionada, con base en la valoración realizada por el Centro de Estudios de las Finanzas Públicas de la Cámara de Diputados, concluye que la iniciativa presentada por el diputado Luis Gustavo Parra Noriega, sí implica un impacto presupuestario aproximado para el primer año de 261.8 millones de pesos.

7. Con fecha 11 de diciembre del año 2008, el Diputado Federal Adolfo Mota Hernández, integrante del Grupo Parlamentario del Partido Revolucionario Institucional, presentó Iniciativa con Proyecto de

Decreto, por la que se expide la Ley Federal de Protección de Datos Personales.

Esa misma fecha, la Presidencia de la Mesa Directiva dispuso que la iniciativa citada en el numeral anterior, fuera turnada a la Comisión de Gobernación de la Cámara de Diputados para su estudio y dictamen, y a la Comisión de Presupuesto y Cuenta Pública, para su opinión.

8.- En sesión celebrada en la Cámara de Diputados el día 13 de abril de 2010, fue aprobado el dictamen presentado por la Comisión de Gobernación; ordenándose remitir a esta Colegisladora el expediente con la Minuta correspondiente.

9. En sesión ordinaria del día 15 de abril de 2010, la Mesa Directiva de la H. Cámara de Senadores recibió la Minuta con Proyecto de 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; turnándola a las Comisiones Unidas de Gobernación y Estudios Legislativos para su estudio, análisis y elaboración del dictamen correspondiente.

10. Estas Comisiones Unidas se reunieron con el fin de analizar la Minuta de mérito y estar en condiciones de elaborar un proyecto de dictamen y discutirlo, mismo que en este acto se somete a consideración de esta Soberanía, en los términos que aquí se expresan.

## II. CONTENIDO DE LA MINUTA

PRIMERO. La Colegisladora plantea que el surgimiento del derecho fundamental a la protección de los datos personales, se genera como consecuencia de la natural evolución de la sociedad.

SEGUNDO. Señala que el siglo XXI comienza con un despliegue tecnológico trascendental. El avance en los campos tecnológico e informático ha generado una expansión que conlleva al intercambio de flujos de información constante, y parte de ella es la relativa a las personas. Ahora es posible, a través de distintos medios, acceder a la información de millones de seres humanos y sus actividades en cualquier parte del planeta. Sin embargo, frente al terreno ganado en materia de libertad de información y expresión, se ha irrumpido silenciosamente en el ámbito de lo privado, pues la sencilla obtención de cualquier tipo de dato sobre una persona física posibilita la generación de perfiles sobre ella y la afectación de la esfera de sus derechos y libertades.

Sin duda, señala la Colegisladora, los avances tecnológicos repercuten generalmente de forma positiva en la calidad de vida del ser humano. Sin embargo, sería ingenuo desconocer que también con ellos nacen nuevos conflictos e interrogantes a los que el Derecho debe dar respuesta.

TERCERO. En la Minuta se indica que diversos instrumentos internacionales han reconocido la importancia del derecho a la privacidad. Entre ellos destacan la Declaración Universal de los Derechos del Hombre, el Convenio para la Protección de los Derechos y las Libertades Fundamentales, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos.

CUARTO. Se menciona que los orígenes del derecho a la protección de los datos personales se encuentran en Europa. Asimismo, se apuntan tanto la serie de instrumentos normativos que han sido la base sobre la cual se ha sustentado la protección de los datos personales como las modificaciones que han sufrido sus contenidos con el propósito de garantizar una tutela efectiva del derecho referido.

QUINTO. Se señalan los esfuerzos continuos realizados por la Organización para la Cooperación y el Desarrollo Económico (OCDE) con el objetivo de generar directrices que sirvan como guía y referente

para proteger la privacidad y los flujos transfronterizos de datos.

El Foro de Cooperación Asia Pacífico (APEC) al igual que la OCDE ha trabajado en el renglón del derecho a la privacidad. Por ello, ha desarrollado los lineamientos generales en la materia con el fin de que los mismos sean contemplados y establecidos en los cuerpos legales correspondientes y con esto lograr un flujo de datos seguros y sin obstáculos.

SEXTO. Se expone que la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) fue publicada en el Diario Oficial de la Federación el día 11 de julio de 2002. Asimismo, se indica que la Ley citada tiene como propósito regular el derecho de acceso a la información.

Se apunta que los artículos 13, 14 y 18 de la LFTAIPG establecen los límites al derecho de acceso a la información. Además, el citado artículo 18 de la LFTAIPG establece que como información confidencial serán considerados los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos señalados en la misma. En adición a lo anterior, en el artículo 3, fracción II de la LFTAIPG se define el término “datos personales”.

Aunado a lo hasta ahora descrito, en el Capítulo IV de la Ley Federal de Transparencia y Acceso a la Información se establecen una serie de disposiciones dirigidas a garantizar el derecho a la protección de datos personales, tales como principios, derechos de los titulares de los datos, la existencia de un registro de protección de datos, así como las algunas reglas en torno a los procedimientos de acceso y corrección de datos personales.

SÉPTIMO. La Colegisladora hace mención de la reforma constitucional al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos publicada el 20 de julio de 2007 en el Diario Oficial de la Federación, con la cual se buscó homologar el derecho de acceso a la información pública gubernamental, en cualquier punto del territorio nacional y en los diversos órdenes de gobierno.

Hace referencia asimismo, al proceso de reforma a la Constitución Política de los Estados Unidos Mexicano llevado a cabo por el Constituyente Permanente de forma reciente, mediante el cual se reformaron los artículos 16 y 73, fracción XXIX-O; siendo publicadas dichas reformas en el Diario Oficial de la Federación los días 30 de abril de 2009 y 1 de junio de 2009, respectivamente.

Con la reforma al artículo 16 constitucional se reconoce en la Carta Magna el derecho a la protección de datos personales. En concordancia con lo anterior, y para dar contenido al derecho antes referido se plasmaron los derechos con los que cuentan los titulares de los datos personales, a saber, acceso, rectificación, cancelación y oposición (denominados derechos ARCO).

La reforma al artículo 73 constitucional estableció la competencia para que el Congreso de la Unión se constituya como la fuente normativa en materia de datos personales en posesión de particulares.

OCTAVO. El proyecto de Decreto aprobado por la Colegisladora tiene los siguientes aspectos relevantes:

\* El objeto de la Ley es la protección de datos personales en posesión de particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

\* Los sujetos obligados son todos los particulares que traten datos personales, excepto las sociedades de información crediticia, los usuarios de ésta y los particulares que usan los datos personales exclusivamente para su uso personal o doméstico.

\* Las disposiciones supletorias de esta Ley serán el Código Federal de Procedimientos Civiles y la Ley Federal del Procedimiento Administrativo.

\* Se proponen definiciones para conceptos y términos fundamentales para la comprensión y aplicación correcta de la presente Ley. Entre ellos se incluyen: el principio de licitud, el principio del consentimiento, el principio de calidad, el principio de finalidad, el principio de proporcionalidad, el principio de responsabilidad, el principio de información, el principio de lealtad, los datos personales sensibles y el derecho al olvido.

\* Se regula un procedimiento ante el responsable que sea sencillo, ágil y eficaz para que los particulares ejerzan los derechos de acceso, rectificación, cancelación y oposición.

\* Asimismo, se regula un procedimiento de protección de derechos ante el Instituto Federal de Acceso a la Información (IFAI), denominado “solicitud de protección de datos”. Mediante este procedimiento los titulares del derecho afectados en el ejercicio de sus derechos —de acceso, rectificación, cancelación y oposición— por parte del responsable del tratamiento de los datos, podrán acudir ante la autoridad a dirimir su controversia.

\* Se plantea que el actual Instituto Federal de Acceso a la Información sea el órgano garante del derecho a la protección de los datos personales. Para ello, se modificaría su actual denominación para ser Instituto Federal de Acceso a la Información y Protección de Datos.

\* Se señala la obligatoriedad para que la persona o entidad responsable así como los encargados y terceros que obtengan, utilicen, transmitan, almacenen y/o resguarden datos personales establezcan medidas de seguridad que impidan el acceso indebido a dicha información.

\* Finalmente, se establecen infracciones y sanciones para desincentivar conductas contrarias al espíritu y contenido de la presente Ley.

