"Revolución Informática con Independencia del Individuo"

LA NUEVA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES: PROS Y CONTRAS

Myrna Elia García Barrera[688]

Julio Téllez Valdés

En nuestro país, se ha incorporado a nuestra Constitución dos nuevos derechos fundamentales, por un lado el derecho de acceso a la información y por el otro, la protección de datos personales, primero en posesión de sujetos públicos y ahora en posesión de particulares; dichos derechos se encuentran entre sí, porque los bienes jurídicos protegidos del acceso a la información son la transparencia y la rendición de cuentas, y los de la protección de datos personales son la privacidad y la intimidad.

El uso de las TIC-tecnologías de la información y las telecomunicaciones ha permitido que en meeuchas ocasiones los datos personales sean utilizados para fines distintos para los que originalmente fueron recabados, y más son transmitidos a instancias o a personas distintas a las que el dueño o titular de los datos confió o entregó; lo que viola la esfera de privacidad de la persona y, en ocasiones, lesiona otros derechos y porque pueden cometerse una serie de delitos, tales como robo de identidad.

Con el fin de equilibrar, los ya mencionados bienes jurídicos de privacidad e intimidad, entre toda persona y aquellas organizaciones públicas o privadas que recaban o colectan datos personales, surgió el concepto de autodeterminación informativa o la protección de los datos personales en Europa y en Iberoamérica; cambio en Estados Unidos, un concepto similar, el concepto de privacidad, con alcances distintos, pero con el mismo fin.

Bajo el concepto de protección de datos personales, el titular o dueño de dichos datos tiene el derecho y la libertad de elegir qué desea comunicar, cuándo y a quién, y sobre todo debe mantener el control sobre su información personal.

Con la aprobación, en 2008, de las reformas a los artículos 16 y 73 constitucionales que se introduce, como ya señalamos a nuestra Constitución, el derecho de toda persona a la protección de su información, de sus datos personales.

El artículo 16 Constitucional reconoce y regula el derecho a la protección de datos personales, porque en la reforma se plasman los derechos de acceso, rectificación,

---

[688] INVESTIGADORA SNI nivel 1. Doctora en Derecho egresada de la Facultad Derecho y Criminología de la UANL. Investigadora en el Centro de Investigación de Tecnología Jurídica y Criminológica de la Facultad Derecho y Criminología de la UANL., y Catedrática de la propia Facultad de Derecho y Criminología de la UANL y de la Universidad de Monterrey.

cancelación y oposición, denominados en la doctrina, 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. La reforma consistió en añadir un segundo párrafo que a la letra dice:

"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".

Ahora bien, el 27 de abril de 2010, se aprobó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y fue publicada el 5 de julio de 2010, en la misma se señala que los datos personales constituyen la información inherente a un individuo, o mejor dicho a una persona física, la cual puede referirse a datos de identificación, patrimoniales, académicos y de salud, entre otros. Esta información debe ser tratada con sumo cuidado, ya que la propagación arbitraria de la misma y sin el consentimiento de su titular, puede traer consecuencias que podrían afectar de diversas formas a la propia persona, invadiendo su privacidad y hasta su intimidad.

Todos los datos que brindamos en el desenvolvimiento de nuestra vida y aquellos que surgen de la interacción con terceros, relacionados con nuestra persona, van conformando un perfil querido no de nuestras actividades, de nuestros gustos, de nuestras situaciones pasadas y presentes. Cualquiera que tenga acceso a los mismos puede tener un panorama global de una u otra persona.

Los datos personales se definen como "toda información concerniente o relativa a una persona física identificada o identificable."[689] Ahora bien, los datos personales y su protección están íntimamente ligados con lo que se conoce como el derecho a la intimidad.

Así, la intimidad[690] es un rasgo ontológico de la persona cuya relevancia jurídica es evidente, pues se trata, de un aspecto muy importante en el desarrollo de la personalidad que repercute directamente en la convivencia, pues ésta sería imposible entre personas que proyectan su vida desde la alteración permanente.

---

[689] Ornelas Lina, "Obligaciones del Estado en materia de Protección de Datos Personales", Instituto Federal de Acceso a la Información, en:
http://www.senado.gob.mx/comisiones/LX/cyt/content/seminarios/tecnologias/Lina_Ornelas.pdf
(18 de octubre de 2010).

[690] De Domingo Pérez, Tomás. 2001 *¿Conflicto entre derechos fundamentales? Un análisis desde las relaciones entre los derechos a la libre expresión e información y los derechos al honor y a la intimidad.* Madrid, España. Centro de Estudios Políticos y Constitucionales. Página 275.

