DICTAMEN CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES.

COMISIÓN DE GOBERNACIÓN.

HONORABLE ASAMBLEA:

A la Comisión de Gobernación de la LX Legislatura, fue turnada para su estudio, análisis y dictamen correspondiente, las iniciativas con proyecto de decreto por las que se expiden la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y la Ley Federal de Protección de Datos Personales.

Esta Comisión, con fundamento en lo dispuesto en los artículos 72 y 73 fracción XXIX-O de la Constitución Política de los Estados Unidos Mexicanos y en los artículos 39, 45 numeral 6, incisos e) y f) y numeral 7 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, así como 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 las Iniciativas de referencia, somete a la consideración de esta Honorable Asamblea el presente dictamen, basándose en los siguientes:

I. ANTECEDENTES

1. Con fecha 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 Particulares,

2. Esa misma fecha, el 4 de noviembre de 2008, la Presidencia de la Mesa Directiva, dispuso que la Iniciativa señalada 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.

3. 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 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 a 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.**

4. 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.

5. Esa misma fecha, el 11 de octubre de 2008, 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.

6. Con fecha 21 de abril del año 2009, los miembros de esta Comisión de Gobernación, discutieron y aprobaron el presente dictamen

II.- CONTENIDO DE LAS INICIATIVAS.

Las iniciativas objeto de estos comentarios, coinciden en el aspecto sustantivo, al pretender normar la protección de los datos personales en posesión de particulares, de conformidad con la atribución otorgada por el Poder Revisor de la Constitución, en el artículo 73 fracción XXIX-O de nuestra Norma Máxima, a este órgano Legislativo Federal. En este sentido, es decisión de los miembros de esta Comisión Dictaminadora, integrarlas y dictaminarlas de manera conjunta.

1.- La iniciativa del Diputado Gustavo Parra Noriega tiene por objeto la protección de los datos personales contenidos en bases de datos en posesión de particulares, con la finalidad de garantizar el derecho al honor, imagen y vida privada de las personas.

Afirma el Diputado Parra Noriega en la parte expositiva de su iniciativa que "*el respeto a la dignidad de la persona constituye la base fundamental de la protección de datos personales, en cuanto a que se refiere a una expresión de su vida privada, toda vez que este derecho se basa en el poder de disposición de los datos por su titular, y de decidir, en la mayoría de los casos, a quienes y bajo que condiciones los entrega; lo anterior implica que la persona que tenga a su cargo el tratamiento de datos personales, los debe utilizar con estricto respeto a los derechos del interesado*."

Por otra parte, el Diputado Parra Noriega advierte que el uso indebido de los datos personales *"puede tener consecuencias graves para una persona que pueden ir desde la provocación de actos de molestia al titular de los datos, consistente en el envío ilimitado de información no solicitada; pasando por actos de discriminación, toda vez que mediante el cruce de información de una persona, se puede configurar un perfil respecto de sus gustos, creencias, afinidades o que decir de su estado de salud o mental, que pueden influir negativamente al momento de solicitar se le proporcione un servicio o adquiera un bien; hasta la comisión de delitos graves como el secuestro o el robo de identidad. El uso perverso de la información puede crear problemas muy serios que han convertido a la persona en un ser vulnerable que vive con la amenaza latente de ser observado en forma permanente."*

Respecto de la estructura normativa de la iniciativa del Diputado Parra Noriega, que se analiza y dictamina por parte de esta Comisión de Gobernación, el legislador presenta una iniciativa conformada por 58 artículos referidos en siete capítulos con cinco artículos transitorios.

En tal tesitura, la exposición de motivos destaca como aspectos importantes del proyecto en cuestión los siguientes:

"a) Se definen diversos conceptos que son fundamentales para la aplicación de la ley, tales como el concepto de datos personales, definido como aquella información concerniente a una persona identificada o identificable, y que para efectos de esta Ley, se divide en datos personales sensibles y datos personales de identificación.

b) En el proyecto se estima que los datos personales sensibles son aquellos relacionados con aspectos genéticos, huella digital o medios de reconocimiento biométrico, así como con la condición médica o de salud, de origen racial o étnico, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas o preferencia sexual del titular. Asimismo, se considera información sensible cualquiera que permita acceder o conocer balances o saldos de cuentas o estados financieros del titular, o en general datos relativos al conocimiento de claves o números de identificación personal de cuentas o tarjetas bancarias, de inversión, títulos u otros instrumentos de crédito.

c) Se establecen los Principios relativos a la Protección de Datos y se considera de obligatoria observancia para los particulares en el tratamiento de datos personales, los principios de licitud, consentimiento, información, calidad, confidencialidad, derecho al olvido y seguridad.

Por lo que respecta al principio del consentimiento, considerado como el eje central en la protección de datos de carácter personal, se establece la obligación consistente en que todo tratamiento de datos personales requiere del consentimiento de su titular y concretamente en lo referente a datos sensibles se prevé que ninguna persona está obligada a proporcionarlos, salvo cuando medie un consentimiento expreso, informado y entendible del titular de los mismos.

d) Se hace referencia a los Derechos de los Titulares de Datos Personales, consistentes en los derechos de acceso, rectificación, cancelación y oposición. Se prevé que todo titular tenga derecho a conocer si sus datos personales se encuentran almacenados en una base de datos y

a solicitar su rectificación o cancelación en forma gratuita y en consultas no menores a seis meses. Además se prevé que los titulares puedan oponerse a proporcionar sus datos personales, salvo que exista obligación por disposición legal, de una relación contractual o por resolución de una autoridad competente.

e) Con la finalidad de que el titular pueda ejercer los derechos ante el Particular, se establece en el Capítulo cuarto un procedimiento ágil consistente en solicitar al Particular el ejercicio de los derechos previstos en la ley, teniendo el Particular un plazo de un máximo de cinco días hábiles para determinar la procedencia de la solicitud, y en su caso permitir el acceso o llevar a cabo la rectificación o cancelación de sus datos personales.

f) Se establece como autoridad administrativa en la materia, la Comisión Nacional de Protección de Datos Personales con la naturaleza jurídica de un organismo descentralizado de la Administración Pública Federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio; contando con plena autonomía técnica y de gestión, así como para dictar sus resoluciones.

g) Se regula el Procedimiento de Declaración Administrativa de Infracción, con la finalidad de que la Comisión determine la procedencia de la solicitud de acceso, rectificación, cancelación u oposición de datos personales, ante una negativa del Particular.

h) Se establecen aquellas conductas que constituyen infracciones a la ley, así como las sanciones a que se harán acreedores aquellas personas que infrinjan la ley, las cuales serán fundadas y motivadas y consistirán desde la obligación para que el particular lleve a cabo los actos solicitados por el titular, hasta multa de 5000 días de salario mínimo vigente en el Distrito Federal."

2.- La iniciativa del Diputado Adolfo Mota Hernández tiene por objeto regular el derecho a la autodeterminación informativa de las personas que permita, por una parte, la transferencia legítima, controlada e informada de los datos personales y por otra, la protección a la privacidad cuando se trate de datos sensibles, así como regular el tratamiento de los datos personales por parte de los sujetos responsables.

En este sentido, el Diputado Mota Hernández reconoce en la Exposición de Motivos de su iniciativa que: "*En el contexto actual de globalización que ha presentado avances impresionantes en la tecnificación de instrumentos y mecanismos de procesamiento de datos de toda índole, la protección de la privacidad de los datos personales se ha convertido en un tema de la mayor importancia que inevitablemente requiere de nuestra atención."*

Bajo tal tesitura, continúa exponiendo en su iniciativa el Diputado Mota Hernández lo siguiente: *"Sin embargo, también encontramos como una realidad ineludible que los datos personales son necesarios para una infinidad de operaciones comerciales o de muy diversas índoles en beneficio de sus titulares y, en general, del comercio y la economía nacional. Incluso, en ocasiones la existencia de estos es el habilitador para industrias enteras, como las de algunos modelos de tercerización de servicios o los llamados centros de contacto. Es decir, no es posible que las múltiples relaciones que se esbozan entre las personas, que incluso se dan*

entre una jurisdicción y otra, puedan llevarse a cabo sin diversos grados de manifestación y uso de los datos personales."
Respecto del desarrollo normativo de la iniciativa del Diputado Adolfo Mota Hernández, que se analiza y dictamina por parte de esta Comisión de Gobernación, ésta se encuentra integrada por 48 artículos divididos en dos Títulos y con cuatro artículos transitorios.

En este contexto, la exposición de motivos del Diputado Mota Hernández, destaca como aspectos importantes los siguientes:

"a) Es necesario entonces desarrollar un marco normativo específico para la protección de los datos personales en posesión de los particulares. En este sentido, sin embargo la legislación que se establezca en nuestro país debe encontrar un balance entre la protección efectiva de los datos, y por tanto de los derechos de los particulares, y la necesidad de dichos datos para la generación de productos y servicios que generen valor económico, empleo y desarrollo en el país.

b) La presente iniciativa desde su construcción, busca establecerse dentro de lo que hemos denominado el modelo híbrido de regulación de los datos personales. En particular, se ha buscado un apego a los principios internacionales reconocidos sobre la materia en los distintos foros internacionales de los que México es parte (principalmente APEC y OCDE) con el fin de dar cumplimiento a los compromisos contraídos por México.

c) *La iniciativa además, se centra en proveer a los titulares de información sobre los datos que se recopilan de ellos y con qué propósito. Esto se logra por medio del aviso de privacidad que los responsables del tratamiento de los datos personales (entendido de la forma más amplia posible) tienen que presentar a los titulares especificando no solamente que datos recopilarán, sino los fines para lo que lo hacen y cualesquiera fines secundarios para los que pudieran utilizarse dichos datos.*

d) La iniciativa determina la existencia de una autoridad central que sea responsable del cumplimiento de la ley y que pueda establecer sanciones en la esfera administrativa. Esta autoridad está particularmente enfocada al cumplimiento de las obligaciones que los responsables de los datos tienen que dar para permitir el acceso y corrección de los datos a los titulares de éstos.

En la iniciativa se reconoce también en la designación de la autoridad, que en los tiempos actuales la creación de organizaciones, si bien necesarias para el cumplimiento de la ley, deben buscar minimizar los costos del Estado. Es por ello que se ha buscado establecer la responsabilidad a un ente especializado pero dependiente de una secretaría de Estado del Ejecutivo federal.