## CONSIDERACIONES

Esta Comisiones dictaminadoras coinciden y comparten plenamente con la Colegisladora el espíritu, el sentido y los propósitos de la Minuta que se estudia y analiza. En ese sentido, estima procedente la aprobación de la misma en los términos que a continuación se exponen:

PRIMERA. A partir de los años setenta, los descubrimientos y avances tecnológicos revolucionaron las condiciones y dinámica de la sociedad, incidiendo de manera directa en su calidad de vida. Este desarrollo perenne de nuevas tecnologías nos ofreció novedosas e impensables herramientas que hoy en día facilitan y coadyuvan a la culminación de nuestros objetivos y tareas cotidianas.

Tan es así, que actualmente gracias al desarrollo de las tecnologías de la información es posible acceder desde cualquier parte del mundo a una ventana ilimitada de información a través de un sencillo ritual, el cual consiste en contar con una computadora, conexión y conocimientos básicos o mínimos sobre navegación en la red de redes –Internet-.

Asimismo, las tecnologías de la información permiten almacenar un número ilimitado de datos personales de millones de individuos y utilizarlos para fines indistintos, los cuales pueden circular en cuestión de segundos entre personas, países, empresas privadas y redes abiertas.

De esta forma, Internet se ha constituido y afianzado como una fuente imprescindible e inagotable de conocimientos y un medio social más, que permite comunicar, entretener y compartir.

De esta manera, las múltiples aplicaciones y funcionalidades que ofrece la World Wide Web representan para los usuarios sitios de entretenimiento, ocio e interacción, donde éstos han pasado de ser “consumidores de contenidos” a consumidores que crean, publican, diseñan o modelan los propios contenidos.

Paralelamente a las bondades de Internet y en la dinámica de la sociedad en la que nos encontramos inmersos -donde los constantes avances científicos y de las tecnologías de la información evolucionan día con día para hacernos la vida más cómoda-, subyacen, a su vez, una serie de riesgos potenciales encaminados a lesionar los derechos y garantías fundamentales de los usuarios, específicamente los riesgos en materia de protección a la información personal que es accesada, almacenada, publicada y transmitida por medio de estas tecnologías.

En la era digital en la que vivimos, dejamos rastro de casi todo lo que hacemos o decimos sin ser conscientes de ello, y por tanto, de que ese rastro puede ser fácilmente seguido, hasta el punto de afirmarse que ninguna faceta de nuestras vidas podrá escaparse de la posibilidad de ser digitalizada.

Así, de una o de otra manera, conscientes o no, hemos sido objeto de algún tipo de violación o amenaza a nuestra información personal por el uso de estas tecnologías en momentos perfectamente determinados, simple y sencillamente por el rastro que dejan las mismas.

Miles de personas reciben a diario correos electrónicos no deseados en materia de publicidad de nuevos productos en el mercado, su imagen ha sido capturada por cámaras ilegalmente instaladas y en algunos países han adoptado el empleo de escáneres de cuerpo completo que hacen uso de ondas de radio milimétricas que rebotan en el cuerpo de los pasajeros, para proyectar una imagen desnuda en la que se puede observar la silueta completa y, por tanto, detectar cualquier cosa escondida bajo la ropa.

Adicionalmente, tanto los Estados como el sector privado para el desarrollo de sus actividades y tareas cotidianas, se han concentrado en conformar, actualizar e intercambiar grandes y valiosas bases de datos con un sinnúmero de información de ingentes cantidades de personas como puede ser aquella relativa a identificación, patrimonial, biométrica, laboral, de salud, entre otras.

En este mismo contexto, existen herramientas o aplicaciones informáticas que permiten la generación del “perfil” de cualquier persona a través de la obtención de cualquier tipo de dato sobre ella, posibilitando con ello una afectación en la esfera de sus derechos y libertades.

De ahí que si bien es cierto que los avances tecnológicos han incidido en el progreso y desarrollo de las sociedades, también lo es que el uso de estas nuevas tecnologías ha supuesto una verdadera irrupción en el ámbito de lo privado, vulnerando con ello la esfera de uno de los derechos fundamentales de los individuos: la privacidad.

Sobre este particular, conviene resaltar que el origen y fundamento de este derecho se encuentra precisamente, en el respeto a la privacidad y dignidad de las personas, colocando su protección y garantía en el marco de los llamados “derechos de tercera generación”, pues es una realidad que no hay democracia consolidada en el mundo que no se preocupe por garantizar la no injerencia arbitraria o ilegal en la esfera privada de las personas.

Este derecho se traduce en el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero -también denominado derecho a la autodeterminación informativa-.

Es decir, es el derecho que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaba y utiliza sus datos personales. Este nuevo derecho implica la libertad que tiene toda persona para elegir qué desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información.

Como bien señala el profesor Stefano Rodotà defensor del derecho a la protección de datos: “El cuadro de derechos fundamentales hoy es más rico y complejo porque ha sido integrado con la formalización de la protección de datos personales como derecho autónomo y fundamental, directamente conectado con la

dignidad y la libertad de la persona”.

Por esta razón, el manejo e intercambio de datos se han convertido en una práctica habitual de poder y control por parte de los sectores tanto público como privado. De ahí que el derecho a la intimidad ha tenido que ir re-direccionando su ámbito de protección, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, supone el reconocimiento de un derecho de control y acceso a su información, es decir, de toda aquella información relativa a su persona.

El legislador francés en la Asamblea Nacional al aprobar la Ley relativa a la informática, los ficheros y las libertades desde 1978, señaló con contundencia que la informática debe estar al servicio del hombre y no éste al servicio de aquélla.

En esa tesitura, es necesario tomar en cuenta que la creación y manejo de bases de datos si bien contribuyen al progreso económico y social; al desarrollo de los intercambios comerciales y científicos; así como al bienestar de los individuos, el Estado debe velar siempre por el respeto a las libertades y derechos fundamentales de las personas físicas. Lo anterior se logra en gran medida, protegiendo y regulando el uso de la información relativa o concerniente a toda persona física, es decir, al individuo, como sujeto de derechos.

En otras palabras, el hecho de que la tecnología posibilite conocer todo sobre una persona: dónde vive, en qué trabaja, su estado civil, número telefónico, correo electrónico, preferencias sexuales, estado de salud, trayectoria laboral, entre muchos otros ejemplos, no significa que también esté permitido utilizar la información para fines indistintos y mucho menos sin el conocimiento y consentimiento del titular de la misma.

De acuerdo con ensayos y publicaciones recientes, cada día dejamos un largo rastro de información personal: consultamos páginas de internet, enviamos correos electrónicos, hacemos compras con tarjeta de crédito, llamadas telefónicas desde nuestro celular y gracias al flujo de información, grandes compañías obtienen al mes un promedio de 2,500 detalles sobre cada uno de nosotros.

Gracias a algoritmos matemáticos y fórmulas aplicadas, dicha información se utiliza para predecir, con asombrosa exactitud, las decisiones que vamos a tomar. Es por ello importante establecer controles y límites al manejo indiscriminado de la información personal que generamos, ya que de lo contrario, nuestras conductas pueden ser manipuladas aún sin percatarnos de ello, coartando y vulnerando nuestras libertades.

Como se señala en el memorándum explicativo de la Directrices de la de la OCDE relativas a la Protección de la Intimidad y de la Circulación Transfronteriza de datos personales, de 1980, todavía vigentes [en la actual Sociedad de la Información]: “la protección de la intimidad y de las libertades individuales constituye quizás el aspecto de debate que está más extendido. Entre los motivos de tal interés están el uso ubicuo de ordenadores para el tratamiento de datos personales, las posibilidades vastamente extendidas de almacenamiento, contrastación, vinculación, selección y acceso a los datos personales, y la combinación de la informática con la tecnología de telecomunicaciones, que puede poner los datos personales simultáneamente a disposición de miles de usuarios en lugares geográficamente dispersos y que permite reunir datos y la creación de redes complejas de datos nacionales e internacionales”.

De esta manera, algunos de los riesgos al derecho fundamental de la protección de datos personales, son el almacenamiento ilícito de datos personales, exactos o inexactos; el abuso o la revelación no autorizada de los mismos; así como la creación de perfiles sin que el titular tenga conocimiento -y mucho menos control- de ello.

Riesgos más específicos son los casos denominados como “phising” y “pharming” fenómenos muy explotados por los ciberdelincuentes para lograr la obtención de datos personales de los usuarios de Internet, incluyendo datos de carácter sensible.

Otro fenómeno consiste en la indexación no autorizada por parte de buscadores de Internet de información personal de los usuarios de las redes sociales. Otro caso cada vez más frecuente, es la suplantación de identidad de usuarios que comprueban que al momento que intentan acceder a su “identidad digital”, esta ya está siendo utilizada.