De lo anterior podemos considerar que si los datos personales están íntimamente relacionados con la intimidad, y siendo que esta última posee una relevancia jurídica debido a que repercute en la convivencia de las personas, de ahí que la divulgación arbitraria por parte del Estado, o cualquier otro ente público, y de los entes privados, de los datos personales de un particular, persona física o moral, podrían traer consigo consecuencias jurídicas.

De la misma forma, el concepto de privacidad incluye el derecho fundamental del individuo a determinar cómo se utiliza su información personal.[691]

¿Cómo se afecta la intimidad con la recopilación de datos personales, por parte de los entes públicos y privados? En primer lugar hay que tener en cuenta que esta información se recopila en la mayoría de los casos sin el consentimiento del titular o dueño de los datos. Cabe aclarar que el otorgamiento de esa información por parte de sus titulares no significa autorizar su uso para otros fines, aunque ello sí suceda en la práctica.

Existen diversos instrumentos internacionales que protegen el derecho a la vida privada tales como la Declaración Universal de los Derechos Humanos, aprobada y proclamada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948, la cual en su artículo 12 establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataque."[692]

Esta violación a la privacidad se hace más patente con el nacimiento de las autopistas de la información, sobre todo con la existencia de redes de computadores que ofrecen información, los sitios que se recorren en la *Web*, los datos que se consultan y los bienes o servicios que se adquieren, etc., y como señala Luhmann:[693] "Parece que así la sociedad moderna haya alcanzado un límite en el cual no hay nada incomunicable,....". Esta nueva amenaza, generará sin duda alguna, un nuevo enfoque para regular el manejo de datos personales en posesión de entes públicos y de los particulares.

La intimidad entendida como una esfera del individuo en la que éste puede desenvolverse sin sufrir injerencia de ninguna especie, es un derecho personalísimo que ha evolucionado a través del tiempo. Ahora en esta nueva sociedad informacional, el derecho a la intimidad[694] protege una zona espiritual íntima, o sea, un reducto personal y

---

[691] Ornelas, Lina. *Loc. cit.*

[692] *Declaración Universal de los Derechos Humanos.*, (Documento web), Asamblea General de las Naciones Unidas, 10 de diciembre de 1948 en: http://www.un.org/spanish/aboutun/hrights.htm (18 de octubre de 2010).

[693] Luhmann, Niklas y Raffaele De Georgi. 1993. *Teoría de la Sociedad.* Universidad de Guadalajara. Universidad Iberoamericana. Instituto Tecnológico y de Estudios Superiores de Occidente. México. Página 125.

[694] Fernández Rodríguez, José Julio. 2004. *Lo público y lo privado en Internet.* Intimidad y libertad de expresión en la red, Editorial Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica. No. 154. UNAM. México. Páginas 97 a 99.

privado frente a posibles agresiones exteriores y frente al conocimiento de los demás, y debe ser garantizado por un poder jurídico sobre la información relativa a una persona o a su familia, imponiendo a terceros y a los propios poderes públicos la obligación de que dichas personas manifiesten su voluntad de no dar a conocer dicha información o, mejor dicho, prohibiendo la difusión de una información no consentida, porque el respecto a la dignidad de la persona es la base fundamental de la protección de datos personales.[695]

Entonces, la protección de datos personales es un derecho personalísimo que permite sustraer a la persona de la publicidad o de otras turbaciones de su vida privada, el cual está limitado por las necesidades sociales y los intereses públicos.

También, es aquel derecho que garantiza a su titular el desenvolvimiento de su vida y de su conducta dentro de un ámbito privado, sin injerencias ni intromisiones que puedan provenir de la autoridad o de terceros, y en tanto dicha conducta no ofenda al orden y a la moral pública, ni perjudique a otras personas.

"Los avances tecnológicos han dado lugar a nuevas formas de agresión a la intimidad y a la vida privada, en un elenco que no está, ni mucho menos cerrado y con una escala de gravedad diversa. Así podemos citar:

La entrada en el disco duro de un ordenador sin consentimiento.

La elaboración de perfiles del navegante (constituidos en torno a su vida privada) con fines publicitarios u otros más graves.

La simple acumulación o registro de datos sin consentimiento.

El empleo de una dirección IP asignada a otro ordenador.

La intercepción de mensajes de correo electrónico y de las comunicaciones en general (leyendo y/o modificando su contenido).

La suplantación de personalidad de un usuario o de la identidad de una computadora.