La elección de la Secretaría de Economía (SE) para que de ella se desprenda la autoridad reguladora no es fortuita. La SE tiene hoy entre sus atribuciones y órganos desconcentrados o especializados la protección de otros derechos como el del consumidor por medio de la Procuraduría Federal del Consumidor (Profeco) o el de la protección de la propiedad industrial por medio del Instituto Mexicano de la Propiedad Industrial (IMPI). Se ha considerado que esta

vocación de la SE de asegurar los derechos de los particulares y al mismo tiempo considerar las necesidades de la actividad industrial y comercial aseguraría el balance necesario entre la protección de los particulares y la necesidad del mercado de utilizar los datos para su operación comercial.

e) La presente iniciativa reconoce también la necesidad de que los responsables de los datos establezcan medidas de seguridad para proteger estos. Sin embargo, se intenta en la iniciativa mantener un principio de neutralidad tecnológica al dejar a determinación del responsable de los datos las medidas a utilizar, estableciendo como requisito que dichas medidas no sean menores a las que el responsable aplica a sus propios datos.

f) Consideramos que la autoridad gubernamental no debe tener el papel de regular las medidas de protección. Las instituciones gubernamentales no cuentan con la experiencia o velocidad para definir las medidas de seguridad al ritmo que lo hace el mercado por medio de las mejores prácticas internacionales. Consideramos asimismo que al no ser estas definidas por la autoridad se reconoce que no todos los responsables tienen las mismas capacidades o necesidades de protección pues existen distintos niveles de sensibilidad de la información y capacidad de protección debido a la naturaleza de las organizaciones que son responsables de los datos.

g) Tanto las medidas relativas a la seguridad como las que se refieren a las limitaciones y derechos a proteger dependen de establecer la responsabilidad de quien trata los datos, aún cuando estos sean transferidos a un tercero para su procesamiento. El enfoque de la iniciativa a diferencia de otras propuestas no establece la responsabilidad de consentimiento ante la transferencia por encontrar que ello no es ni práctico, ni establece un nivel efectivo de protección para el titular de los datos. La iniciativa reconoce la necesidad de la transferencia para las operaciones comerciales, sin embargo, establece que la responsabilidad de los datos no solamente no cesa ante la transferencia sino que las condiciones establecidas en el aviso de privacidad deben mantenerse por parte del tercero y los niveles efectivos de protección deben ser mantenidos por dicho tercero que tratará los datos. Con ello, se establece un nivel efectivo de protección para el titular, mientras que se reconoce la necesidad de los modelos de negocio para hacer más eficiente la operación de las empresas.

h) Finalmente, la iniciativa establece dos procedimientos fundamentales para otorgar protección efectiva para los titulares de los datos. El primero, es el procedimiento de acceso ante el responsable. En el se establecen las condiciones para que los titulares de los datos personales puedan ejercer sus derechos de acceso corrección, cancelación y oposición ante los responsables del tratamiento de sus datos personales. Esto genera certidumbre en cuanto a establecer procedimientos comunes para el efectivo ejercicio de los derechos.

En segundo lugar se establece un procedimiento ante la autoridad que tiene el objeto de corregir faltas u omisiones que el responsable haya podido cometer, que es la verdadera necesidad del titular, estableciendo sanciones ante el incumplimiento. La posibilidad de que el responsable corrija la situación que despierta la queja del titular, debe ser la principal razón del procedimiento y no la sanción por ella misma. ”

Establecidos los antecedentes y el contenido de las Iniciativas, los miembros de la Comisión de Gobernación de la LX Legislatura de la Cámara de Diputados que suscriben el presente dictamen, exponemos las siguientes:

III. CONSIDERACIONES

A) Valoración de las Iniciativas.

Los miembros de esta Comisión Dictaminadora, coinciden en que el surgimiento del derecho fundamental a la protección de los datos personales, se genera como consecuencia, de la natural evolución de la sociedad.

En efecto, John Rawls señala, que una sociedad puede definirse como una asociación más o menos autosuficiente de personas que reconocen ciertas reglas de conducta como obligatorias en sus relaciones, y que en su mayoría actúan de acuerdo con ellas. En ese sentido, la sociedad se caracteriza típicamente tanto por un conflicto como por una identidad de intereses. Esta doble faceta en la caracterización de la sociedad surge debido a que, si bien es cierto que la cooperación social hace posible para todos una vida mejor de la que cada uno tendría viviendo en el aislamiento, también lo es que las personas no son indiferentes respecto a cómo han de distribuirse los mayores beneficios producidos por la colaboración.[1]

Sin duda, a lo largo de los estadios por los que ha pasado la historia de la humanidad, ésta se ha agrupado y gobernado bajo regímenes normativos muy diversos, creando importantes cuerpos normativos[2], no obstante lo cual hasta antes del siglo XVIII, no era posible aludir a la existencia de un conjunto de valores (listado de derechos) respecto de los cuales se tuviera la certeza histórica que el ser humano compartía en común. En ese sentido, la Ilustración señala el momento a partir del cual dio inicio la evolución de las instituciones que han forjado al Estado Moderno, entre cuyos productos se encuentran las declaraciones de derechos y las constituciones políticas.

Con las ideas de la Ilustración, comenzó una revolución normativa irreversible de la que derivarían, 200 años más tarde, instrumentos como la Declaración Universal de los Derechos Humanos, en la que se contiene en “germen” la síntesis de un movimiento dialéctico que comenzó con la universalidad abstracta de los derechos naturales, pasó por la particularidad concreta de los derechos positivos nacionales y terminó con la universalidad ya no abstracta sino concreta de los derechos positivos universales, dando inicio a un largo proceso cuya realización última no podemos aún ver[3].

Constata lo anterior, la existencia de las distintas fases por las que han pasado los derechos humanos. En un primer tiempo se afirmaron los derechos de libertad, es decir, todos aquellos derechos que tienden a limitar el poder del Estado y a reservar al individuo o a grupos

[1] *Vid*. RAWLS, John. *Teoría de la Justicia*, México, Fondo de Cultura Económica 1979, p. 1.
[2] El Código de Hammurabi en la antigua Mesopotamia, las XII Tablas y el denominado *Corpus Iuris Civilis* en Roma, así como el derecho común europeo en la Alta Edad Media, entre otros.
[3] *Vid*. PECES- BARBA, Gregorio. *Derecho positivo de los derechos humanos*, Madrid, Debate, 1987,

particulares una esfera de libertad frente al mismo. En un segundo momento se proclamaron los derechos políticos, al concebirse la libertad no sólo como el "no impedimento", sino positivamente como autonomía, teniendo por consecuencia una participación cada vez más amplia, difundida y frecuente de los miembros de una comunidad por el poder político (es decir, libertad dentro del Estado). Por último, se reconocieron los derechos sociales, que expresan la maduración de nuevas exigencias, de nuevos valores, como los del bienestar y de la igualdad no solamente formal, derechos a los que se podría llamar libertad a través o por medio del Estado.[4]

El siglo XXI comienza con un despliegue tecnológico trascendental. No puede concebirse más la vida de los seres humanos ni su interacción, sin el uso de tecnologías. Dicha expansión conlleva el intercambio de flujos de información incluida 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, ya que la sencilla obtención de cualquier tipo de dato sobre una persona física posibilita la generación de perfiles sobre ella y afectar la esfera de sus derechos y libertades.

Los avances tecnológicos repercuten generalmente de forma positiva en la calidad de vida del ser humano, mas sería ingenuo desconocer que también con ellos nacen nuevos conflictos e interrogantes a los que el Derecho debe dar respuesta. La tecnología no ha de permanecer ajena al Derecho, ni evidentemente, a la Constitución.

Por esa razón y desde hace décadas, cada vez más países aprueban nuevas leyes sobre privacidad o protección de datos[5], esto en atención al menor o mayor grado de importancia que a la privacidad se le asigne, ya que está ligada al pasado cultural e histórico de cada sociedad.[6]

Recientemente, la Cumbre Mundial de la Sociedad de la Información ha hecho un llamamiento para pedir normas "mundiales" para la privacidad en el sentido siguiente: *"Hacemos un llamamiento a todas las partes interesadas para garantizar el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de legislación, la aplicación de marcos de colaboración, mejores practicas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios".*[7]

---

[4] *Vid*. BOBBIO, Norberto. *El tiempo de los derechos*, Madrid, Sistema, 1991, p 109.

[5] El último reporte sobre Privacidad y Derechos Humanos 2006 del E*lectronic Privacy Information Center (EPIC*), da cuenta de los desarrollos constitucionales, legales y del marco regulatorio en materia de protección a la privacidad en mas de 75 países alrededor del mundo. Ver www.epic.or

[6] Esta afirmación corresponde, entre otros a J. DHONT y M. V. PEREZ ASINARI, "*New Physics and the Law. A comparative Approach to the EU and US Privacy and Data Protection Regulation, looking for Adequate protection"* en Flujos transfronterizos y extraterritorialidad: La postura europea, PUOLET, Ives, Revista Española de Protección de Datos p.112. Julio-Diciembre 2006. Thomson Civitas.

[7] Idem.

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 la importancia de esta; así, el artículo 12 de la Declaración Universal de los Derechos del Hombre[8] (10 de diciembre de 1948) 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.

En el mismo sentido, el artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales[9] (14 de noviembre de 1950), 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[10] (16 de diciembre de 1966), 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[11] 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.

Ahora bien, 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. Así, en 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar 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[12]".

En un momento posterior, surgen diversas leyes nacionales, en 1977 era aprobada la Ley de Protección de Datos de la República Federal Alemana, mucho más ambiciosa que su predecesora del *Land* de *Hesse*, en 1978 corresponde el turno a Francia mediante la publicación de la Ley de Informática, Ficheros y Libertades, aún vigente. Otros países entre los que se emitió regulación en la materia son Dinamarca con las leyes sobre ficheros públicos y privados (1978), Austria con la Ley de Protección de Datos (1978) y Luxemburgo con la Ley sobre la utilización de datos en tratamientos informáticos (1979)[13].

[8] http://www.un.org/spanish/aboutun/hrights.htm.
[9] http://www.derechos.org/nizkor/espana/doc/conveudh50.html.
[10] http://www.derechos.org/nizkor/ley/pdcp.html.
[11] http://www.oas.org/juridico/spanish/Tratados/b-32.html.
[12] *Vid.* Piñar Mañas, José Luis. El derecho fundamental a la protección de datos personales, en Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Valencia, 2005, p 20.
[13] *Ibidem*.