Adicionalmente, son una realidad y una preocupación internacional algunos riesgos que enfrentan los menores y adolescentes al pertenecer, interactuar y participar en las redes sociales como el acceso a contenidos publicados de carácter inapropiado para su edad; la posibilidad de entablar contacto en línea, e incluso presencialmente, con usuarios malintencionados o la proliferación de información personal gráfica de los menores con desconocimiento y falta de conciencia de los riesgos asociados a tal hecho.

Otros riesgos asociados con estas tecnologías son la discriminación, difamación, violencia física o psicológica, acoso sexual y pornografía.

De ahí que frente a esta nueva realidad, el derecho no puede permanecer inmóvil. Los representantes de la sociedad estamos obligados a sensibilizarnos con los nuevos requerimientos sociales.

Así, para prevenir y abatir, en la medida de lo posible, los riesgos asociados al desarrollo de las tecnologías de la información y a fin de salvaguardar y respetar las libertades y derechos de los usuarios, los actores involucrados -estados, gobiernos, instituciones educativas, académicos, industria, sociedad civil organizada y sociedad en general- estamos obligados a adoptar y consensar medidas preventivas y proactivas en materia de prevención, educación, legislación y ética profesional, muestra de ellos es la ley que se dictamina como parte fundamental de este enorme reto que tenemos enfrente.

Lo anterior, suena sencillo pero es un desafío complejo que involucra el consenso de todos los actores involucrados, a fin de hacer efectivas todas las acciones tendentes a proteger la información personal tratada por medio de las cada vez más sofisticadas tecnologías de la información.

SEGUNDA. Como bien relata la Minuta sujeta a dictamen, existen diversos instrumentos internacionales que han reconocido la importancia del derecho a la privacidad. Entre ellos destacan la Declaración Universal de los Derechos del Hombre, el Convenio para la Protección de los Derechos y las Libertades Fundamentales, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos.

En efecto, por lo que se refiere al reconocimiento al derecho a la privacidad en el ámbito internacional, de la que el derecho a la protección de los datos personales es una expresión de la misma, han sido diversos los instrumentos internacionales que han reconocido su importancia.

Primeramente, el artículo 12 de la Declaración Universal de los Derechos del Hombre (10 de diciembre de 1948),<sup>8</sup> establece el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques.

El artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales (14 de noviembre de 1950),<sup>9</sup> reconoce el derecho de la persona al respeto de su vida privada y familiar de su domicilio y correspondencia.

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (16 de diciembre de 1966),<sup>10</sup> señala que 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.

En el mismo tenor, la Convención Americana sobre derechos humanos (22 de noviembre de 1969) en su artículo 11 apartado 2, establece que 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.

Sin embargo, y como lo refiere acertadamente la Colegisladora, los orígenes del derecho a la protección de los datos personales, en cuanto a derecho autónomo respecto de la privacidad y la intimidad, se ubican en Europa.

En 1967, el seno del Consejo de Europa, se creó una Comisión Consultiva para analizar las tecnologías de información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a la intimidad. Como fruto de la Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre los "derechos humanos y nuevos logros científicos y técnicos".

En 1977 fue aprobada la Ley de Protección de Datos de la República Federal Alemana. En Francia, en el año de 1978 fue publicada la Ley de Informática, Ficheros y Libertades, aún permanece vigente.

Posteriormente países como Dinamarca (1978); Austria, (1978); y Luxemburgo(1979) expidieron su legislación en la materia.

En la década de los 80's en el propio Consejo de Europa se dio un respaldo definitivo a la protección de la intimidad frente a la potencial agresividad de las tecnologías, siendo expedido en consecuencia el Convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal, el cual entró en vigor el 1 de octubre de 1985. Este Convenio fue creado con el propósito de garantizar a los ciudadanos de los estados contratantes, el respeto de sus derechos y libertades, en particular, el derecho a la vida privada frente a los tratamientos de datos personales, conciliando el respeto a ese derecho y la libre circulación de la información entre los estados. De esta forma, el Convenio 108 constituye el primer instrumento de carácter vinculante para los Estados en el que se plasman los principios de la protección de los datos de carácter personal.

Posteriormente, la Directiva 95/46/CE, sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, fue aprobada como lo refiere la Colegisladora con un doble objetivo: (i) garantizar el derecho a la vida privada reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos, en particular por lo que respecta al tratamiento de datos personales e (ii) impedir la restricción de la libre circulación de los datos personales en todos los estados miembros de la Unión Europea.

Asimismo, debe señalarse que la Carta de Derechos Fundamentales de la Unión Europea fue aprobada por la cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza el 7 de diciembre de 2000. Con su aprobación se reconocieron entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8, cuestión que se retoma en el Tratado de Lisboa del año 2007.

De esta forma, es dable señalar que a partir de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y como un derecho autónomo del derecho a la intimidad y a la privacidad de las personas.

TERCERA. México ha consolidado avances paulatinos, pero trascendentales y contundentes en nuestra legislación nacional, que van desde el año 2002 con la publicación de la Ley Federal de Transparencia y Acceso a la Información Gubernamental que reconoció por primera vez el derecho a la protección de datos en el ámbito público a nivel federal, hasta las recientes reformas constitucionales a los artículos 16 y 73 -que entraron en vigor en 2009- mismos que establecen respectivamente, el derecho fundamental a la protección de datos personales y lo dotan de contenido, así como la obligación del Congreso Federal de expedir una ley en la materia aplicable a los particulares.

Este alcance constitucional que adquirió el derecho de protección de datos, considerado de tercera generación, se desarrolló de la mano de los avances científicos y tecnológicos que permiten la utilización, conservación y transmisión de información personal para diversos fines, tanto por entes públicos como privados, quedando de manifiesto que los datos sólo pueden ser utilizados para fines explícitos y legítimos y por las personas autorizadas.

Con estas reformas, el Estado Mexicano dio un gran paso al reconocer el derecho a protección de datos personales como un derecho fundamental y autónomo, distinto al derecho a la intimidad ya que cuenta con caracteres propios que dotan al individuo del poder de disposición sobre la información que le concierne. Lo anterior contribuye sin duda a mejorar la dignidad humana al garantizar la no injerencia y uso indiscriminado y excesivo de los datos de las personas que circulan a diario por el avance de las tecnologías de la información.

Asimismo, estas reformas sentaron las bases para la expedición de una ley en la materia que regule el tratamiento de datos personales en el sector privado, demanda latente desde el año 2001.

Por otro lado, es importante señalar que al expedir una ley de protección de datos personales en posesión de los particulares, México se coloca entre las democracias consolidadas que ya cuentan con marcos normativos en la materia. Asimismo, existen diversos foros y organismos internacionales de los cuales México es integrante y en los cuales, desde hace décadas, se habían contraído compromisos en esta rubro. Este sistema internacional cuenta con instrumentos en materia de protección de datos personales, los cuales permiten el flujo transfronterizo de datos, garantizando la protección de los mismos a través del cumplimiento de un mínimo de reglas establecidas.

Tal es el caso de la Organización para la Cooperación y el Desarrollo Económico (OCDE); la Organización de las Naciones Unidas (ONU); el Foro de Cooperación Economía Asia Pacífico (APEC). Asimismo, tanto el Tratado de Libre Comercio de Norteamérica, como el Acuerdo de asociación económica, concertación política y cooperación entre la Comunidad Europea y sus Estados miembros, también denominado Tratado de Libre Comercio con la Unión Europea (TLCUE) prevén disposiciones sobre la protección de datos personales: en este último acuerdo México se compromete a contar con un nivel adecuado de protección.

Finalmente, es importante señalar que México es miembro de la Red Iberoamericana de Protección de Datos Personales en el seno de la cual se aprobaron las Directrices para la armonización de la protección de datos en la comunidad Iberoamericana, las cuales constituyen un modelo acerca de lo que debe contener una legislación en los estados miembros.

Así, hace más de 9 años que se discuten iniciativas de ley en materia de protección de datos personales con 8 iniciativas presentadas, en las que se iba del modelo garantista que entorpece el libre flujo de datos al requerir consentimiento expreso para todo tipo de tratamiento de datos (opt-in) al modelo liberalizado sin puntos mínimos regulatorios que den certeza al ciudadano.

En este sector, se tiene una regulación dispersa que efectivamente ya prevé algunos mecanismos de

protección de datos y medidas de confidencialidad para el tratamiento de datos de solvencia patrimonial y crédito y los registros -Registro Público de Consumidores y Registro Público de Usuarios para ejercer el derecho de oposición-, entre otras regulaciones.