El hostigamiento electrónico.
El uso indebido de directorios de correos electrónicos o listas de usuarios.
La alteración o destrucción de información.
El impedimento para acceder a la información (interrupción del servicio).

---

[695] Diputado Luis Gustavo Parrra Noriega. Avances y Retos en la Legislación en materia de Protección de Datos Personales *"Avances y Propuestas Legislativas en materia de Protección de Datos Personales"* 25 de febrero de 2009.
http://www3.diputados.gob.mx/camara/content/download/210061/515613/file/DIP.%20LUIS%20GUSTAVO%20PARRA%20NORIEGA.ppt (21 de marzo de 2010).

El acceso a la cuenta del administrador."[696]

Antes de la reforma del artículo 6º Constitucional,[697] la protección de datos personales no estaba nominada en nuestra Constitución, había autores que interpretaban que en el propio artículo 16 Constitucional, claro antes de la reforma, estaba regulada al señalar: "*Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud del mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*" Por lo que, se presumía que se abarcaba la protección de datos personales y la intimidad.

Ahora bien, con la reforma, y con la del artículo 6, que señala:

"*Para el ejercicio del Derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: I. Toda información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. II. La información que se refiere a la ida privada y los datos personales será protegida en los términos y las excepciones que fijen las leyes. III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos. IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión. V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos. VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales. VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en términos que dispongan las leyes.*"

Ha quedado regulada la protección literal sobre la información relativa a la vida privada y sobre los datos personales, en su fracción II. "La información a que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes." En posesión de sujetos públicos obligados.

Además, la de reforma del artículo 16 Constitucional, regula la protección de datos personales en posesión de particulares, agrega un párrafo como sigue:

---

[696] Fernández Rodríguez, José Julio. *Op. Cit.* Páginas 99 y 100.
[697] Decreto publicado el 20 de julio de 2007.

"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."

El titular de los datos personales tendrá derecho a oponerse al tratamiento de sus datos personales, en el supuesto de que éstos se hubiesen recabado sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario. De actualizarse tal supuesto, el responsable deberá excluir del tratamiento, los datos relativos al interesado.

Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables.

La solicitud de acceso, rectificación, cancelación u oposición deberá contener:

I. El nombre del solicitante y domicilio u otro medio para recibir notificaciones, como el correo electrónico, así como los datos generales de su representante, en su caso;

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

III. Cualquier otro elemento que facilite la localización de la información; y

IV. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser mediante consulta directa, copias simples, certificadas o cualquier otro medio.

En el caso de solicitudes de rectificación de datos personales, el interesado deberá indicar, las modificaciones a realizarse y aportar la documentación que sustente su petición.

Tratándose de solicitudes de cancelación, la solicitud deberá indicar si revoca el consentimiento otorgado, de manera expresa.

En el caso de las solicitudes de oposición deberá manifestar los motivos fundados para tal determinación de dicha oposición. Otra de las razones que justifica la existencia del derecho de oposición es que se emplea como una herramienta para combatir determinaciones basadas únicamente en un tratamiento automatizado de datos destinado a evaluar ciertos aspectos relativos a la personalidad, como el rendimiento laboral, fiabilidad, conducta, entre otros."[698]

---

[698] *Dictámenes de Discusión de la Comisión de puntos constitucionales con proyecto de decreto que adiciona un*

Respecto a los niveles de seguridad de datos personales se deberá elaborar un documento que establezca las medidas de seguridad físicas, técnicas y administrativas adoptadas para cada sistema de datos personales que posean, las cuales garanticen el nivel de seguridad adecuado, de conformidad al tipo de datos contenidos en dichos sistemas y con base en los estándares internacionales de seguridad y sobre todo darlos a conocer al titular de los datos personales.

El documento de seguridad deberá incluir el nombre y cargo de los responsables de los tratamientos de datos personales.

Las medidas de seguridad deberán establecerse atendiendo a la siguiente clasificación:[699]

A los sistemas de datos personales que contienen alguno de los datos que se enuncian a continuación deberán aplicarse las medidas de seguridad de nivel básico:

Datos de identificación: Nombre, domicilio, número de teléfono particular, número de teléfono celular, dirección de correo electrónico, estado civil, firma, firma electrónica, Registro Federal de Contribuyentes, Clave Única de Registro de Población, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, nombres de familiares dependientes y beneficiarios, fotografía, idioma o lengua, entre otros.

Datos laborales: Documentos de reclutamiento y selección, de nombramiento, de incidencia, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, teléfono institucional, actividades extracurriculares, referencias laborales, referencias personales, entre otros.