Hacia la década de los años ochenta surgen los instrumentos normativos en los que se plasma un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como las medidas de seguridad a observar por parte de los responsables de los ficheros. Es en esta década cuando desde el Consejo de Europa se dio un respaldo definitivo a la protección de la intimidad frente a la potencial agresividad de las tecnologías, siendo decisivo para ello la promulgación del convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.[14]

El Convenio 108 sobre protección de datos personales (en adelante el Convenio 108) entró en vigor el 1 de octubre de 1985 y es 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.

Hay que decir que el Convenio 108 no proporcionó la suficiente protección homogénea en materia de protección de datos que se había esperado. Esto debido esencialmente a la naturaleza del Convenio: el mismo a pesar de ser vinculante, establecía únicamente unos principios mínimos, permitiendo que posteriormente fueran los estados firmantes los que los desarrollaran.[15]

En este contexto, 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 con un doble objetivo: por un lado, 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, ampliando los principios ya recogidos en otras normas internacionales y otorgando un mayor nivel de protección dentro de la Comunidad, sin disminuir el ya existente; y, por otro lado impedir la restricción de la libre circulación de los datos personales en todos los Estados miembros de la Unión Europea.[16]

El proyecto de Directiva 95/46, se inspira esencialmente en la doctrina constitucional alemana y en la ley francesa de 1978. Sin embargo, los trabajos se paralizan, dado que diversos estados consideran que no es posible la aprobación por parte de las instituciones comunitarias de una norma reguladora de un derecho fundamental de los ciudadanos, al no tener tal hecho cabida en las normas rectoras del Derecho Comunitario vigentes en ese momento.[17]

---

[14] *Idem*, pp. 20-21.
[15] *Vid.* **ARENAS RAMIRO**, Mónica. *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, p. 156.
[16] **ARENAS RAMIRO**, Mónica. *op. cit.,* pp. 277-278.
[17] **PUENTE ESCOBAR**, Agustín. *Breve descripción de la evolución histórica y del marco normativo internacional de la protección de datos de carácter personal,* en Protección de Datos de Carácter Personal en Iberoamérica (II

A partir de ese momento, los trabajos se centraron en la necesidad de adoptar un texto de Directiva 95/46 referido exclusivamente a la protección de datos de carácter personal como fundamento no a la protección de un derecho fundamental, sino la adopción de un marco comunitario que garantice la libre circulación de los datos de carácter personal, no pudiendo los Estados miembros invocar el derecho a la protección de datos como justificación para impedir dicha libre circulación.[18] La Directiva 95/46, finalmente, es aprobada el 24 de octubre de 1995.

Por su parte, 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, reconociendo 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, 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.

Asimismo, en este recuento, no debe pasarse por alto, las recomendaciones que sobre la materia, ha emitido la Organización para la Cooperación y el Desarrollo Económico (OCDE).

La recomendación de la Organización para la Cooperación y el Desarrollo Económico en la que se contienen las “Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales, adoptada el 23 de septiembre de 1980 (Recomendaciones de la OCDE), constituye el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos de carácter personal.[19]

Su adopción se funda en la constatación por parte del Consejo de la OCDE de la inexistencia de uniformidad en la regulación de esta materia en los distintos Estados miembros, lo que dificultaba el flujo de los datos personales entre los mismos.[20]

La primera parte de la Recomendación, establece las definiciones aplicables, la parte segunda establece los principios básicos aplicables al tratamiento de los datos personales, la tercera está dedicada a las transferencias internacionales de datos, la cuarta trata, en términos generales, sobre los medios de implantación de los principios básicos expuestos en las partes anteriores y la quinta tiene que ver con cuestiones de asistencia mutua entre los países miembros.

Son igual de importantes, los principios emitidos por el Foro de Cooperación Económica Asia Pacífico (APEC). Uno de los grupos formados en este organismo, es el Grupo de Manejo del Comercio Electrónico (ECSG) establecido en febrero de 1999, y que dentro de sus principales

---

Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Valencia, 2005,, p. 43.

[18] *Idem.*

[19] *Vid.* **PUENTE ESCOBAR**, Agustín. *op. cit*., p 51.

[20] *Ibidem.*

actividades esta el desarrollo de legislaciones y políticas compatibles entre las Economías en el campo de la Privacidad, para lo cual 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 seguro y sin obstáculos.

Los principios desarrollados para el Marco de Privacidad de APEC se basan en las Recomendaciones de la OCDE. Estos principios tienen como fin los siguientes aspectos: Proteger la Privacidad de información personal; prevenir la creación de barreras innecesarias al flujo transfronterizo de datos; fomentar la uniformidad por parte de empresas multinacionales en los métodos utilizados para la recolección, uso y procesamiento de datos personales; fomentar los esfuerzos nacionales e internacionales para promover y hacer cumplir las disposiciones legales de protección de datos personales.

La protección de la privacidad está diseñada para prevenir a los individuos a efecto de que sus datos no se recolecten erróneamente o bien se haga un mal uso de ellos, estableciendo medidas de resarcimiento proporcionales, en los casos que así proceda. Entre los principios que se reconocen encontramos el de aviso, limitación de la recolección, el de integridad de la información personal y el de salvaguardias a la seguridad, entre otros.

En el ámbito de la Organización de las Naciones Unidas, la Resolución 45/95 de de 14 de diciembre de 1990, contiene fundamentalmente una lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial, entre otros, los de licitud, exactitud, finalidad, acceso y no discriminación.

Ubicándonos ahora en el ámbito nacional, tenemos que con fecha 11 de julio de 2002, fue publicada en el Diario Oficial de la Federación, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Ley Federal de Transparencia)[21], la cual tiene por objeto regular el derecho a la información en una de sus vertientes, la del acceso a la información.

En este ordenamiento jurídico, los límites al derecho de acceso están señalados de manera expresa en los artículos 13 y 14 y en el artículo 18. Entre las hipótesis normativas previstas en el artículo 18 de la Ley Federal de Transparencia, se 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.

Los datos personales se definen como aquella información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad[22].

[21] http://www.diputados.gob.mx/LeyesBiblio/decre/LFTAIPG_06jun06.doc.
[22] Artículo 3 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Aunado a lo hasta ahora descrito, en el capítulo IV de la Ley Federal de Transparencia se establecen una serie de disposiciones dirigidas a garantizar el derecho a la protección de datos personales, tales como principios, derechos de los interesados, 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.

Con posterioridad a la expedición de la Ley de Transparencia y Acceso a la Información Pública Gubernamental, con fecha 20 de julio de 2007, se publicó en el Diario Oficial de la Federación, la reforma al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, fundamentalmente, con el objeto de homologar el derecho de acceso a la información pública gubernamental, en cualquier punto del territorio nacional y en los diversos órdenes de gobierno.

Al respecto, en el dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, de la Cámara de Diputados se señaló lo siguiente:

“La iniciativa que se dictamina, surge de un análisis pormenorizado y exhaustivo de una problemática nacional que no debemos aceptar: luego de cuatro años de marcha de las leyes de transparencia y acceso a la información, se ha cristalizado una heterogeneidad manifiesta y perjudicial de los cimientos para el ejercicio del derecho, que contienen diversas leyes, tanto federal como estatales.

..”.

La reforma al artículo 6 de la Constitución Federal plantea diversos nuevos retos a la transparencia gubernamental en nuestro país que se materializaron en siete fracciones. En las tres primeras se establecieron los principios fundamentales que dan contenido básico al derecho, mientras que en las fracciones cuarta, quinta y sexta se plantearon las bases operativas que deberán contener las leyes en la materia para hacer del derecho una realidad viable, efectiva y vigente, según señala el ya citado dictamen de la Cámara de Diputados.

El reformado artículo 6, fracción II, establece como parte de los principios en materia de acceso, que la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

Al respecto, en el dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, de la Cámara de Diputados, en el apartado en el que se hace el análisis de la iniciativa, se indicó lo siguiente:

“…

En ella se establece una segunda limitación al derecho de acceso a la información, misma que se refiere a la protección de la vida privada y de los datos personales. Esta información no

puede estar sujeta al principio de publicidad, pues pondría en grave riesgo otro derecho fundamental, que es el de la intimidad y la vida privada.

Es fundamental esclarecer que aunque íntimamente vinculados, no debe confundirse la vida privada con los datos personales…

La fracción segunda establece también una reserva de ley en el sentido que corresponderá a ésta, determinar los términos de la protección y las excepciones a este derecho…

…"

El mencionado artículo 6, fracción II, tiene la virtud de ser la primera disposición en la historia de nuestro país que hace un reconocimiento expreso al derecho a la protección de datos personales en la cúspide normativa, dando continuidad a la labor iniciada por el legislador ordinario a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Ahora bien, en forma reciente, y después de un proceso legislativo tortuoso, El Congreso de la Unión y las legislaturas de los Estados, como parte del proceso de reforma a la Constitución General, aprobaron las reformas a los artículos 16 y 73 de la Constitución General.

La reforma al artículo 16, pendiente de publicación en el Diario Oficial de la Federación, adiciona un párrafo segundo a dicho numeral constitucional, con la finalidad de reconocer en nuestro máximo ordenamiento jurídico, el derecho a la protección de los Datos Personales, en los siguientes términos:

"Artículo 16. . . .

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

Con la reforma al artículo 16 constitucional finalmente se reconoce y da contenido al derecho a la protección de datos personales. En ese sentido, en la reforma se plasman los derechos con los que cuentan los titulares de los datos personales como lo son los de acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO).
Por otra parte, se hace referencia a la existencia de principios a los que se debe sujetar todo tratamiento de datos personales, así como los supuestos en los que excepcionalmente dejarían de aplicarse dichos principios.

Por lo que se refiere al artículo 73 fracción XXIX-O, el cual fue aprobado por los órganos que integran el Poder Reformador de la Constitución, establece la competencia para que el

Congreso de la Unión se constituya como la fuente normativa en materia de datos personales en posesión de particulares.

Existen diversas razones que sustentan que la ley que regule los datos personales en posesión de los particulares, tenga un ámbito de aplicación nacional: por una parte, la necesidad de unificar la tutela de un derecho fundamental en todo el país, en cuanto a derechos, principios y procedimientos de tutela, evitando de esta manera su respeto asimétrico al expedirse tantas leyes como entidades federativas tiene la República mexicana; por otro lado, tenemos al comercio internacional, en virtud de que el Estado Mexicano hacia el exterior es uno y como tal debe contar con una legislación uniforme en sus relaciones internacionales, independientemente del área del territorio nacional donde materialmente se estén tratando los datos personales, y por la otra, que la materia de comercio es federal, de conformidad con nuestra Ley Fundamental.