Sin embargo, no se garantiza en todos los casos los derechos de acceso, rectificación, cancelación y oposición, así como la observancia de principios de protección de datos personales que den sustento a esta nueva garantía reconocida constitucionalmente.

CUARTA. La Minuta enviada por la Colegisladora tiene como objeto una doble vertiente. Por un lado, impone obligaciones a los sujetos que utilizan la información de las personas, de manera que sólo utilicen los datos personales para los fines para los cuales fueron recabados, observando medidas de seguridad que eviten su pérdida, robo o acceso no autorizado. Por el otro, el titular de los datos gozará del derecho de controlar la información que sobre él detente cualquier particular: tiendas departamentales, hospitales privados, universidades, aseguradoras o bancos, entre otros. Asimismo, los ciudadanos tendrán la posibilidad de acudir ante una autoridad independiente que les garantice pleno acceso a su información, la rectificación de sus datos en caso de estar incorrectos, pedir la eliminación o borrado de informaciones incorrectas o innecesarias, y exigir el respeto a su derecho a oponerse a la utilización de su información, a menos que se cuente con su consentimiento.

Se trata de fomentar el desarrollo de las tecnologías de la información con la conciencia de que las bases de datos y el tratamiento de las mismas están siempre al servicio del hombre y que, por lo tanto, deben respetarse las libertades y derechos fundamentales de las personas físicas y, en particular, la protección de sus datos personales y contribuir al progreso económico y social, al desarrollo de los intercambios, así como al bienestar de los individuos.

La minuta en análisis cumple con los requisitos indispensables para brindar una adecuada protección a las personas, con relación al uso que se da a su información en la era de las comunicaciones. Hasta ahora, sólo se encontraban protegidos los datos en posesión del gobierno en sus tres órdenes, pero esta nueva ley, completará el ciclo de protección, ampliando las obligaciones en esta materia, para todo ente privado que trate datos personales en sus actividades cotidianas.

A partir de esta ley, toda persona tendrá la facultad de decidir quién, cómo y para qué usa su información personal, al ser el consentimiento el eje rector de este nuevo derecho ya que los datos si tienen un dueño: el propio individuo.

Así, el consentimiento se erige como el título esencial que justifique injerencias en nuestra privacidad. No es el único, ya que es posible prever supuestos en que incluso, sin consentimiento de la persona, se permita el uso legítimo de la información que le concierne.

Al respecto, comenta el Dr. Piñar Mañas que existen estudios empíricos que han demostrado que para el individuo ese control es capital: se ha constatado que quienes perciben que mantienen el control sobre el uso que se hace de sus datos tras haberlos facilitado a un tercero, sienten su privacidad menos invadida que quienes piensan que han perdido el control sobre ellos.

Continúa explicando, que de hecho la violación del derecho de una persona a controlar su esfera privada, sea ésta física o informativa, constituye el factor más importante para que sienta invadida su privacidad. No es para ello necesario que la información sea más o menos importante o sensible. Una persona puede hacer pública información que le afecte sin que por ello considere violada su privacidad. Pero si pierde el control sobre ella, si alguien se la apropia, entonces pensará que su intimidad ha sido violada, porque el hecho de facilitar o permitir el acceso en una o múltiples ocasiones a la propia información personal, no quiere decir que exista una renuncia del titular a su privacidad.

Dado que resulta indispensable abatir el la compra-venta de información que ha convertido a México en un paraíso de datos personales, esta Ley, -debe quedar claro-, no impedirá el libre flujo de datos, antes bien, este se dará bajo unas reglas claras y respetuosas dictadas por el propio titular de dicha información.

De esta forma, México cumplirá finalmente con los compromisos adquiridos por en foros regionales o internacionales en materia de protección de datos, los cuales nos obligaban ya desde el 1995 a regularizar esta materia, a efecto de observarlos.

Ahora bien, en materia económica, esta Ley que se dictamina hará a nuestro país más competitivo al alinearse con los países miembros de la OCDE, APEC y de la Unión Europea, al contar con un marco de disposiciones que prevén los principios en materia de protección de datos personales actualmente observados por los países miembros de dichos organismos.

Asimismo, se contará con un solo régimen de protección para todo el país, otorgando ventajas competitivas frente a otras naciones. De no expedirse la Ley, prevalecerían los regímenes estatales vigentes en Colima, Jalisco y Tlaxcala, lo cual podría evitar la inversión nacional y extranjera en dichas entidades federativas, al tiempo de considerarse por otros países como un régimen atomizado y regulado de manera diferenciada y, por tanto, difícil de administrar para grandes empresas.

En este mismo contexto, México sería el primer país que emita una ley que cumpla con los Estándares Internacionales en materia de privacidad aprobados en la Conferencia Mundial de Comisionados de privacidad y protección de datos de noviembre de 2009 celebrada en Madrid, España. Dichos estándares contaron con el consenso de la industria y la sociedad civil internacional.

Lo anterior, significa que el contar con una ley en esta materia permitirá flujos de inversión extranjera directa al brindar certeza jurídica en los intercambios comerciales transfronterizos, ya que evitaría la existencia de barreras encubiertas a dichos intercambios en nombre del derecho a la protección de datos consagrado actualmente por nuestra Constitución.

Lo anterior nos situará en la tendencia mundial de alcanzar niveles de integración que permitan la libre circulación de mercancías, personas, bienes y capitales, al tiempo que se protege la información de las personas, por lo que el derecho de referencia se erige en un instrumento fundamental para dicha integración.

Adicionalmente, una Ley de esta naturaleza posibilitará la generación de empleos y de fuentes de ingreso y la ampliación de la oferta de servicios como call centers o investigación médica.

Finalmente, en materia económica, esta Ley no impedirá u obstaculizará el intercambio comercial con nuestros principales socios comerciales, Estados Unidos y Canadá, al no imponer altos costos de transacción para su observancia, impidiendo la creación de barreras encubiertas al comercio.

QUINTA.- Ahora bien, en relación con el contenido de la Minuta que se dictamina, debe precisarse que ésta comprende sesenta y seis artículos divididos en diez capítulos.

En estricto sentido, representa un modelo híbrido que conjuga con un justo equilibrio los principios de protección de datos personales internacionalmente reconocidos, que permite el libre flujo de datos para el crecimiento económico, así como las garantías necesarias para el titular de los datos de que el tratamiento de su información se lleve a cabo de manera lícita e informada. Lo anterior en consonancia con las recomendaciones de la OCDE y otros bloques comerciales.

En particular, se constituye como un marco general de regulación que contempla aspectos mínimos para garantizar un tratamiento adecuado por parte de los particulares de los datos personales en cada una de sus fases, desde la obtención inicial de los mismos hasta la supresión u otra medida análoga.

Las excepciones a la aplicación de la ley son mínimas y justificadas, acotadas tan sólo a dos supuestos siendo las sociedades de información crediticia de acuerdo con la ley que las regula y los particulares que usan los datos personales exclusivamente para su uso personal, es decir, en el ámbito doméstico, sin que ello se traduzca en la prestación de bienes o servicios. Asimismo, cada sector puede prever mayores garantías en caso de requerirlo dentro de dicho marco.

Así, conviene resaltar los cuatro ejes rectores que desarrolla la ley que se analiza:

1. El desarrollo de los principios internacionalmente reconocidos en materia de protección de datos, a saber, de licitud, consentimiento, finalidad, proporcionalidad, calidad, información y responsabilidad.
2. El desarrollo de los derechos de los titulares de los datos de acceso, rectificación, cancelación y oposición (conocidos como derechos ARCO).
3. Los mecanismos para ejercer dichos derechos que se traducen en el procedimiento para exigir al responsable de los datos los derechos ARCO, así como el procedimiento de tutela de dichos derechos en caso de la negativa de los responsables, ante una autoridad independiente y especializada en la materia que es el Instituto Federal de Acceso a la Información Pública.
4. Un régimen de infracciones y sanciones que desaliente conductas inadecuadas con relación al tratamiento de la información.

Con relación a los principios internacionalmente reconocidos, es importante señalar que la garantía de la privacidad de la persona, se ha traducido habitualmente en una serie de principios básicos, de obligado respeto y cumplimiento, que pretenden garantizar al individuo un poder de decisión y control sobre la información que le concierne.

Es por eso, que nuestra Colegisladora puso especial atención en garantizar a plenitud, todos y cada uno de los principios recogidos en el documento denominado “Estándares Internacionales sobre protección de datos personales y privacidad” o comúnmente conocido como Resolución de Madrid, aprobada en noviembre de 2009, a través de una labor conjunta de los órganos garantes de protección de datos personales de cincuenta países, la participación de la industria a nivel mundial y la sociedad civil organizada.