Los sistemas de datos personales que contengan alguno de los datos que se enuncian a continuación, además de cumplir con las medidas de seguridad de nivel básico, deberán observar las identificadas con nivel medio:

Datos patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, servicios contratados, referencias personales relacionadas con servicios financieros, entre otros.

Datos sobre procedimientos jurisdiccionales o administrativos seguidos en forma de juicio: Información relativa a una persona que se encuentre sujeta a un procedimiento

---

párrafo segundo al artículo 16 a la Constitución Política de los Estados Unidos Mexicanos, Gaceta Parlamentaria, Cámara de Diputados, número 2653-II, jueves 11 de diciembre de 2008 en: http://gaceta.diputados.gob.mx/Gaceta/60/2008/dic/20081211-II.html#Dicta20081211-2 (18 de octubre de 2010).

[699] Artículo 79 de la Ley de Transparencia y Acceso a la Información del Estado de Nuevo León, tomado del *Código modelo: Código de Buenas Prácticas y Alternativas para el Diseño de Transparencia y Acceso a la Información Pública en México*, www.ifai.org.mx.. (18 de octubre de 2010).

administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal o administrativa.

Datos académicos: Trayectoria educativa, títulos, cédula profesional, certificados y reconocimientos, entre otros.

Datos sobre tránsito y movimientos migratorios: Información relativa al movimiento de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Los sistemas de datos personales que contengan alguno de los datos que se enuncian a continuación, además de cumplir con las medidas de seguridad de nivel básico y medio, deberán observar las identificadas con nivel alto.

Datos ideológicos y religiosos: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.

Datos de salud: Estado de salud, historial clínico, alergias, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, intervenciones quirúrgicas, vacunas, consumo de sustancias tóxicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.

Características personales: Tipo de sangre, ADN, huella digital, u otros análogos.

Características físicas: Color de piel, color de iris, color de cabello, señas particulares, estatura, peso, complexión, discapacidades, entre otros.

Vida sexual: Preferencia sexual, hábitos sexuales, entre otros.

Origen: Datos sobre el origen étnico y racial.

Los sujetos obligados al tratar sistemas de datos deberán de observar los siguientes principios:

Consentimiento.

Información previa, (respecto a la finalidad de los ficheros a los titulares).

Licitud.

Calidad de la información.

Confidencialidad.

Seguridad.

Garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Contar con una autoridad independiente de control, como órgano garante de la protección de datos personales.

La seguridad, privacidad y confidencialidad son el desafío de la protección de datos personales. Hoy en día, las nuevas tecnologías llevan fuera de nuestros hogares las cosas más íntimas, como por ejemplo:

El personal de centros comerciales, conoce todos nuestros hábitos de consumo.

Nuestro banquero, conoce nuestra liquidez monetaria y capacidad económica.

El buro de crédito o las sociedades de información crediticia conocen nuestros créditos y su cumplimiento o incumplimiento.

Nuestro acreedor, conoce nuestros estados financieros y record crediticio.

Nuestro operador de internet, nuestros sitios preferidos.

Nuestro operador telefónico, nuestra agenda y el record de las llamadas recibidas y realizadas.

Nuestra universidad o centro de estudios, nuestros datos académicos.

Nuestro Estado y nuestro Municipio, conocen nuestros datos de identificación, crediticios, entre otros.

Por lo asentado anteriormente de manera enunciativa, más no limitativa, porque nos encontramos una infinidad de ejemplos, resulta necesario, reconocer un derecho a la protección de los datos personales, como ya hemos avanzado en nuestro país, incorporando en el texto constitucional, porque de esta manera se generara una certeza indiscutible del derecho: le brindaría seguridad y estabilidad a la protección de datos personales ahora en posesión de entes públicos como de particulares.

Por otro lado, la citada reforma contiene ciertas excepciones o limitaciones respecto a la protección de datos personales, tales como el hecho de que este respeto se encuentre en contraposición con otro derecho, de tal manera que se necesite una ponderación por parte del juzgador de manera que prevalezca el bien común. Concretamente dichas excepciones son los casos en que se pudiera afectar la seguridad nacional, el orden, seguridad y salud públicos, o que se requiera proteger los derechos de terceros.