Aunado a todo lo anterior, esta Comisión que dictamina destaca la importancia de la presente Ley en potencia, toda vez que con un ordenamiento jurídico de esta naturaleza, nuestro país se haría más competitivo en el ámbito mundial, ubicándose en posición de privilegiado en el aspecto económico, ya que al contar con una ley específica en la materia, no sólo se permitirá al gobernado ejercer eficazmente un nuevo derecho fundamental, sino que también traerá consigo que nuestro país, pueda ampliar su relación comercial con bloques económicos de la importancia de la Unión Europea, toda vez que nos encontraremos en posibilidades de garantizar conforme a los estándares internacionales, un nivel de protección de datos personales adecuado al prever principios y derechos de protección y una autoridad independiente que los garantice.

Al respecto, en América Latina, únicamente Argentina cuenta con el reconocimiento de la Unión Europea como país con nivel adecuado de protección de datos, mismo que, dicho sea de paso, representa para la economía argentina ingresos anuales significativos tan sólo en el terreno de las inversiones en el ámbito de la investigación médica y de ensayos clínicos. Detrás de Argentina, países como Uruguay y Chile persiguen actualmente adecuar sus marcos normativos para atraer inversiones en el terreno de la oferta de servicios que requieran el tratamiento de datos personales a través de las tecnologías de la información.

Frente a una crisis económica mundial como la que estamos encarando, México tiene ante sí una oportunidad importante de intensificar su relación comercial con Europa; de constituirse en un país competitivo y en uno de los socios latinoamericanos más importantes del bloque europeo, sobre todo ahora que nuestro país es considerado como un socio estratégico del viejo continente, sin perjuicio de mantener nuestra intensa relación comercial en el ámbito del tratado de Libre Comercio de América del Norte. Al respecto, vale la pena señalar que Canadá también cuenta con reconocimiento por parte de la Unión Europea de país con nivel adecuado de protección de datos. Así, Canadá se constituye como el mejor referente de convivencia en el que el diseño bajo el que se traza su legislación le permite sostener un intercambio comercial importante con la órbita de países del bloque comercial europeo, así como con Estados Unidos de América; asociaciones que impactan amplia y positivamente en su economía, debido a la relevancia de las economías de referencia en el ámbito comercial mundial.

B) Modificaciones a la Iniciativa.

I. Los miembros de esta Comisión que dictamina, se dieron a la tarea de revisar la redacción del artículo 1 de las propuestas de ley en la materia, en las que se fija el objeto de dicho cuerpo legal, reglamentario de los recién reformados artículos 16 y 73 constitucionales. A la luz de lo anterior, entendemos que el objeto de la ley es garantizar la protección de datos personales en posesión de los particulares, en todo el territorio nacional. Lo anterior es así, porque en realidad la protección que se busca por parte del legislador, es a la persona en relación con el tratamiento que se da a su información en el desarrollo de las actividades que día con día, realizan los entes privados. Dado que el uso extendido de la tecnología en ocasiones resulta intrusivo para la privacidad de las personas, ya que permite que se pueda conocer desde sus hábitos de consumo, hasta información sensible, como la ideología o estado de salud, esta Comisión consideró que para efectos de claridad en el objeto de la ley, debiera agregarse la protección all honor, la imagen y la vida privada a través de garantizar el adecuado tratamiento de los datos personales. Por lo anterior, toda persona tendrá el poder de decidir y controlar si un tercero puede transmitir o utilizar sus datos que van desde el teléfono o domicilio, hasta su religión.

En virtud de lo anterior, los miembros redactores de este dictamen, estimamos conveniente, retomar los elementos de ambas incitativas para generar la siguiente propuesta de redacción del artículo 1, para quedar de la siguiente manera:

> **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 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.

II. Respecto a los sujetos obligados por la ley, la iniciativa del diputado Adolfo Mota señala en su artículo 3 que no resultan sujetos obligados de la misma, los poderes públicos federales; los sindicatos y asociaciones de profesionales; las Sociedades de Información Crediticia; cualquier otra institución u órgano de naturaleza pública, y las asociaciones religiosas. Por su parte la iniciativa del diputado Gustavo Parra únicamente exceptúa de la aplicación de la Ley a las Sociedades de Información Crediticia, y a 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.

En ese punto en particular, respecto de los sujetos obligados por la Ley, esta Comisión considera importante hacer la reflexión siguiente. La voluntad del constituyente al reformar el artículo 73 de nuestra carta magna, fue la de sujetar a los particulares a un régimen de protección de datos personales en todo el territorio nacional, dado que por virtud del artículo 6º, los ciudadanos ya gozan de la protección a la información sobre su vida privada y datos

personales contenidos en los archivos públicos. Lo anterior se hace efectivo a través de leyes especiales en la materia o de los capítulos sobre protección de datos que se incluyan en las leyes de transparencia y acceso a la información en los tres órdenes de gobierno. De esa forma, la asignatura pendiente era emitir una ley para completar la protección que ya procura el sector público al privado, y en ese sentido, esta Comisión considera que todos los particulares que traten datos personales deben estar sujetos a esta ley, con excepción de las Sociedades de Información Crediticia, dado que la Ley que las regula ya prevé todos los principios y derechos en materia de protección de datos personales, así como mecanismos procedimentales para hacerlos valer. Por lo anterior, no se considera justificada la excepción de grupos o categorías de particulares que tratan datos, sobre todo, aquellos que se consideran especialmente protegidos, cuando no existe en el orden jurídico vigente, regulación alguna que prevea garantías a los titulares de dichos datos. Por ello, se considera que únicamente se debiera excepcionar de la aplicación de esta Ley a las Sociedades de Información Crediticia y a todos aquellos particulares que utilizan datos personales exclusivamente para su uso personal o doméstico, como pudieran ser agendas u otro tipo de listados de información personal.

Por lo antes manifestado, la redacción del artículo 2 sería la siguiente:

> ***Artículo 2.*** *Son sujetos regulados por la presente Ley, las 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 que hayan sido autorizadas por la Secretaría de Hacienda y Crédito Público para operar con ese carácter, quienes en lo relativo al tratamiento de los datos personales crediticios de sus usuarios, y a las relaciones jurídicas entre éstos y aquellas, están reguladas por 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.

I) Una vez delimitado el objeto y ámbito de aplicación de esta Ley, resulta indispensable abordar los principios que rigen la protección de datos personales. Si bien ambas iniciativas previeron distintos principios, se considera por los miembros de esta Comisión, que resulta nodal completar la columna vertebral sobre la que se despliega el derecho a la protección de datos personales. Para ello se utilizó como referente los estándares tanto nacionales como internacionales en la materia y por tanto, se aclaró el contenido y alcance de los mismos y se añadieron aquellos principios indispensables que hacían falta. Los principios de protección de obligado cumplimiento son las premisas para garantizar al individuo un poder de decisión y control sobre la información que le concierne, plasmados aunque con distintos enfoques en ambas iniciativas. Así, la iniciativa del Diputado Gustavo Parra se

prevén los principios de licitud, consentimiento, información, calidad, confidencialidad, derecho al olvido y seguridad.

Por su parte, la propuesta del Diputado Adolfo Mota establece que los datos personales deberán tratarse conforme a los principios de licitud, aviso, calidad, acceso y corrección de información, seguridad y custodia y consentimiento. Ahora bien, ambas iniciativas mezclan principios y derechos aplicados al tratamiento de datos personales. Asimismo, en ambos casos se omitieron principios torales en esta materia como son el principio de finalidad, proporcionalidad y responsabilidad.

En virtud de lo anterior, los miembros redactores de este dictamen, estimamos conveniente, modificar la propuesta de redacción del artículo 7 de ambas iniciativas, para quedar de la siguiente manera:

> ***Artículo 7.*** *Los particulares en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, proporcionalidad y responsabilidad, previstos en la Ley.*

III. Definiciones

Ahora bien, en cuanto al apartado de definiciones, los miembros de esta Comisión consideran que es relevante que las éstas describan claramente los conceptos y alcances de cada de ellas para evitar interpretaciones incorrectas. En ese sentido, la Iniciativa del diputado Adolfo Mota ofrece mayor claridad al establecer las figuras de responsable, titular y tercero.

Principio de licitud

A continuación se analizan los alcances de cada principio. El principio de licitud implica que el tratamiento de los datos personales debe llevarse a cabo de forma leal y lícita; es decir, con pleno cumplimiento de la legalidad y respeto de la buena fe y los derechos del individuo, cuya información es sometida a tratamiento. Este deber se traduce en la prohibición de cualquier tratamiento que implique recabar o conservar los datos mediante la utilización de engaño o fraude, de forma que el individuo no pueda conocer con propiedad los términos y condiciones vinculados a ese tratamiento.

Al respecto, ambas iniciativas coinciden en el contenido de este principio. Sin embargo, la iniciativa del diputado Gustavo Parra añade un concepto innovador que refuerza el espíritu que subyace en el principio de licitud denominado como “la expectativa razonable de privacidad”, el cual se traduce en la confianza que deposita el titular en el responsable en el sentido de que los datos personales serán tratados conforme lo acordado y bajo los términos establecidos.

Derivado de lo anterior, los miembros redactores de este dictamen, estimamos conveniente, plasmar el principio de licitud de la siguiente manera en la ley que se analiza:

> ***Artículo 8.*** *Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por ésta Ley y demás normatividad aplicable.*

La obtención de datos personales no puede hacerse a través de medios ilícitos, engañosos o fraudulentos.

En toda recolección o 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.

- **Principio del consentimiento**

Dado que el derecho a la protección de datos consiste en el poder de decisión y control que goza el individuo sobre el tratamiento de sus datos de carácter personal, la mayor parte de los instrumentos nacionales o internacionales reguladores de esta materia sitúan al consentimiento del interesado, como manifestación de este poder decisorio como causa principal legitimadora del tratamiento de los datos personales.

Este consentimiento debe caracterizarse por ser previo, libre, inequívoco, informado y por último, puede ser revocado por el individuo en cualquier momento, no pudiendo exigirse para esa revocación más requisitos que los que fueron necesarios para la previa prestación del consentimiento. Al respecto, ambas iniciativas prevén este principio universal en sus propuestas. Sin embrago, con la finalidad de lograr la mayor exactitud al principio consagrado, se estima conveniente incorporar la definición de las modalidades del consentimiento establecidas en el Código Civil Federal vigente, ya que es en razón de la naturaleza del dato que se emplea uno u otro.