En este sentido, conviene destacar que la Minuta que se analiza parte de la premisa que la causa legitimadora de todo tratamiento de información personal es el consentimiento del titular, el cual deberá caracterizarse por ser:

- \* Libre, lo que implica que debe ser obtenido sin la intervención de algún vicio del consentimiento en los términos regulados por el Código Civil Federal.
- \* Específico, es decir, referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento.
- \* Informado, que se traduce en que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades para las que el mismo se produce.
- \* Inequívoco, lo que implica que exista expresamente una acción u omisión que implique la existencia del consentimiento por parte del afectado.

Así, la Minuta, en materia del consentimiento prevé reglas básicas y contundentes encaminadas a que los titulares no pierdan ese poder de control sobre su información personal, y al mismo tiempo se garantice el libre flujo de estas como base de las actividades y transacciones del sector privado.

Ahora bien, en este punto y a fin de comprender los alcances de las excepciones al consentimiento previstas por la Minuta en sus artículos 10 y 37, se considera indispensable aclarar que éstas resultan aplicables a todo tipo de datos personales, incluidos los sensibles.

Sin embargo, estas Comisiones Unidas consideran necesario dejar sentados elementos de interpretación a la autoridad que brinden certeza a las personas respecto de las excepciones al consentimiento en el caso de datos sensibles. Por lo tanto, de la lectura a los principios de protección de datos de la Minuta se advierte que las excepciones al consentimiento, en el caso de datos sensibles, sólo resultarán procedentes si se cumple con los principios de protección que establece la Minuta y en particular, cuando se actualicen dos condiciones necesarias. Por un lado, que las finalidades de dicho tratamiento sean legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado, y por el otro, que se cumpla con el principio de proporcionalidad. De no darse estas condiciones, se dejaría abierta la posibilidad de que tan sólo por citar un ejemplo, para una relación laboral (relación jurídica de acuerdo con la fracción IV del artículo 10), un empleador pudiera solicitar el dato de preferencia sexual o ideología a un candidato, a efecto de condicionar la firma del contrato respectivo, sin necesidad de contar con su consentimiento. Lo anterior, conculcaría otros derechos o libertades de las personas.

Otro caso de excepción al consentimiento, sería que los prestadores de servicios de salud podrán proceder al tratamiento de datos de pacientes en virtud de la existencia de una ley que los habilita al efecto; o bien, cuando sean necesarios para la prestación del servicio que el titular está contratando. En estos casos, no sería necesario obtener el consentimiento expreso y por escrito de los titulares de los datos. Sin embargo, no debe olvidarse, que de actualizarse algún supuesto de excepción al consentimiento, de cualquier forma, los responsables del tratamiento estarán obligados a informar de manera clara las finalidades del mismo a través del aviso de privacidad; además de observar el resto de los principios y medidas de seguridad que la ley prevé. Por lo tanto, el hecho de que bajo ciertos supuestos establecidos en ley, no se requiera el consentimiento expreso y por escrito, no significa que los datos personales no estén sujetos a la protección de la ley.

Adicionalmente, cabe hacer mención que las operaciones bancarias se regulan apropiadamente, al quedar comprendidas dentro del supuesto contemplado en la fracciones I y IV del artículo 10 de la minuta. En ese sentido, se considera que la minuta permite el tratamiento de datos necesarios para llevar a cabo operaciones bancarias entre las instituciones financieras y sus clientes, al establecer que no será necesario el consentimiento de éstos cuando dichas operaciones estén previstas una Ley que resulte aplicable y cuando los datos sean necesarios para el perfeccionamiento de una relación jurídica. Cabe mencionar que de cualquier forma, los datos deberán utilizarse únicamente para la finalidad de llevar a cabo dichas operaciones bancarias.

Finalmente, vale la pena añadir que en materia del otorgamiento del consentimiento por parte de menores de edad o incapaces, éste deberá ser prestado por sus padres o tutores, o bien, por las reglas del derecho civil que resulten aplicables.

Y en este rubro, también es importante mencionar que el principio de información para el caso de menores, debe traducirse en un aviso de privacidad acorde con el lenguaje e idiosincrasia propia de este grupo vulnerable.

Por otra parte, los derechos de los titulares constituyen el complemento imprescindible de los principios,

en razón de que garantizan al individuo el poder de decisión y control sobre la información que le concierne, y en consecuencia su derecho a la privacidad en relación con el tratamiento de sus datos personales.

Asimismo, actúan como complemento del deber del responsable de velar por el efectivo cumplimiento de los principios de protección, permitiéndole conocer aquellos supuestos en los que el tratamiento pudiera no resultar ajustado a los mismos.

En la actualidad son universalmente reconocidos los derechos de los interesados a conocer los distintos extremos relacionados con el tratamiento de sus datos personales (derecho de acceso), a obtener la rectificación de los datos inexactos o desactualizados (derecho de rectificación), o a la supresión o eliminación total de una base de datos (derecho de cancelación) y a oponerse bajo determinadas circunstancias, al tratamiento de los datos para una determinada finalidad (derecho de oposición).

Por otro lado, la Minuta otorga una amplia protección a los llamados “datos sensibles”. No podemos soslayar que la exposición de datos relacionados con preferencias sexuales, origen étnico o racial, o estado de salud, constituyen grupos de carácter vulnerable que pueden ser utilizados o mal utilizados para discriminar, o bien excluir a una persona. De ahí que su debido tratamiento coloca al proyecto a la vanguardia de la protección de derechos de tercera generación y a nuestro país en su conjunto, a la altura de cualquier democracia moderna.

Asimismo, la Ley prevé mecanismos ágiles, expeditos y sencillos para ejercer los derechos ARCO ante los responsables de las bases de datos, y en caso de ser vulnerados o conculcados, el titular tiene la opción de solicitar la tutela ante el órgano garante, el Instituto Federal de Acceso a la Información Pública (IFAI).

Respecto a la designación del IFAI como la autoridad garante para la adecuada observancia de esta ley, estas Comisiones dictaminadoras consideramos que dicha determinación se convierte en pieza clave para la debida consecución de los fines de la misma plantea.

Lo anterior es así, por varias razones. En primer lugar, por la experiencia acumulada por el IFAI durante los 7 años en los que ha resuelto miles de quejas ciudadanas (recursos de revisión) en materia de protección de datos personales, atendiendo casos de acceso y corrección de datos, pero también al llevar a cabo verificaciones al cumplimiento de los principios de protección, recomendando medidas preventivas o correctivas a los responsables del tratamiento de datos.

En segundo lugar, porque se garantiza la unicidad de criterio de la autoridad en una doble vertiente, por un lado, para que la protección sea la misma para datos en poder del Estado, que para aquellos en poder de los particulares, y por otro lado, para que en aquellos casos de tensión de derechos entre acceso a la información pública y la protección de datos personales, sea el IFAI quien pondere el interés público preponderante impidiendo dar marcha atrás en materia de transparencia. Lo anterior, dado lo ocurrido en otros países, donde la interpretación de la autoridad en materia de protección de datos, en muchas ocasiones ha negado el derecho a conocer información relativa personal, directamente conectada con la rendición de cuentas y el uso de recursos públicos.

En ese sentido, México se suma a una tendencia reciente en Europa, de incluir en una misma autoridad ambas materias –acceso a la información y protección de datos- tal y como ocurre en Reino Unido, Suiza, Hungría y Eslovenia.

En tercer lugar, la coadyuvancia del IFAI con las autoridades reguladoras que prevé la minuta, garantizará que ninguna disposición administrativa sectorial rebase los principios de protección de datos

personales y no impidan o disminuyan el ejercicio de los derechos ARCO por parte de los titulares de los datos. Por su parte, el IFAI contará con atribuciones para emitir recomendaciones y criterios generales para el adecuado ejercicio del derecho de protección de datos personales.

En ese sentido, la minuta tiene la bondad de dotar de facultades al IFAI enfocadas a la vigilancia, supervisión, investigación, inspección y sanción de conductas indebidas, a fin de garantizar el debido cumplimiento y observancia de la ley que se dictamina. Cabe resaltar que en materia de verificaciones, éstas deberán realizarse en términos del artículo 16 constitucional, es decir, de manera fundada y motivada, por lo que el IFAI podrá solicitar únicamente aquella información y documentación que se relacione necesariamente con la materia y el objeto de dichas verificaciones.