Al respecto debemos analizar la definición de seguridad nacional. La Ley de Seguridad Nacional, en el artículo 3, señala que:

Artículo 3.- Para efectos de esta Ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:

I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país;

II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;

III. El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;

IV. El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

V. La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y

VI. La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes. [700]

Es clara la excepción señalada, referente a que la protección de datos personales no podrá afectar la seguridad nacional. Ahora bien, respecto a la seguridad pública,[701] la misma se conceptualiza como una cualidad de los espacios públicos y privados, caracterizada por la inexistencia de amenazas que socaven o supriman los bienes y derechos de las personas, y en la que existen condiciones propicias para la convivencia pacífica y el desarrollo individual y colectivo de la sociedad.

En cambio, salud pública,[702] se define como un derecho subjetivo público, el cual tiene como obligación correlativa a cargo del Estado, la consistente en preservar la salud pública y la todos los individuos que componen la colectividad.

El orden público consistirá, por su parte, en el arreglo, sistematización o contraposición de la vida social con vista a la determinada finalidad de satisfacer una

---

[700] *Ley de Seguridad Nacional.* México. 31 de enero. 2005. última reforma publicada en el DOF: 26 de diciembre. 2008. en: http://www.cddhcu.gob.mx/LeyesBiblio/pdf/LSegNac.pdf
21 de marzo de 2010).

[701] García Ramírez, Sergio. *En torno a la seguridad pública. Desarrollo penal y evolución del delito. Cit. por* Arellano Trejo Efrén. "Definición". en Seguridad Pública, (Documento web), Centro de Estudios Sociales y de Opinión Pública. Febrero. 2006. en: http://archivos.diputados.gob.mx/Centros_Estudio/Cesop/Comisiones/dtseguridad%20publica1.htm
(21 de marzo de 2010).

[702] Burgoa Orihuela, Ignacio. 1984. *Diccionario de Derecho Constitucional Garantías y Amparo.* Editorial Porrúa. México. Páginas 392 y 393.

necesidad colectiva, a procurar un bienestar público o a impedir un mal al conglomerado humano.[703]

Del recuento anterior podemos resaltar que para que exista el orden público en una norma se requiere que su fin último sea el de satisfacer una necesidad colectiva, procurar un bienestar público o impedir un mal al conglomerado humano, lo cual prevalecerá ante la protección de datos personales.

Como se señalamos previamente, se deben reconocen los principios que rigen la protección de los datos personales a saber: los de consentimiento, información previa, licitud, calidad de la información, confidencialidad y seguridad.

El principio del consentimiento es el eje fundamental a partir del cual se ha construido el derecho a la protección de los datos personales, y conlleva la idea de la autodeterminación informativa. Implica que todo tratamiento de datos personales requiere ser autorizado previamente por el titular de éstos últimos. En este sentido, la manifestación de la voluntad por parte del titular de los datos deberá ser libre, informada y especifica.

El segundo de los principios es el de información, que supone que el responsable del tratamiento de los datos tiene la obligación de dar a conocer a su titular la existencia del tratamiento, los fines de éste, así como la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición. Del cabal cumplimiento de este principio depende que el consentimiento sea válido, pues de no conocerse de manera precisa los alcances del tratamiento, aquél puede considerarse como invalido.

El tercer principio es el de calidad. Éste propone que los datos recabados deben ser adecuados, exactos, pertinentes y no excesivos, según sea la finalidad para la que fueron recabados.

Por su parte, el principio de licitud consiste en que las entidades gubernamentales sólo deben desarrollar o tener sistemas de datos personales relacionados directamente con sus facultades y atribuciones. La posesión de sistemas de datos personales que no estén directamente relacionados con las atribuciones de una entidad gubernamental violenta directamente este principio.

El principio de confidencialidad establece que los sujetos obligados deben asegurar el manejo confidencial de los sistemas de datos personales, y que su transmisión o divulgación solamente puede darse previo consentimiento del titular.

El principio de seguridad conlleva la obligación de quien recaba los datos de adoptar las medidas de carácter técnico y organizativo que aseguren un tratamiento seguro. En esta materia se reconoce que no todos los datos personales requieren del mismo grado de seguridad, por lo cual pueden establecerse diferentes niveles. Así por ejemplo, los datos de identificación de una persona como el domicilio, el número

---

[703] *Ibid.* Página 326.

telefónico, el RFC, o la fecha de nacimiento requieren de un nivel de protección bajo, a diferencia de los datos sensibles, que son aquéllos relacionados con las preferencias ideológicas, religiosas, la vida sexual o la salud, que necesitan un nivel de protección alto.

Es menester conocer la evolución de estos derechos fundamentales:[704] La primera generación de normas que regularon este derecho se contiene en la Resolución 509 de la Asamblea del Consejo de Europa sobre derechos humanos y nuevos logros científicos y técnicos.