El consentimiento tácito resultará de hechos o actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente. Este tipo de consentimiento es conocido también como el opt-out y resulta nodal para el sano flujo de datos para el comercio y el crecimiento económico, ya que si se requiriera acreditar de manera fehaciente que la persona ha consentido el tratamiento, tendría que hacerse por escrito estampando su firma o a través de otro medio de autenticación, lo cual podría entorpecer el dinamismo de las transacciones comerciales.

Por su parte, el consentimiento será expreso cuando se manifieste por escrito, medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Este tipo de consentimiento solo se requiere en el caso del tratamiento de datos sensibles, y en aquellos en los que se ha modificado por el responsable de la base de datos de manera sustancial y antagónica, la finalidad originaria para la cual fueron recabados, con excepción del tratamiento que efectúa el sector de prospección comercial.

Por lo anterior, a juicio de esta dictaminadora, se añadió la definición de consentimiento como sigue, además de incluir en el artículo 9 que este puede ser revocado, para quedar de la siguiente manera:

Artículo 3…

I. ***Consentimiento:*** *Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. El consentimiento será expreso cuando se manifieste por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, incluido entre estos últimos el poner a disposición del titular el aviso de privacidad;*

Artículo 9. *Todo tratamiento de datos personales estará sujeto al consentimiento previo de su titular, el cual podrá manifestarse de forma verbal, escrita, a través de medios electrónicos, ópticos o de cualquier otra tecnología o a través de signos inequívocos de acuerdo a lo establecido por 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 10. *Tratándose de datos sensibles, el responsable deberá obtener el consentimiento expreso 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 información que directa o indirectamente contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas y concretas.

Ahora bien, en este punto también se considera indispensable establecer bajo qué condiciones no resulta necesaria la obtención del consentimiento. Al respecto, ambas iniciativas contemplaban los supuestos bajo los cuales resulta válido el tratamiento de datos sin que el titular de los mismos tenga que consentirlo; sin embargo, se considera que para efectos de certeza jurídica y claridad, había que concentrarlos en una disposición que englobara los supuestos correspondientes y evitar nombrar a estas excepciones como fines primarios en un aviso de privacidad, ya que lo anterior aborda otro supuesto relativo a la finalidad del tratamiento.

- **Principio de calidad**

El principio de calidad del dato ha de entenderse específicamente vinculado con la veracidad y exactitud en la que se mantienen los datos personales, de forma que aquél refleje realmente de forma fiel, la realidad de la información tratada. Ello conlleva un doble esfuerzo para los particulares responsables: por un lado deberán asegurarse en el momento de la recogida de la información, sobre todo cuando la misma no procede directamente del interesado, de que

aquella resulta exacta y actualizada; por otro debería, siempre que ello sea posible, adoptar las medidas razonables para que la información responda a esa veracidad mientras persiste en su tratamiento.

En este sentido, ambas propuestas se pronuncian sobre la exactitud y actualización de los datos personales objeto de tratamiento. Sin embargo, con la finalidad de dar mayor exactitud a la definición y alcance de este principio, los miembros redactores de este dictamen, estimamos conveniente, plasmar el principio de calidad de la siguiente manera en la ley que se analiza:

> ***Artículo 12****. El responsable procurará que los datos personales contenidos en las bases de datos sean correctos, consistentes 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.*

- **Principio de finalidad**

La manifestación esencial de la protección de la privacidad en relación con el tratamiento de los datos personales se funda en que el tratamiento únicamente sea llevado a cabo en el ámbito de finalidades determinadas, explícitas y legítimas relacionadas con la actividad del responsable. Junto con esta regla general, se ha venido reconociendo la posibilidad de proceder a este tratamiento para otros fines, siempre que los mismos **no sean incompatibles** con los que motivaron el tratamiento inicial del dato.

El concepto de compatibilidad a los efectos de la aplicación de esta ley, ha de ser necesariamente indeterminado, dado que resulta imposible determinar *a priori* cuándo existe o no la misma. Dicho esto, una interpretación razonable permite concluir que no sería posible restringir el principio considerando prohibida la utilización de datos para ninguna finalidad distinta de la que motivó el tratamiento, pero tampoco sería acorde con la protección que se pretende, el conferir una interpretación extensiva que considere que toda la actividad de un responsable puede considerarse compatible con la parte de la misma que dio lugar al tratamiento. En todo caso, la aplicación de esta regla impone al responsable la necesidad de encontrar legitimado el tratamiento de los datos con arreglo a los principios contenidos en la ley que se somete a consideración, en aquellos supuestos en los que no se produce tal compatibilidad.

Ninguna de las iniciativas prevén el principio de finalidad como tal, a pesar de que de manera indirecta en la iniciativa del diputado Gustavo Parra se incluye el término “fin lícito” en su artículo 7 y por su parte, la iniciativa del Diputado Mota aborda los “fines primarios y secundarios”. Por lo anterior, esta dictaminadora considerando esencial el contemplar y definir el principio de finalidad como uno de los ejes rectores de la protección de datos, al tiempo que se retoma el régimen de finalidades de la propuesta del diputado Mota de manera más concisa, para quedar de la siguiente manera:

Artículo 13. *El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades primarias y secundarias previstas en el aviso de privacidad.*

La obtención y el tratamiento de los datos personales, deberá estar relacionado con la finalidad primaria puesta a disposición del titular. En el caso del tratamiento de datos personales que vayan a ser utilizados para finalidades secundarias, no se requerirá recabar el consentimiento del titular, siempre y cuando en el aviso de privacidad se incluyan dichos fines secundarios.

En aquellos casos en que el responsable pretenda tratar los datos para un nuevo fin secundario, que no resulte compatible o análogo a los fines establecidos en el aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

- **Principio de proporcionalidad**

Pasando ahora al principio de proporcionalidad, es menester mencionar que se encuentra directamente relacionado con el de finalidad. La exigencia al responsable de únicamente tratar datos proporcionales para la finalidad para la que se obtuvieron ha sido analizada por los distintos derechos regionales o nacionales desde dos perspectivas distintas, aunque complementarias: por una parte, los datos sólo deberían ser los adecuados o necesarios para la finalidad que justifica el tratamiento (principio de proporcionalidad en sentido estricto); por otra, quien procede al tratamiento de los datos deberá analizar las finalidades que justifican el tratamiento, de modo que sólo debería tratar la mínima cantidad de información necesaria para conseguir la finalidad perseguida (principio de minimización).

Bajo este tenor, la ley que se analiza trata de vincular ambos principios, debiendo la entidad o persona responsable configurar, bien directamente o a través de un prestador de servicios, el tratamiento de los datos de forma que únicamente sean objeto de aquél los mínimos datos necesarios para la finalidad que lo justifica. La segunda consecuencia de la aplicación de este principio será que deberá tenderse siempre que sea posible en el tratamiento de los datos a realizar el mismo de forma anonimizada o disociada.

Sobre el particular, ambas propuestas no incluyen en sus disposiciones este principio toral en todo tratamiento de datos personales, razón por la cual, los miembros redactores de este dictamen estimamos conveniente incorporar una disposición que recoja la definición, alcance y sentido del principio de proporcionalidad de la siguiente manera en la ley que se analiza:

Artículo 14. *El tratamiento de datos de carácter personal será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el artículo anterior. En particular para datos sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de conservación de los datos de carácter personal para que el tratamiento sea el mínimo necesario.*

- **Principio de responsabilidad**

Ahora bien, sin temor a equivoco, la aportación central de esta dictaminadora es el incorporar el principio de responsabilidad, el cual debe entenderse, en el sentido de que corresponderá a la entidad o persona responsable el deber de velar por el cumplimiento de los principios y rendir cuentas al titular en caso de incumplimiento. Este principio es la verdadera garantía para el titular de los datos quien deposita su confianza en el responsable, mismo que deberá tomar todas las previsiones para que los datos sean tratados de acuerdo con la voluntad del dueño de la información y bajo las medidas de seguridad que se prevean por la vía contractual. Así, dado que existe un tráfico de datos intenso y en muchas ocasiones este se da fuera de las fronteras de nuestro país, el ciudadano tendrá la tranquilidad de que si su información ha trascendido a manos de terceros en otras latitudes, éste estará enterado de las cautelas con que debe tratar su información.

El responsable es quien en última instancia decide que se proceda al tratamiento de los datos de carácter personal. Por este motivo, será él quien deba asegurarse de que el tratamiento dentro y fuera del país donde fueron recabados originalmente, se lleva a cabo en cumplimiento de los principios esenciales de protección de la privacidad en lo referente al tratamiento de los datos personales.

Al respecto, ambas iniciativas carecen de una disposición específica que plasme el sentido y motivo de ser de este principio fundamental en la materia, si bien el artículo 18 de la Iniciativa del diputado Adolfo Mota de manera innovadora, establece el régimen de subrogación a las obligaciones del responsable por parte del tercero receptor del dato y del aviso de privacidad, los miembros redactores de este dictamen consideramos conveniente incorporar una disposición que recoja la definición, alcance y sentido de este principio de la siguiente manera en la ley que se analiza:

> *Artículo 15 El responsable velará por el cumplimiento de los principios de protección de datos 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, será respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.*

- **Principio de información**

La protección a la privacidad de la persona en lo relativo al tratamiento de sus datos personales ha de traducirse necesariamente en el derecho, y correlativo deber para la entidad o persona responsable, de poder conocer efectivamente la existencia misma del tratamiento y las características esenciales del mismo, en términos que le resulten fácilmente comprensibles. Este derecho/deber se traduce en el denominado principio de información. Este principio permite a la persona conocer los tratamientos de sus datos personales que están siendo llevados a cabo y, lo que resulta esencial, ejercer los derechos comúnmente reconocidos en relación con esos tratamientos. Desde el punto de vista de su extensión, el principio de

información ha de aplicarse a todos los tratamientos que se lleven a cabo, con independencia de si los datos proceden del interesado o de otras fuentes, así como a la información útil relativa a cada uno de ellos. El principio de información se materializa a través de un aviso de privacidad, el cual debe darse a conocer al momento de la recolección de los datos personales.

> Al respecto, la iniciativa del diputado Adolfo Mota define al principio de referencia como principio de aviso. Asimismo, establece el contenido y modalidades del aviso de privacidad. Por su parte, la iniciativa del diputado Gustavo Parra en los artículos 15, 16, 17 señala la obligación del responsable de proporcionar el aviso de privacidad, el contenido y las modalidades de dicho aviso, respectivamente. Sin embrago, con la finalidad de dar mayor exactitud a la definición y alcance de este principio, los miembros redactores de este dictamen, estimamos conveniente, plasmar el principio de información como estableció en los artículos 15, 16, 17 y 18.