Adicionalmente, el proyecto satisface los elementos básicos que garantizan la protección de los datos personales: contiene los principios, derechos, procedimientos (ante el responsable y ante la autoridad), definición de autoridades reguladora y garante; así como un catálogo de infracciones y de sanciones relacionadas con las mismas. Lo anterior, de conformidad con lo establecido por el artículo 16 de la CPEUM.

Otra de las bondades es que retoma los elementos del marco de privacidad de APEC que lo hacen muy flexible, dándole preeminencia a las decisiones del titular de la información y evitando imponer cargas excesivas e innecesarias de cumplimiento a los sujetos obligados, a saber:

- \* No se requiere un Registro de las bases de datos en posesión de los particulares, lo cual conllevaría un proceso burocrático que no añade bondades significativas a la protección de los datos de los titulares.
- \* No se prevé la obligación de solicitar al órgano garante la autorización de las transferencias internacionales que pretendan efectuarse por los sujetos regulados, sino mecanismos que garanticen que el destinatario de los datos se obliga a observar las mismas reglas de protección que el responsable originario (principio de responsabilidad).
- \* Garantiza la coherencia normativa en la materia de protección de datos al regular la coadyuvancia de las autoridades sectoriales con el IFAI, tal y como lo demandan los sujetos regulados (sector privado);
- \* Se logra el equilibrio entre la protección a la persona y el desarrollo de la tecnología y de los mercados, a través de facilitar un libre flujo de información transfronterizo, con las adecuadas garantías para la debida utilización del dato.
- \* Establece la posibilidad a los sujetos obligados de impugnar las resoluciones del órgano garante brindando un control de legalidad en la imposición de multas, al establecer la procedencia del Juicio de Nulidad ante el Tribunal Fiscal y de Justicia Administrativa.
- \* Aclara y añade definiciones importantes y tecnológicamente neutras, a saber: bloqueo, transferencia de datos, encargado y tercero, que permitirán el flujo de datos de manera regulada, pero permitiendo a la industria tratar los datos personales sin necesidad de solicitar cada vez el consentimiento del titular del dato.
- \* Prevé la existencia de mecanismos de autorregulación que faciliten la observancia de la ley dentro y fuera de las fronteras de nuestro país.

Lo anterior incluiría las reglas corporativas entre negocios de una misma familia para que los datos personales sean tratados bajo los mismos principios y estándares de seguridad. Así, se evita la necesidad de contar con el consentimiento del titular del dato para que sea tratado aún en otro país distinto a México, brindando ventajas competitivas a las empresas.

En materia de infracciones y sanciones, se prevé todo un catálogo de las mismas y otorga al IFAI la potestad sancionadora y condiciones indispensables para el adecuado cumplimiento de la ley.

Para la imposición de multas IFAI deberá ponderar, la naturaleza del dato; la notoria improcedencia o

negativa del responsable, para realizar los actos solicitados por el titular, en términos de esta ley; el carácter intencional o no, de la acción u omisión constitutiva de la infracción; la capacidad económica del responsable, y la reincidencia. Lo anterior garantiza que no se vean afectados sectores económicos como el de las MiPymes o Pymes.

Finalmente, se establece un régimen transitorio que permitirá que los sujetos obligados adecuen sus prácticas actuales y las autoridades emitan la regulación mínima indispensable para la correcta observancia del derecho.

Ahora bien, es importante señalar que la *vacatio legis* establecida por el artículo Tercero Transitorio que se refiere a la expedición de avisos de privacidad, incluye también la obtención del consentimiento expreso, ya que el último párrafo del artículo 16 de la minuta dispone que “en el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos”. Es decir, la *vacatio legis* aplica para los dos tipos de consentimiento tácito y expreso.

SEXTO.- Por último debe señalarse que no pasa desapercibido para estas Comisiones dictaminadoras la Iniciativa con proyecto de decreto por el que se expide la Ley de Protección de Datos Personales, presentada por el Senador José Guillermo Anaya Llamas, integrante del Grupo Parlamentario del Partido Acción Nacional, presentada el día 8 de diciembre de 2009 y turnada a la Comisión de Gobernación.

El Senador proponente menciona que uno de los aspectos más relevantes de los seres humanos es su vida íntima y personal. Destaca que el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos reconoce como una garantía individual el derecho a la protección de toda información que se refiera a la vida privada y los datos personales.

En ese sentido, señala que el avance tecnológico y las interpretaciones erróneas que puedan darse al derecho a la información, ha provocado que en múltiples ocasiones se vea vulnerado el derecho de las personas a su intimidad, debido a que la mayor parte de las actividades que se realizan en la vida cotidiana implican una relación con la información de su vida privada.

En la misma tesitura, destaca que la información recabada es almacenada en expedientes o archivos electrónicos que conforman bases de datos, las cuales muchas veces son transmitidas a otros que utilizan estos datos para extorsionar o estafar. Por ello, sostiene, es de vital importancia regular nuestro ordenamiento con la finalidad de que haya una eficaz protección a los datos personales.

Como consecuencia de ello, considera que la propuesta que presenta hace posible la garantía individual consagrada en el artículo 6º Constitucional, ya que se contarán con mecanismos jurídicos que regulen la protección de dicha información y del mismo modo, al ampliar la competencia del Instituto Federal de Acceso a la Información, permitirá que haya compatibilidad del derecho a la información con el derecho de las personas a su vida privada e íntima.

Ahora bien, de un análisis minucioso a esta iniciativa, estas Comisiones dictaminadoras consideran que la misma es afín a la Minuta que se dictamina en los aspectos torales, principalmente en lo referente al objeto de la ley, al ámbito de aplicación de la misma, la definición de “datos personales”, el tratamiento de los datos personales, los derechos de las personas en relación con sus datos personales, las atribuciones otorgadas al Instituto Federal de Acceso a la Información como órgano garante en esta materia, las sanciones e infracciones en caso de incumplimiento de lo establecido en dicha Ley, así como los medios con que contará el particular que considere violentados los derechos que en esta Ley se protegen.

Bajo las consideraciones que han sido expuestas, estas Comisiones estiman que es de aprobarse la

Minuta en estudio, para los efectos del inciso a) del artículo 72 de la Constitución Política de los Estados Unidos Mexicanos, en consecuencia, sometemos a la consideración del Pleno de esta H. Asamblea el siguiente:

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.

ARTÍCULO PRIMERO. Se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES

EN POSESIÓN DE LOS PARTICULARES

CAPÍTULO I

Disposiciones Generales

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

Artículo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Artículo 3.- Para los efectos de esta Ley, se entenderá por:

I. 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, de conformidad con el artículo 15 de la presente Ley.

II. Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.

III. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

IV. Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el

tratamiento de los mismos.

V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

VII. Días: Días hábiles.

VIII. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

IX. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

X. Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el Reglamento de esta Ley.

XI. Instituto: Instituto Federal de Acceso a la Información y Protección de Datos, a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

XII. Ley: Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

XIII. Reglamento: El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

XV. Secretaría: Secretaría de Economía.

XVI. Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

XVII. Titular: La persona física a quien corresponden los datos personales.

XVIII. Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

XIX. Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

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

Artículo 5.- A falta de disposición expresa en esta Ley, se aplicarán de manera supletoria las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo.

Para la substanciación de los procedimientos de protección de derechos, de verificación e imposición de sanciones se observarán las disposiciones contenidas en la Ley Federal de Procedimiento Administrativo.

## CAPÍTULO II

### De los Principios de Protección de Datos Personales

Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.

La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.

En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.

Artículo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.

El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

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

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

Artículo 10.- No será necesario el consentimiento para el tratamiento de los datos personales cuando:

I. Esté previsto en una Ley;

II. Los datos figuren en fuentes de acceso público;

III. Los datos personales se sometan a un procedimiento previo de disociación;

IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o

VII. Se dicte resolución de autoridad competente.

Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

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

Artículo 13.- El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable.

Artículo 14.- El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por esta Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. 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.

Artículo 15.- El responsable tendrá la obligación de informar a los titulares de los datos, la información

que se recaba de ellos y con qué fines, a través del aviso de privacidad.

Artículo 16.- El aviso de privacidad deberá contener, al menos, la siguiente información:

I. La identidad y domicilio del responsable que los recaba;

II. Las finalidades del tratamiento de datos;

III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;

IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;

V. En su caso, las transferencias de datos que se efectúen, y

VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Artículo 17.- El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y

II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Artículo 18.- Cuando los datos no hayan sido obtenidos directamente del titular, el responsable deberá darle a conocer el cambio en el aviso de privacidad.