La segunda generación se caracteriza por la materialización del derecho de referencia en leyes nacionales. En ese sentido, en 1977 era aprobada la Ley de Protección de Datos de la entonces República Federal Alemana. En 1978 corresponde el turno a Francia mediante la publicación de la Ley de Informática, Ficheros y Libertades. 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).

Durante los años ochenta hacen su aparición los instrumentos normativos que conforman la tercera generación, caracterizados por la aparición de un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como por la irrupción de las exigencias de las medidas de seguridad por parte de los responsables de los sistemas de datos personales. Es en esta década cuando desde el Consejo de Europa se dio un respaldo definitivo a la protección de los datos personales 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.

Cabe mencionar que la protección de datos personales y el acceso a la información son derechos fundamentales complementarios y que, en nuestra legislación, tanto federal como local se protegió primeramente el derecho de acceso a la información, o sea el derecho a la publicidad, sin proteger debidamente el derecho a la privacidad, si, como expusimos con antelación, ya tenemos la publicación de la Ley Federal de Protección de Datos Personales en posesión de particulares, para poder garantizar a toda persona sus derechos de acceso, rectificación, cancelación y oposición, respecto a los datos personales en posesión de entes privados y su órgano garante es el IFAI, ahora Instituto Federal de Acceso a la Información y de Protección de Datos Personales.

---

[704] *Dictámenes de Discusión de la Comisión de puntos constitucionales con proyecto de decreto que adiciona un párrafo segundo al artículo 16 a la Constitución Política de los Estados Unidos Mexicanos*, Gaceta Parlamentaria, Cámara de Diputados, número 2653-II, jueves 11 de diciembre de 2008 en: http://gaceta.diputados.gob.mx/Gaceta/60/2008/dic/20081211-II.html#Dicta20081211-2

(20 de marzo de 2010).

Ahora las atribuciones del nuevo IFAI, serán: Proteger los datos personales en posesión de particulares. Elaboración y difusión de estudios, investigaciones y programas que promuevan la protección de datos personales. Emitir el Reglamento, teniendo un plazo de un año y medio contados a partir de la publicación de la Ley. Vigilar y verificar el cumplimiento de las disposiciones contenidas en la Ley. Procurar la solución de las diferencias entre los titulares de datos personales y los particulares. Conocer y resolver los procedimientos de Declaración de Infracción Administrativa y de los Recursos de Revisión y lo más importante, imponer sanciones por incumplimiento de la propia Ley.

Ahora bien, seguimos teniendo el gran problema de la dispersión del marco legal en materia de protección de datos personales, por tener las dos reformas constituciones y por tener la protección de datos personales en posesión de entes públicos en la Ley de Transparencia y Acceso a la Información Pública Gubernamental y en las 32 leyes de Transparencia de las Entidades Federativas.

Hemos avanzado y debemos sentirnos muy orgullosos, porque a protección de datos personales es un tema con plena vigencia e importancia en las sociedades democráticas, porque la apropiación y el uso irrestricto de los datos personales por parte del Estado y otras entidades públicas y privadas, chocan directamente con el derecho de los individuos a mantener una zona de su personalidad alejada del escrutinio público, la zona más intima o privada de la persona.

CONTRAS

Esta Ley Federal de Protección de Datos Personales en Posesión de los Particulares publicada en el Diario Oficial de la Federación en México el 5 de julio de 2010 es notoriamente tardía, considerando que desde finales de los sesentas la ONU advertía sobre las probables amenazas derivadas del uso inadecuado de las computadoras a efecto de obtener beneficios propios o ajenos en detrimento de los intereses de terceras personas y de que la primera ley de datos personales data de 1970 (en este caso en el estado alemán de Hesse).

En México, a pesar de los niveles de informatización con implicaciones técnicas, sociales y económicas por mencionar solo algunas, los intereses empresariales y políticos, aunados al desconocimiento de las personas, propiciaron este "retardo" en cuanto la emisión de una ley en la materia y ahora "que se tiene", no deja de revestir matices tangenciales, comenzando porque solo se refiere a los archivos privados (en este caso en posesión de los particulares) dejando al descubierto el manejo inadecuado de los llamados archivos públicos.