IV. Procedimiento ante el responsable y tutela de derechos

Los redactores de este dictamen, coincidimos en que en esta materia, el procedimiento para que el ejercicio de los derechos de acceso, rectificación, cancelación u oposición deber ser sencillo, ágil, eficaz, que no conlleve demoras o costos indebidos y a través del cual los titulares puedan acceder, rectificar, cancelar o hacer efectivo su derecho de oposición respecto de los datos personales que le conciernen.

Ahora bien, ambas iniciativas prevén procedimientos para el ejercicio de estos derechos en los que los plazos estipulados son muy cortos, lo cual implicaría un potencial riesgo de incumplimiento del responsable ante las solicitudes recibidas. Asimismo, los procedimientos previstos son confusos e imprecisos imposibilitando la comprensión de los mismos por parte de los titulares.

De manera particular la iniciativa del diputado Gustavo Parra enumera una serie de excepciones por las cuales se puede negar el ejercicio de cualquiera de los derechos y las causales por las cuales el titular afectado en sus derechos por el responsable puede solicitar una declaración administrativa de infracción ante la autoridad garante.

Por otra parte, la iniciativa del diputado Adolfo Mota prevé los siguientes aspectos relativos al procedimiento: a) modalidades para otorgar el acceso a los titulares ante el responsable; b) prevención ante una solicitud ambigua; c) plazos para el cumplimento de la obligación del responsable y d) notificación de la respuesta.

Así, los miembros de esta Comisión de Gobernación, convencidos de las bondades de que la ley en potencia, en su aspecto adjetivo, desarrolle un procedimiento expedito mediante el cual los titulares puedan ejercer los derechos de acceso, rectificación, cancelación u oposición, y derivado de un análisis y valoración a las disposiciones contenidas en ambas iniciativas relativas al procedimiento aludido, consideramos establecer como ejes rectores la determinación de plazos razonables de respuesta; el establecimiento de causales de negativa del responsable para el ejercicio de los derechos referidos; la posibilidad de aclaración ante una solicitud ambigua; la enumeración de los requisitos que debe contener la solicitud del titular; así

como la gratuidad en la entrega de los datos personales o costos pertinentes para consultas posteriores.

Derivado de lo anterior, y por cuestiones de técnica legislativa, que deberá desencadenar en una mejor comprensión, interpretación y aplicación del procedimiento aludido, estimamos necesario crear un capítulo IV específico denominado “Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición”.

V. Autoridades reguladoras

Los miembros de esta Comisión consideran que nuestro país debe adoptar el modelo regulatorio que aplica en la materia en Canadá, a través del cual cada autoridad emite regulación secundaria derivada de esta Ley, en el ámbito de sus atribuciones y por su parte, existe una instancia u órgano garante frente al titular de los datos que resuelve sus quejas denominadas solicitudes de protección de datos personales. De esa forma, dada la especialización en temas como comercio, comunicaciones y transportes o salud, correspondería a las Secretarías de Estado del ramo específico, el emitir lineamientos, recomendaciones y criterios que permitan la adecuada observancia de los principios y derechos que rigen en materia de protección de datos.

En particular, y toda vez que es en materia comercial donde se da el mayor flujo de información, repercutiendo directamente en el mejoramiento de la economía nacional al crear fuentes de empleo e impulsar la venta de bienes y servicios tanto a nivel nacional como internacional, será la Secretaría de Economía la que gozará de nuevas atribuciones para la consecución de una adecuada rectoría de esta materia.

VI. Instituto Federal de Acceso a la Información Pública como autoridad garante

Respecto a la autoridad, en la iniciativa del diputado Gustavo Parra se propone la creación de una nueva institución que tenga por objeto la función protección de datos personales en posesión de entes privados denominada Comisión Nacional de Protección de Datos Personales. Por otro lado, la iniciativa del diputado Adolfo Mota propone la creación de un Instituto de Protección de Datos Personales, organismo descentralizado dependiente de la Secretaría de Economía.

Tomando en cuenta las consideraciones de los integrantes de la **Comisión de Presupuesto y Cuenta Pública** en el sentido de que la creación de un nuevo organismo descentralizado impactaría negativamente en las finanzas públicas dados sus costos de implementación, se señala lo siguiente. Esta dictaminadora considera que el Instituto Federal de Acceso a la Información Pública (IFAI) debiera contar con nuevas atribuciones por virtud de esta ley para garantizar, además del derecho a saber de los ciudadanos, la protección de su información personal, por las siguientes razones.

a) **Ahorro de costos adicionales.** Se evitarían gastos e inversiones importantes que sobrevendrían con la creación de una nueva autoridad en materia de protección de datos personales. En su lugar, con una economía importante, se destinarían los recursos

humanos, financieros y materiales estrictamente necesarios para adecuar la estructura del IFAI, de modo que se adapte para ejercer nuevas atribuciones en el ámbito del sector privado.

Pero no solo por razones de costos de creación institucional resulta conveniente que el IFAI asuma la aplicación e interpretación de esta nueva pieza legislativa. En México, el IFAI está a cargo de la protección de datos en la Administración Pública Federal. La legislación mexicana reconoce el acceso y la protección de datos personales a través de derechos y principios reconocidos internacionalmente. Por otra parte, el IFAI ha expedido regulación secundaria -lineamientos y recomendaciones- con el objeto de establecer las políticas y los procedimientos para asegurar el adecuado tratamiento de los datos personales, incluido los niveles de seguridad atendiendo a su sensibilidad, así como su acceso y rectificación por parte de sus titulares. En relación con la solución de controversias, el IFAI ha resuelto privilegiando el acceso a los solicitantes de sus datos personales bajo el criterio de que no hay de causal de clasificación oponible a ese derecho fundamental.

Las ventajas de concentrar en el IFAI la función de proteger datos personales en posesión de entes privados serían las siguientes:

b) Unicidad de criterio. Se evitarían conflictos potenciales entre los criterios de apertura de información y la protección de datos personales. Esto es importante para garantizar al ciudadano seguridad y certeza jurídicas en cuanto al alcance de dos derechos reconocidos constitucionalmente. En México se podrían dar casos donde el IFAI garantice la publicidad del nombre de personas que reciben recursos públicos, mientras que el órgano encargado de la protección de datos personales considere que esa información es confidencial. Lo anterior representaría un retroceso en el terreno hasta ahora ganado por el derecho a saber y el principio de máxima publicidad en los actos de gobierno. Asimismo, podrían presentarse asimetrías en el grado de observancia de los principios de protección de datos personales exigidos a los responsables de sistemas de datos en posesión del Estado, de aquellos en posesión de los particulares. Los problemas de unicidad de criterio se reflejan en el caso francés y portugués.

c) Curva de aprendizaje. En el caso del IFAI se aprovecharía la acumulación de conocimiento y especialización en materia de datos personales, incluida la implementación de regulación secundaria –lineamientos y recomendaciones-, solución de controversias para la tutela de derechos de acceso y rectificación, así como los que sobrevendrían de cancelación y oposición (derechos ARCO), supervisión del cumplimiento regulatorio –verificaciones-, promoción de la cultura y capacitación en la sociedad, las relaciones institucionales nacionales e internacionales, la membresía de grupos de trabajo *ad-hoc*, organizaciones internacionales, y la participación en foros especializados.

d) Autonomía. Tal y como se pretende en ambas iniciativas, para efectos de la creación de un nuevo organismo, el IFAI reúne las características de ser un organismo descentralizado no sectorizado de la Administración Pública Federal con autonomía técnica y de gestión, así como con personalidad jurídica y patrimonio propios. Adicionalmente, tiene otras ventajas como el hecho de ser reconocido como un órgano especializado e imparcial con una clara

autonomía presupuestaria, operativa y de decisión en ese respecto; su órgano máximo de decisión está integrado de manera colegiada -lo que se recomienda en este tipo de instituciones- y es la autoridad suprema tanto para efectos sustantivos –pleno- como administrativos -órgano de gobierno-, sin injerencia de una Junta de Gobierno integrada por representantes de otras instancias dependientes del Ejecutivo Federal.

e) **Posicionamiento del tema en el entorno político y social.** El IFAI cuenta ya con un grado de conocimiento del público superior al 54% de la población en tan sólo 5 años de operación. Con respecto a la percepción ciudadana sobre la confianza y la calificación en sus instituciones públicas, el IFAI, a pesar de su corta vida, ocupa un lugar comparable al del IFE y superior a la CNDH y la SEP. Adicionalmente, debe destacarse que, en los mismos 5 años, el IFAI logró que el grado de conocimiento de la Ley de Transparencia avanzara de un 22% a un 66% de la población. Finalmente, buena parte de la población percibe al IFAI como el garante y promotor de los derechos fundamentales de acceso a la información y de protección de los datos personales en la Administración Pública Federal –*Vg.* expedientes médicos-, por lo que no sería problema orientar esa percepción en materia de protección de la privacidad en los entes privados.

VII. Procedimiento de tutela de derechos ante el Instituto

Los redactores de este dictamen, coincidimos en lo preponderante que es establecer un procedimiento sencillo y expedito por medio del cual los titulares que se consideren afectados en el ejercicio de sus derechos de acceso, rectificación, cancelación u oposición por parte del responsable del tratamiento, puedan presentar lo que consideramos debe denominarse como solicitud de protección de datos ante el IFAI.

Así, la iniciativa del diputado Gustavo Parra lo denomina “procedimiento de declaración administrativa de infracción”, en el cual describe las causales de procedencia; los plazos de sustanciación; la información mínima que deberá contener la solicitud del titular; los elementos de prueba admitidos; los requisitos que deberá cumplir los alegatos del responsable y la publicidad de las resoluciones de la autoridad garante.

Por otro lado, la iniciativa del diputado Adolfo Mota prevé un procedimiento administrativo de protección de datos sustanciado ante la autoridad garante, en el cual contempla las causales de procedencia; los requisitos que deberá cumplir el titular afectado en su solicitud; plazos y condiciones de sustanciación; sentido de las resoluciones; causales de improcedencia y sobreseimiento del procedimiento y medios de impugnación de las resoluciones emitidas por la autoridad garante.