No resulta aplicable lo establecido en el párrafo anterior, cuando el tratamiento sea con fines históricos, estadísticos o científicos.

Cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares, o a la antigüedad de los datos, previa autorización del Instituto, el responsable podrá instrumentar medidas compensatorias en términos del Reglamento de esta Ley.

Artículo 19.- Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo

de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

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

Artículo 21.- El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

### CAPÍTULO III

#### De los Derechos de los Titulares de Datos Personales

Artículo 22.- Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos.

Artículo 23.- 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.

Artículo 24.- El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos.

Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.

La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.

Una vez cancelado el dato se dará aviso a su titular.

Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también.

Artículo 26.- El responsable no estará obligado a cancelar los datos personales cuando:

I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;

II. Deban ser tratados por disposición legal;

III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;

IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;

V. Sean necesarios para realizar una acción en función del interés público;

VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y

VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Artículo 27.- 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.

#### CAPÍTULO IV

Del Ejercicio de los Derechos de Acceso, Rectificación,

Cancelación y Oposición

Artículo 28.- El titular o su representante legal podrán solicitar al responsable en cualquier momento el acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen.

Artículo 29.- La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:

I. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;

II. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;

III. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y

IV. Cualquier otro elemento o documento que facilite la localización de los datos personales.

Artículo 30.- Todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la presente Ley. Asimismo fomentará la protección de datos personales al interior de la organización.

Artículo 31.- En el caso de solicitudes de rectificación de datos personales, el titular deberá indicar, además de lo señalado en el artículo anterior de esta Ley, las modificaciones a realizarse y aportar la documentación que sustente su petición.

Artículo 32.- El responsable comunicará al titular, en un plazo máximo de veinte días, contados desde la fecha en que se recibió la solicitud de acceso, rectificación, cancelación u oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días siguientes a la fecha en que se comunica la respuesta. Tratándose de solicitudes de acceso a datos personales, procederá la entrega previa acreditación de la identidad del solicitante o representante legal, según corresponda.

Los plazos antes referidos podrán ser ampliados una sola vez por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Artículo 33.- La obligación de acceso a la información se dará por cumplida cuando se pongan a disposición del titular los datos personales; o bien, mediante la expedición de copias simples, documentos electrónicos o cualquier otro medio que determine el responsable en el aviso de privacidad.

En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y ésta resulta no serlo, bastará con que así se le indique al titular por cualquiera de los medios a que se refiere el párrafo anterior, para tener por cumplida la solicitud.

Artículo 34.- El responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al tratamiento de los mismos, en los siguientes supuestos:

I. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;

II. Cuando en su base de datos, no se encuentren los datos personales del solicitante;

III. Cuando se lesionen los derechos de un tercero;

IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y

V. Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular.

En todos los casos anteriores, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

Artículo 35.- La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos.

Dicho derecho se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.

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.

## CAPÍTULO V

### De la Transferencia de Datos

Artículo 36.- Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera,

el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Artículo 37.- Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:

- I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
- II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
- III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
- IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
- V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
- VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
- VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

## CAPÍTULO VI

### De las Autoridades

#### Sección I

##### Del Instituto

Artículo 38.- El Instituto, para efectos de esta Ley, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.

Artículo 39.- El Instituto tiene las siguientes atribuciones:

- I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;
- II. Interpretar en el ámbito administrativo la presente Ley;
- III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;

IV. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación;

V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;

VI. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda;

VII. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos;

VIII. Rendir al Congreso de la Unión un informe anual de sus actividades;

IX. Acudir a foros internacionales en el ámbito de la presente Ley;

X. 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;

XI. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados, y

XII. Las demás que le confieran esta Ley y demás ordenamientos aplicables.

## Sección II

### De las Autoridades Reguladoras

Artículo 40.- La presente Ley constituirá el marco normativo que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del Instituto.

Artículo 41.- La Secretaría, para efectos de esta Ley, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto.

Artículo 42.- En lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización.

Artículo 43.- La Secretaría tiene las siguientes atribuciones:

I. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial;

II. Fomentar las buenas prácticas comerciales en materia de protección de datos personales;

III. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en

coadyuvancia con el Instituto, a que se refiere la presente Ley;

IV. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, en coadyuvancia con el Instituto;

V. Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 de la presente Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto;

VI. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento;

VII. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales;

VIII. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales;

IX. Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial, y

X. Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.

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

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

## CAPÍTULO VII

### Del Procedimiento de Protección de Derechos

Artículo 45.- El procedimiento se iniciará a instancia del titular de los datos o de su representante legal, expresando con claridad el contenido de su reclamación y de los preceptos de esta Ley que se consideran vulnerados. La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable.

En el caso de que el titular de los datos no reciba respuesta por parte del responsable, la solicitud de protección de datos podrá ser presentada a partir de que haya vencido el plazo de respuesta previsto para el responsable. En este caso, bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud de acceso, rectificación, cancelación u oposición.

La solicitud de protección de datos también procederá en los mismos términos cuando el responsable no entregue al titular los datos personales solicitados; o lo haga en un formato incomprensible, se niegue a efectuar modificaciones o correcciones a los datos personales, el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponda a la información requerida.

Recibida la solicitud de protección de datos ante el Instituto, se dará traslado de la misma al responsable, para que, en el plazo de quince días, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga.

El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del responsable las demás pruebas que estime necesarias. Concluido el desahogo de la 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.

Para el debido desahogo del procedimiento, el Instituto resolverá sobre la solicitud de protección de datos formulada, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, como pueden serlo aquéllos que deriven de la o las audiencias que se celebren con las partes.

El Reglamento de la Ley establecerá la forma, términos y plazos conforme a los que se desarrollará el procedimiento de protección de derechos.

Artículo 46.- La solicitud de protección de datos podrá interponerse por escrito libre o a través de los formatos, del sistema electrónico que al efecto proporcione el Instituto y deberá contener la siguiente información:

- I. El nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay;
- II. El nombre del responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales;
- III. El domicilio para oír y recibir notificaciones;
- IV. La fecha en que se le dio a conocer la respuesta del responsable, salvo que el procedimiento inicie con base en lo previsto en el artículo 50;
- V. Los actos que motivan su solicitud de protección de datos, y
- VI. Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

La forma y términos en que deba acreditarse la identidad del titular o bien, la representación legal se establecerán en el Reglamento.

Asimismo, a la solicitud de protección de datos deberá acompañarse la solicitud y la respuesta que se recurre o, en su caso, los datos que permitan su identificación. En el caso de falta de respuesta sólo será necesario presentar la solicitud.

En el caso de que la solicitud de protección de datos se interponga a través de medios que no sean electrónicos, deberá acompañarse de las copias de traslado suficientes.

Artículo 47.- El plazo máximo para dictar la resolución en el procedimiento de protección de derechos será de cincuenta días, contados a partir de la fecha de presentación de la solicitud de protección de datos. Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo.

Artículo 48.- En caso que la resolución de protección de derechos resulte favorable al titular de los datos, se requerirá al responsable para que, en el plazo de diez días siguientes a la notificación o cuando así se justifique, uno mayor que fije la propia resolución, haga efectivo el ejercicio de los derechos objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento al Instituto dentro de los siguientes diez días.

Artículo 49.- En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el artículo 46 de esta Ley, y el Instituto no cuente con elementos para subsanarlo, se prevendrá al titular de los datos dentro de los veinte días hábiles siguientes a la presentación de la solicitud de protección de datos, por una sola ocasión, para que subsane las omisiones dentro de un plazo de cinco días. Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de protección de datos. La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver la solicitud de protección de datos.

Artículo 50.- El Instituto suplirá las deficiencias de la queja en los casos que así se requiera, siempre y cuando no altere el contenido original de la solicitud de acceso, rectificación, cancelación u oposición de datos personales, ni se modifiquen los hechos o peticiones expuestos en la misma o en la solicitud de protección de datos.

Artículo 51.- Las resoluciones del Instituto podrán:

- I. Sobreseer o desechar la solicitud de protección de datos por improcedente, o
- II. Confirmar, revocar o modificar la respuesta del responsable.

Artículo 52.- La solicitud de protección de datos será desecheda por improcedente cuando:

- I. El Instituto no sea competente;
- II. El Instituto haya conocido anteriormente de la solicitud de protección de datos contra el mismo acto y resuelto en definitiva respecto del mismo recurrente;
- III. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el titular que pueda tener por efecto modificar o revocar el acto respectivo;
- IV. Se trate de una solicitud de protección de datos ofensiva o irracional, o
- V. Sea extemporánea.