Desde su denominación, esta ley es poco afortunada ya que la acepción "en posesión de los particulares" es francamente poco clara y si revisamos más allá nos encontramos con concepto poco claridosos como los del artículo 1 que mencionan un tratamiento "legítimo, controlado e informado"

Otras inconveniencias lo son las llamadas bases de datosen cuanto conjunto "ordenado" (art 3 fracción II), por otro lado, en materia de consentimiento, porque no

posibilitar a un representante legal y no limitar a esta figura exclusivamente para el ejercicio de los derechos propiamente dichos, lo que nos parece que esto atenta derechos elementales en materia de representación legal, por otro lado y derivado de la fracción IV de este mismo artículo, desata dudas porque no se habla de que el responsable debe ser una persona fisica o moral nacional, de carácter privado, en caso de estar domiciliado en el extranjero, como hacerle valer esta ley sin tratocar el elemental principio internacional de extraterritorialidad de las leyes, cabe decir que en materia informática es muy común obtener datos en forma automatizada sin que sepamos a ciencia cierta en donde se resguarda dicha información, lo cual en ocasiones se "resguarda" en el extranjero. De igual forma, y en el rubro de conceptos y de la ley en sí misma, debiera aclararse que esta ordenamiento se aplica indistintamente para archivos manuales, semiautomáticos o automatizados (ver fracción XIV).

En materia de revocación de consentimiento, el llamado "responsable" (denominación incompleta) es quien establece en el llamado aviso de privacidad los mecanismos y procedimientos para dicha revocación sin señalar parámetros o reglas mínimas a seguir (ver artículo 8 *in fine*).

Otros claroscuros de ésta ley, lo constituyen los siguientes puntos:

¿Porque hablar de consentimiento expreso y por escrito en el artículo 9°, si en el artículo anterior se mencionan las 3 modalidades igualmente validas, y en todo caso, porque obligar a que sea por escrito?

El artículo 10 f. IV nos parece ambiguo respecto la f. VI respecto a la obtención del consentimiento de un familiar o responsable legal del titular y en última instancia, se prescindiría del consentimiento como lo marca el precepto. Por su parte, la f. VI da cabida al eventual tratamiento de datos por parte de aseguradoras.

En el artículo 11 se menciona que el responsable "procurará", acaso implica ello una obligación legal adecuada? por otra parte, ¿qué se entiende por "pertinentes"? Asimismo, en lugar de cancelados quizás sería mejor hablar de "suprimidos" o "eliminados" cuando que en párrafos anteriores se habla de eliminación de información, por lo que las terminologías no son uniformes.

En el artículo 12, es muy vago al no aclarar que se entiende por fin análogo

En el artículo 13, el término "relevante" es irrelevante, ¿a que se refieren con esfuerzos "razonables"?. Sin duda una ambigüedad que puede generar usos inadecuados y en su caso dificultad en cuanto la aplicación de sanciones.

En el artículo 14, el responsable puede permitir el tratamiento de datos a un tercero sin notificarlo al titular, la pregunta es: ¿porqué?, esto notoriamente puede ser *invasivo*, y si ese tercero se encuentra en el extranjero, de qué modo el responsable podrá pedirle cuentas y por ende atender los eventuales reclamos por parte del titular, aún si en el artículo 3 se habla que puede ser extranjero.

En el artículo 15, pareciera que no se toma el parecer y por ende obtención del consentimiento por parte de los titulares, pudiendo el responsable "disponer" de los datos con el simple aviso de privacidad.

En el artículo 16, el aviso de privacidad debe aclarar taxativamente que la información estará resguardada en territorio nacional.

En el artículo 18, tampoco habla de un consentimiento por parte del titular

En el artículo 19, falta aclarar los casos en que la información se resguardara en territorio nacional y que dichas medidas sean efectivas, del más alto nivel de seguridad existente, tecnología más avanzada, etcétera, aunque el segundo párrafo trata de clarificar el punto, pero de manera muy desafortunada al mencionar como parámetro las medidas que se adoptan respecto a la propia información (¿y qué pasa si las medidas son nulas o deficientes?), en este caso debiera hablarse que deben ser del más alto nivel independientemente de las que se tengan para la propia información.

En el artículo 20, no queda claro quien valora que sean significativas y el que deben darse a conocer al titular todo tipo de "vulneración" para que él determine si adopta o no medidas.

Y del artículo 21, ¿que obligación tienen los terceros?, ¿en qué momento se le notificó al titular y éste autorizo su "participación"?.

En el artículo 22, ¿"cuál otro derecho"?, se refiere a los llamados derechos ARCO o alguno otro distinto?, en todo caso hay que explicitarlo. Por otro lado, ¿a qué se refieren que "los datos personales deben ser resguardados", quien haría y en qué términos este resguardo?, en el entendido que se está dando un manejo inadecuado de dichos datos por parte del responsable.