Ahora bien, en ambas iniciativas los plazos previstos para emitir una resolución se consideran muy cortos, lo cual implica un potencial riesgo de incumplimiento de la autoridad garante para atender debidamente la solicitud del titular de los datos. De igual forma, se considera necesario aclarar algunas fases del procedimiento para brindar mayor certeza jurídica a las partes. En esa misma tesitura y derivado de un análisis y valoración de las disposiciones contenidas en ambas iniciativas y a efecto de lograr una mejor comprensión, interpretación y aplicación del procedimiento ante el Instituto, estimamos imprescindible crear un capítulo específico

denominado “Del Procedimiento de Tutela de Derechos” en la ley que se analiza, el cual establece los ejes rectores que le dan vida al mismo.

Finalmente, vale la pena señalar que se añade un procedimiento de conciliación entre el responsable y el solicitante, por medio del cual se busca reducir los plazos del procedimiento y lograr satisfacer los extremos de su petición. El acuerdo conciliatorio constará por escrito y tendrá efectos vinculantes para las partes y el Instituto verificará el cumplimiento respectivo.

VIII. Medidas de seguridad

Ahora bien, la seguridad en el tratamiento de los datos de carácter personal es vital para garantizar de forma efectiva la privacidad de las personas, estableciendo controles o medidas que impidan el acceso indebido a la información.

Pero al propio tiempo, la adecuada garantía de la protección de datos personales exige también que se mantenga la integridad y exactitud de la información personal, de modo que con estas medidas se permita evitar la pérdida total o parcial de los datos o su alteración.

Las medidas de seguridad no sólo deben referirse al funcionamiento de los sistemas de información en que se traten y almacenen datos de carácter personal (tales como la identificación y autenticación o el establecimiento de [bitácoras] logs de acceso a los datos, entre otras), sino que también deben necesariamente complementarse con medidas físicas y administrativas dentro de la organización que, por objeto, permitan el control de acceso físico a los centros de proceso de datos o la entrada y salida de los soportes en que puedan almacenarse datos de carácter personal y la formación de una cultura de seguridad integral.

Así, tanto la persona o entidad responsable como los encargados y terceros (estos últimos vía contractual) deben proteger los datos de carácter personal que sometan a tratamiento mediante la implementación de medidas técnicas, físicas y organizativas que resulten idóneas para garantizar su integridad, confidencialidad y disponibilidad. Sobre el particular, ambas iniciativas hacen referencia a que las bases de datos deberán reunir las condiciones de seguridad suficientes para garantizar la debida custodia de la información que alojan; sin embargo, a juicio de esta Comisión, consideramos importante que las autoridades a que se refiere el artículo 61 de la propuesta que se presenta, puedan hacer valer los estándares nacionales vigentes, así como emitir recomendaciones de carácter orientativo, sobre estándares y mejores prácticas internacionales para lograr dicho objetivo. Para lograr lo anterior, se deberá tomar en cuenta, la naturaleza y tipo de datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable. Lo anterior por su puesto, bajo estándares de neutralidad tecnológica. Asimismo y retomando la propuesta en ese particular del diputado Adolfo Mota, se añade que 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 interesados; la sensibilidad de los tratamientos, y el desarrollo tecnológico.

IX. Infracciones y sanciones:

Finalmente, la ley prevé un capítulo de infracciones que retoma conductas previstas por ambas iniciativas y añade otras que se consideraron por esta Comisión, como supuestos que se presentan en el tratamiento de datos y que consideramos deben ser sancionadas desde el apercibimiento hasta la imposición de multas máximas, bajo un sistema de modulación de la penalidad, de acuerdo con la gravedad de las conductas. Al respecto, los montos de las sanciones fueron retomados de la iniciativa del diputado Gustavo Parra, ya que se considera por un lado, que la ley debe desincentivar conductas contrarias a lo establecido por la misma, y por otro, al tratarse de un derecho fundamental reconocido a nivel constitucional, consideramos fehacientemente que debe garantizarse al ciudadano que una vez que ha sido conculcado su derecho, habrá una consecuencia para el responsable que actúo con negligencia o dolo en el debido tratamiento de su información, máxime cuando esta fuere sensible.

Por lo antes expuesto, los diputados integrantes de la Comisión de Gobernación, someten a la consideración del Pleno de esta Honorable Asamblea, el siguiente:

DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

ÚNICO.- SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES, PARA QUEDAR COMO SIGUE:

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 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 la presente Ley, las 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, quienes en lo relativo a la recolección, uso, divulgación y almacenamiento de los datos personales que intercambien con sus usuarios, y a las relaciones jurídicas entre éstos y aquellas, están reguladas por 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 principio de información a que se refiere el texto de la presente Ley

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

III. **Consentimiento:** Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. El consentimiento será expreso cuando se manifieste por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, incluido entre estos últimos el poner a disposición del titular el aviso de privacidad.

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

V. **Datos Sensibles:** La información concerniente a una persona relativa a su origen racial o étnico, estado de salud, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas o preferencia sexual;

VI. **Días:** Días hábiles;

VII. **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.

VIII. **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;

IX. **Instituto:** Instituto Federal de Acceso a la Información y Protección de Datos.

X. **Ley:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares;

XI. **Responsable:** Personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales sujetos a la presente Ley.

XII. **Secretaría:** La Secretaría de Economía, la cual es una Secretaría de Estado en términos de lo dispuesto por la Ley Orgánica de la Administración Pública Federal;

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

XIV. **Titular:** La persona física a quien corresponden los datos personales, y

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

Artículo 4. ****** Los son datos personales siguientes estarán protegidos bajo los nprincipios que establece esta Ley:

I. El nombre, puesto, dirección o teléfonos de trabajo de un empleado, prestador de servicios o miembro de una organización;

II. La información que una persona hace pública de forma deliberada, o permite que sea hecha pública, o que es obtenida de registros públicos, u otras fuentes accesibles al público en general de conformidad con las leyes.

III. La que es pública en términos de lo dispuesto en otras leyes.

Artículo 5. 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 6. A falta de disposición expresa en esta Ley, se aplicarán de manera supletoria las disposiciones contenidas en el Código Federal de Procedimientos Civiles y para efectos del procedimiento de protección de datos las contenidas en la Ley Federal de Procedimiento Administrativo.

CAPÍTULO II
De los Principios de Protección de Datos Personales.

Principios de protección de datos
Artículo 7. Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, proporcionalidad y responsabilidad, previstos en la Ley.

Principio de licitud
Artículo 8. 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 ilícitos, engañosos o fraudulentos.

En toda recolección o 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.

Principio del consentimiento

Artículo 9. Todo tratamiento de datos personales estará sujeto al consentimiento previo de su titular, el cual podrá manifestarse de forma verbal, escrita, a través de medios electrónicos, ópticos o de cualquier otra tecnología o a través de signos inequívocos de acuerdo a lo establecido por 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.

Consentimiento para datos sensibles

Artículo 10. Tratándose de datos sensibles, el responsable deberá obtener el consentimiento expreso 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 información que directa o indirectamente contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas y concretas.

Excepciones al consentimiento:

Artículo 11. No será necesario el consentimiento para la obtención de los datos personales cuando:

I. Esté previsto en una ley;

II. Sean necesarios para el mantenimiento o cumplimiento de una relación jurídica, de negocios, laboral o administrativa;

III. Sean necesarios para efectuar un tratamiento para la prevención o diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que el interesado 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;

IV. Los datos figuren en fuentes de acceso público y se requiera su tratamiento;

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

VI. Cuando así lo exija la resolución de una autoridad competente, y

VII. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes.

Principio de calidad

Artículo 12. El responsable procurará que los datos personales contenidos en las bases de datos sean correctos, consistentes 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.

Principio de finalidad

Artículo 13. El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades primarias y secundarias previstas en el aviso de privacidad.

La obtención y el tratamiento de los datos personales, deberá estar relacionado con la finalidad primaria puesta a disposición del titular. En el caso del tratamiento de datos personales que vayan a ser utilizados para finalidades secundarias, no se requerirá recabar el consentimiento del titular, siempre y cuando en el aviso de privacidad se incluyan dichos fines secundarios.

En aquellos casos en que el responsable pretenda tratar los datos para un nuevo fin secundario, que no resulte compatible o análogo a los fines establecidos en el aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular.

Principio de proporcionalidad

Artículo 14. El tratamiento de datos de carácter personal será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el artículo anterior. En particular para datos sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de conservación de los datos de carácter personal para que el tratamiento sea el mínimo necesario.

Principio de responsabilidad

Artículo 15. El responsable velará por el cumplimiento de los principios de protección de datos 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, será respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.

Principio de información

Artículo 16. 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.

Aviso de privacidad

Artículo 17. 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. Cualesquiera opciones y medios que el responsable ofrezca a los titulares para limitar el uso, divulgación de los datos, o ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley, y

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

Modalidades del aviso de privacidad

Artículo 18. El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otro, de la siguiente manera:

I. Cuando los datos hayan sido obtenidos directamente del titular, el aviso 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;

II. De igual forma, en recolecciones efectuadas por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología el aviso de privacidad debe proporcionarse de manera resumida en el momento de la recolección, poniendo a disposición el texto del aviso completo.

Artículo 19. 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 una Ley expresamente lo prevea, cuando el tratamiento sea con fines históricos, estadísticos o científicos, o cuando dar a conocer el aviso de privacidad al titular resulte imposible o exija esfuerzos desproporcionados, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Medidas de seguridad

Artículo 20. 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 por daño, pérdida, alteración, destrucción o el uso, acceso o divulgación no autorizado. El Instituto divulgará estándares y mejores prácticas internacionales en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable.

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 interesados; la sensibilidad de los tratamientos, y el desarrollo tecnológico.

Vulneraciones de seguridad

Artículo 21. 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 por el responsable al Instituto y al titular, a fin de que éste último tome las medidas correspondientes.

Deber de secreto

Artículo 22. 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

Sección I
De los Derechos de los Titulares de Datos Personales.

Derechos ARCO

Artículo 23. 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. La procedencia de estos derechos, en su caso, se hará efectiva una vez que el interesado o su representante legal acrediten su identidad o representación, respectivamente. Los datos personales deben ser almacenados de tal manera, que permitan el ejercicio de los derechos mencionados en este artículo.

Derecho de acceso

Artículo 24. Los titulares tienen derecho a obtener sus datos personales que obran en poder del responsable, así como a tener acceso al aviso de privacidad al que está sujeto el tratamiento.

Derecho de rectificación

Artículo 25. El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos, siempre que no sea imposible o exija esfuerzos desproporcionados al responsable.