Artículo 53.- La solicitud de protección de datos será sobreseída cuando:

- I. El titular fallezca;
- II. El titular se desista de manera expresa;

III. Admitida la solicitud de protección de datos, sobrevenga una causal de improcedencia, y

IV. Por cualquier motivo quede sin materia la misma.

Artículo 54.- El Instituto podrá en cualquier momento del procedimiento buscar una conciliación entre el titular de los datos y el responsable.

De llegarse a un acuerdo de conciliación entre ambos, éste se hará constar por escrito y tendrá efectos vinculantes. La solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

Para efectos de la conciliación a que se alude en el presente ordenamiento, se estará al procedimiento que se establezca en el Reglamento de esta Ley.

Artículo 55.- Interpuesta la solicitud de protección de datos ante la falta de respuesta a una solicitud en ejercicio de los derechos de acceso, rectificación, cancelación u oposición por parte del responsable, el Instituto dará vista al citado responsable para que, en un plazo no mayor a diez días, acredite haber respondido en tiempo y forma la solicitud, o bien dé respuesta a la misma. En caso de que la respuesta atienda a lo solicitado, la solicitud de protección de datos se considerará improcedente y el Instituto deberá sobreseerlo.

En el segundo caso, el Instituto emitirá su resolución con base en el contenido de la solicitud original y la respuesta del responsable que alude el párrafo anterior.

Si la resolución del Instituto a que se refiere el párrafo anterior determina la procedencia de la solicitud, el responsable procederá a su cumplimiento, sin costo alguno para el titular, debiendo cubrir el responsable todos los costos generados por la reproducción correspondiente.

Artículo 56.- Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

Artículo 57.- Todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo identifiquen o lo hagan identificable.

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

## CAPÍTULO VIII

### Del Procedimiento de Verificación

Artículo 59.- El Instituto verificará el cumplimiento de la presente Ley y de la normatividad que de ésta derive. La verificación podrá iniciarse de oficio o a petición de parte.

La verificación de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos a que se refiere el Capítulo anterior o se presuma fundada y motivadamente la existencia de violaciones a la presente Ley.

Artículo 60.- En el procedimiento de verificación el Instituto tendrá acceso a la información y documentación que considere necesarias, de acuerdo a la resolución que lo motive.

Los servidores públicos federales estarán obligados a guardar confidencialidad sobre la información que conozcan derivada de la verificación correspondiente.

El Reglamento desarrollará la forma, términos y plazos en que se sustanciará el procedimiento a que se refiere el presente artículo.

## CAPÍTULO IX

### Del Procedimiento de Imposición de Sanciones

Artículo 61.- Si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, éste tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, iniciará el procedimiento a que se refiere este Capítulo, a efecto de determinar la sanción que corresponda.

Artículo 62.- El procedimiento de imposición de sanciones dará comienzo con la notificación que efectúe el Instituto al presunto infractor, sobre los hechos que motivaron el inicio del procedimiento y le otorgará un término de quince días para que rinda pruebas y manifieste por escrito lo que a su derecho convenga. En caso de no rendirlas, el Instituto resolverá conforme a los elementos de convicción de que disponga.

El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Asimismo, podrá solicitar del presunto infractor las demás pruebas que estime necesarias. Concluido el desahogo de las pruebas, el Instituto notificará al presunto infractor el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación.

El Instituto, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, resolverá en definitiva dentro de los cincuenta días siguientes a la fecha en que inició el procedimiento sancionador. Dicha resolución deberá ser notificada a las partes.

Cuando haya causa justificada, el Pleno del Instituto podrá ampliar por una vez y hasta por un período igual este plazo.

El Reglamento desarrollará la forma, términos y plazos en que se sustanciará el procedimiento de imposición de sanciones, incluyendo presentación de pruebas y alegatos, la celebración de audiencias y el cierre de instrucción.

## CAPÍTULO X

### De las Infracciones y Sanciones

Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:

I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;

II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación,

cancelación u oposición de datos personales;

III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;

X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;

XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;

XIV. Obstruir los actos de verificación de la autoridad;

XV. Recabar datos en forma engañosa y fraudulenta;

XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;

XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;

XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y

XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

Artículo 64.- Las infracciones a la presente Ley serán sancionadas por el Instituto con:

I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior;

II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior;

III. Multa de 200 a 320,000 días de salario mínimo general vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y

IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Artículo 65.- El Instituto fundará y motivará sus resoluciones, considerando:

I. La naturaleza del dato;

II. La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos de esta Ley;

III. El carácter intencional o no, de la acción u omisión constitutiva de la infracción;

IV. La capacidad económica del responsable, y

V. La reincidencia.

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

## CAPÍTULO XI

### De los Delitos en Materia del Tratamiento Indebido

#### de Datos Personales

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

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

Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

#### Transitorios

Primero.- El presente Decreto entrará en vigor al día siguiente al de su publicación en el Diario Oficial de la Federación.

Segundo.- El Ejecutivo Federal expedirá el Reglamento de esta Ley dentro del año siguiente a su entrada en vigor.

Tercero.- Los responsables designarán a la persona o departamento de datos personales a que se refiere el artículo 30 de la Ley y expedirán sus avisos de privacidad a los titulares de datos personales de conformidad a lo dispuesto por los artículos 16 y 17 a más tardar un año después de la entrada en vigor de la presente Ley.

Cuarto.- Los titulares podrán ejercer ante los responsables sus derechos de acceso, rectificación, cancelación y oposición contemplados en el Capítulo IV de la Ley; así como dar inicio, en su caso, al procedimiento de protección de derechos establecido en el Capítulo VII de la misma, dieciocho meses después de la entrada en vigor de la Ley.

Quinto.- En cumplimiento a lo dispuesto por el artículo tercero transitorio del Decreto por el que se adiciona 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, las disposiciones locales en materia de protección de datos personales en posesión de los particulares se abrogan, y se derogan las demás disposiciones que se opongan a la presente Ley.

Sexto.- Las referencias que con anterioridad a la entrada en vigor del presente Decreto, se hacen en las leyes, tratados y acuerdos internacionales, reglamentos y demás ordenamientos al Instituto Federal de Acceso a la Información Pública, en lo futuro se entenderán hechas al Instituto Federal de Acceso a la Información y Protección de Datos Personales.

Séptimo.- Las acciones que, en cumplimiento a lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, corresponda realizar al Ejecutivo Federal, se sujetarán a los presupuestos aprobados de las instituciones correspondientes y a las disposiciones de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

Octavo.- El Presupuesto de Egresos de la Federación para el Ejercicio Fiscal de 2011 considerará partidas suficientes para el adecuado funcionamiento del Instituto Federal de Acceso a la Información y Protección de Datos en las materias de esta Ley.

Artículo Segundo. 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, para quedar como sigue:

Artículo 3.- Para los efectos de esta Ley se entenderá por:

I. ...

II. Datos personales: Cualquier información concerniente a una persona física identificada o identificable;

III. a VI. ...

VII. Instituto: El Instituto Federal de Acceso a la Información y Protección de Datos, establecido en el

Artículo 33 de esta Ley;

VIII. a XV. ...

## Capítulo II

### Del Instituto

Artículo 33.- El Instituto es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades.

### Transitorio

Único.- El presente Decreto entrará en vigor al día siguiente al de su publicación en el Diario Oficial de la Federación.

DADO EN EL SALÓN DE PLENOS DE LA H. CÁMARA DE SENADORES, EN MÉXICO, DISTRITO FEDERAL, A 19 DE ABRIL DE 2010.

COMISIÓN DE GOBERNACIÓN

COMISIÓN DE ESTUDIOS LEGISLATIVOS

Nota: Con fundamento en Las Reglas Provisionales en Relación con la Gaceta del Senado de la Junta de Coordinación Política de fecha 11 de octubre del año 2006, por el que se crea la Gaceta del Senado y con base en la Regla Segunda, inciso cuatro de ese ordenamiento, la publicación impresa de la Gaceta del Senado y la que aparece en medios electrónicos, tiene sólo propósitos informativos y no genera consecuencias jurídicas fuera del propio Senado.

Opina en [uenlacetransparencia@senado.gob.mx](mailto:uenlacetransparencia@senado.gob.mx)

SENADO DE LA REPÚBLICA: Xicoténcatl No.9, Centro Histórico  
Ciudad de México, Distrito Federal  
C.P 06010 Teléfono: 51-30-22-00