Derecho de cancelación

Artículo 26. El titular tendrá en todo momento el derecho a cancelar sus datos personales.

La cancelación da lugar al bloqueo del dato por un periodo en el que el responsable lo conservará para efectos de responsabilidades y durante el cual no podrá darse tratamiento alguno al dato. El periodo de conservación precautoria será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en términos de la normatividad aplicable. Cumplido el periodo anterior, deberá procederse a la supresión del dato, que implica el borrado o eliminación del mismo.

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 rectificación o cancelación, para que proceda a efectuarla.

Excepciones al derecho de cancelación

Artículo 27. 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. 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 o por otra persona con un deber equivalente al del secreto;

III. Deban ser tratados por disposición legal;

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

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

VI. Sean necesarios para realizar una acción en función del interés público, y

VII. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular.

Derecho de oposición

Artículo 28. El titular de los datos tendrá derecho a oponerse al tratamiento de los mismos, en el supuesto de que no los hubiere proporcionado al responsable y la Ley no disponga lo contrario. De actualizarse tal supuesto, el responsable deberá excluir del tratamiento los datos relativos al titular.

Sección II
De la Transferencia de Datos

Transferencia de datos

Artículo 29. Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros, deberá comunicar a éstos su aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

El contrato respectivo incluirá una cláusula que prevea que el tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad. El tercero receptor de los datos personales, quedará sujeto a las mismas obligaciones que corresponden al responsable que los transfirió.

Artículo 30. 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 o 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 para la celebración 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 IV
Del ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición

Inicio del procedimiento

Artículo 31. El titular o su representante legal podrán presentar ante el responsable una solicitud de acceso, rectificación, cancelación u oposición, respecto de los datos personales que le conciernen.

Requisitos para el ejercicio de los derechos ARCO

Artículo 32. 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, como el correo electrónico;

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

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 33. Todo responsable deberá designar a una persona, o departamento de datos personales, el cual recibirá, dará trámite y registrará las solicitudes de los titulares y las notificaciones efectuadas por el Instituto, para el ejercicio de los derechos a que se refiere el artículo anterior. Asimismo, fomentará la protección de datos personales al interior de la organización.

Artículo 34. El responsable comunicará al titular, en un plazo máximo de veinte días contados desde la presentación de 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 35. 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 la información solicitada ya esté disponible al público en medios impresos, tales como libros, compendios, trípticos, archivos públicos, en formatos electrónicos disponibles en Internet o en cualquier otro medio, se le hará saber al solicitante por escrito o por medios electrónicos la fuente, el lugar y la forma en que puede consultar, reproducir o adquirir dicha información.

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 primero de este artículo, para tener por cumplida la solicitud.

Negativa al ejercicio de derechos ARCO
Artículo 36. 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 si una parte de los datos solicitados no encuadra en alguna de las causales antes citadas, 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.

Solicitud de Rectificación

Artículo 37. 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.

Entrega gratuita de datos personales

Artículo 38. 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 3 días de salario mínimo general vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas.

Artículo 39. 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 siguiente capítulo.

CAPÍTULO V
Del Procedimiento de Tutela de Derechos

Disposiciones Generales

Inicio del procedimiento

Artículo 40. 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 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 y manifieste lo que a su derecho convenga.

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 aquellos 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 solicitud de protección de datos personales, considerando la presentación de pruebas y alegatos, la celebración de audiencias y el cierre de instrucción.

Requisitos para la interposición de la solicitud de protección de datos

Artículo 41. 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 los siguientes datos:

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. La dirección para oír y recibir notificaciones;

IV. La fecha en que se le dio a conocer la respuesta del responsable, salvo que el recurso se interponga 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 establecerá 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.

Plazo máximo para dictar resolución
Artículo 42. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de 50 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.

Plazo para que el responsable haga efectivo el derecho
Artículo 43. En caso que la resolución de tutela 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 la tutela, debiendo dar cuenta por escrito de dicho cumplimiento al Instituto dentro de los siguientes diez días.

Prevención
Artículo 44. En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere el artículo 41 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.

Suplencia de la queja
Artículo 45. 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.

Efectos de las resoluciones
Artículo 46. 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.

Causales de desechamiento

Artículo 47. La solicitud de protección de datos será desechada por improcedente cuando:

I. Sea extemporánea;

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. El Instituto no sea competente;

IV. Por tratarse de una solicitud de protección de datos ofensiva, frívola o irracional;

V. 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, o

VI. Por desistimiento expreso del titular de los datos.

Causales de sobreseimiento

Artículo 48. La solicitud de protección de datos será sobreseída cuando:

I. Por cualquier motivo quede sin materia la misma;

II. El titular fallezca, o

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

Conciliación

Artículo 49. 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.

Procedimiento en caso de falta de respuesta

Artículo 50. 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.

Medios de defensa contra las resoluciones del Instituto

Artículo 51. Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

Publicidad de las resoluciones

Artículo 52. Todas las resoluciones del Instituto serán susceptibles de difundirse públicamente en versiones públicas, eliminando aquellas referencias al titular de los datos que lo indentifiquen o lo hagan identificable.

Artículo 53. Si con motivo del desahogo del procedimiento que se regula en el presente apartado o derivado de una verificación que realice el Instituto, éste tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, distinta de las relativas al ejercicio de los derechos de acceso, rectificación, cancelación u oposición, iniciará la investigación correspondiente a efecto de determinar la sanción que corresponda.

Derecho a indemnización

Artículo 54. 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 VI
De las Autoridades

Sección I
Atribuciones del Instituto

Artículo 55. 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 velar 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 56. El Instituto tiene las siguientes atribuciones:

I. Interpretar en el ámbito administrativo la presente Ley;

II. Conocer y resolver los procedimientos de tutela de derechos señalado en esta Ley e imponer las sanciones según corresponda;

III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;

IV. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley mediante el procedimiento que se establezca en el Reglamento. Para ello podrá solicitar y conocer en todo momento, la información que resulte necesaria para la observancia de este ordenamiento, en el ámbito de su competencia, con las excepciones previstas por la legislación;

V. Emitir los criterios, recomendaciones y normas técnicas de conformidad con las disposiciones aplicables en materia de esta Ley;

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

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

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

IX. 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;

X. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en posesión de particulares y brindar capacitación a los sujetos obligados;

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

Sección II
De las Autoridades Reguladoras

Emisión de regulación secundaria
Artículo 57. La presente ley y su Reglamento constituirán el marco de referencia que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, previa opinión del Instituto.

De la Secretaría de Economía
Artículo 58. 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 59. 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 60. La Secretaría tiene las siguientes atribuciones:

I. Establecer las políticas públicas en el ámbito de su competencia en materia de datos personales como insumo del comercio y la economía digital;

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

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

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

V. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad a que se refiere la presente ley;

VI. Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 61 de la presente Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, previa opinión del Instituto;

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;

X. Emitir opinión sobre asuntos vinculados con la protección de los datos personales en el ámbito de su competencia;

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

XII. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 57, y

XIII. Verificar y vigilar el cumplimiento de las leyes, acuerdos o tratados comerciales internacionales, decretos, reglamentos, y demás ordenamientos generales de su competencia en materia de protección de datos personales.

Mecanismos de autorregulación

Artículo 61. Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles y gubernamentales, o ambas, nacionales o extranjeras, esquemas de autorregulación en la materia, que complementen lo dispuesto por la presente Ley.

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
De las Infracciones y Sanciones

De las infracciones

Artículo 62. 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 17 de esta Ley;

VI. Incumplir el deber de confidencialidad establecido en el artículo 22 de esta Ley;

VII. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 13;

VIII. Transmitir 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;

IX. 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;

X. Incurrir en una vulneración de seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

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

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

XIII. Obstruir los actos de verificación de la autoridad;

XIV. Recabar datos en forma engañosa y fraudulenta;

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

XVI. Tratar los datos personales cuando con ello se afecte el ejercicio de los derechos establecidos por la Constitución;

XVII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 63;

XVIII. Crear bases de datos en contravención a lo dispuesto por el Artículo 10, 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.

Sanciones

Artículo 63. 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 2000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II, III, IV, V, XVII y XIX del artículo anterior;

III. Multa de 200 a 5,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV, XVI y 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 300 a 10,000 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 64. 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 65. Las sanciones que se señalan en este capítulo, se impondrán sin perjuicio de la responsabilidad civil o penal que resulte.

Artículo 66. Los ingresos que la Federación obtenga efectivamente de multas por infracción a esta Ley, se destinarán al Instituto para el desarrollo de procedimientos de verificación del cumplimiento de esta Ley, la elaboración y publicación de estudios e investigaciones para difundir y ampliar el conocimiento en materia de datos personales, así como a la capacitación en la materia.

Sólo ingresarán a los citados fondos el importe de las multas efectivamente pagadas y que hubieren quedado firmes. La distribución de los fondos se hará en los términos que el Reglamento de esta Ley señale.

TRANSITORIOS

ARTÍCULO PRIMERO. La presente Ley entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.

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

ARTÍCULO TERCERO. Los Titulares podrán ejercer ante los Responsables sus derechos de acceso, rectificación, cancelación y oposición contemplados en el Capítulo IV de la presente Ley; así como dar inicio, en su caso, al procedimiento de tutela de derechos establecido por el Capítulo V de la misma, tres años después de la entrada en vigor de la Ley.

ARTÍCULO CUARTO. Las autoridades a que se refiere el artículo 57 de esta Ley emitirán la regulación secundaria que resulte indispensable para el cumplimiento de la misma, a más tardar, dos años después de la entrada en vigor de la presente Ley.

ARTÍCULO QUINTO. Los responsables designarán a la persona o departamento de datos personales a que se refiere el artículo 33 y expedirán sus avisos de privacidad a los titulares de datos personales de conformidad a lo dispuesto por los artículos 17 y 18 a más tardar 1 año después de la entrada en vigor de la presente Ley.

ARTÍCULO SEXTO. Se abrogan las leyes en materia de protección de datos personales en posesión de particulares que se hubieren expedido, y se derogan las demás disposiciones que se opongan a la presente Ley.

ARTÍCULO SÉPTIMO. Los presupuestos de egresos de la Federación que correspondan, deberán establecer las previsiones presupuestales necesarias para el cumplimiento de la presente Ley, en los plazos señalados en las disposiciones anteriores,

PALACIO LEGISLATIVO DE SAN LÁZARO.- MÉXICO, DISTRITO FEDERAL, A VEINTIOCHO DE ABRIL DE DOS MIL NUEVE.