En el artículo 23, se habla de que los datos obren en poder del responsable y la ley habla de posesión, hay que aclarar el alcance de estos conceptos. Quizás previo a este derecho de acceso a los datos en sí mismos, el titular debiera tener el derecho de acceder a las instalaciones o conocer las políticas de privacidad, resguardo, seguridad con motivo de dichos datos.

Los artículos 24 y 25 deben hablar de un derecho exigible hacia el responsable para esa rectificación o cancelación, supresión o eliminación. El titular no puede hacerlo por sí mismo pero si dar la instrucción que se haga. No estaría por demás, decir que así como en la rectificación es por inexactos o incompletos, hablar que en la cancelación o supresión lo serán por "irrelevantes", aunque no haya necesidad de dar justificación alguna. Esa conservación, bloqueo y eventual transmisión a terceros, nos parece que por su relevancia, deben ser motivos de una mayor explicitación, y si fueron transmitidos al extranjero, en qué momento se le entero al titular y ¿cómo podrán hacerse efectivamente validos sus derechos?.

En el artículo 26, habría que aclarar algunos rubros, como el caso de la f. VII, en se podrían presentar posibles abusos por parte fundamentalmente de las aseguradoras.

Del artículo 27, parece necesario aclarar que se entiende por "causa legítima" para ejercer ese derecho de oposición.

En el capítulo IV de dicha ley, falta ser más preciso respecto al ejercicio de los derechos, sería conveniente reducir términos de respuesta y ejercicio de los derechos. Por su parte el artículo 33 segundo párrafo no parece muy "garante" respecto los derechos del titular, y puede prestarse a irregularidades

En el artículo 35 *in fine,* no queda claro que se entenderá por "solicitud de protección de datos".

Del artículo 36, habría que clarificar a que se refieren con "terceros nacionales" o "extranjeros distintos del encargado" y en su caso quien es el "encargado". En el *segundo párrafo* y distinto a lo establecido en artículos anteriores, se habla de las mismas obligaciones del "tercero receptor" respecto del responsable, pero ¿si fueron transmitidos al extranjeros, cómo podrían hacerse validos los derechos contemplados en una ley de un país distinto en donde se encuentran los datos?

Respecto el artículo 39, ¿cómo interpretar la fracción IX que faculta al IFAI a acudir a foros internacionales como atribución legal? ¿Acaso esto amerita ser un atribución a manera de "justificación legal" de continuos viajes?

El artículo 40, es poco claro respecto los rubros de archivos privados y no públicos.

Del artículo 42, ¿por qué no hacerlo extensivo también a archivos manuales o semiautomáticos?

Al parecer la premura de querer cumplir con el Segundo Transitorio del Decreto de Adición de la fracción XXIX-O del art 73 constitucional, motivo una redacción apresurada y poco cuidadosa.

Ante tantos vacíos legales y ambigüedades, pareciera que la emisión del Reglamento, así como la aplicación de los ordenamientos supletorios como el Código Federal de Procedimientos Civiles y la Ley Federal de Procedimiento Administrativo, así como los fallos judiciales, tendrían que subsanar todas estas problemáticas, cuando que es una elemental obligación en materia de técnica de redacción legislativa, considerar el mayor número de escenarios posibles presentes y futuros que puedan derivarse de la aplicación de una ley.

Y más grave aún, pareciera que esta Ley es insuficiente para instrumentar adecuadamente lo previsto en el artículo 16 párrafo segundo de nuestra Carta Magna (de la cual debiera ser una ley reglamentaria), dejando ésta labor a un Reglamento emanado del ejecutivo, vulnerando flagrantemente el llamado principio de "reserva de ley".

La *vacatio legis* de entrada en vigor de la ley es excesiva, así como la emisión del Reglamento correspondiente, pareciera como si no hay un verdadero ánimo de "recuperar" tiempo perdido en un tema tan delicado como esto, o como si se intentara seguir protegiendo intereses mezquinos que desean que no se regule este rubro, que se tarde en regular o que la regulación sea inadecuada

Finalmente, durante años hemos sostenido que el IFAI , al menos en los términos actuales y considerando sus casi ocho años de existencia se ha caracterizado por muy pobres logros , demasiado dispendio , estructura oligárquica, con comisionados poco preparados en el tema y algunos con exageradas ambiciones y compromisos políticos al grado de no terminar sus periodos de encargo con tal de "catapultarse" a otros puestos políticos como Secretarias de Estado, etcétera. Reconociendo filiaciones o simpatías partidistas y amistades con presidentes de la República en turno. Por otro lado, no existe algún tipo de consejo consultivo plural que represente a los distintos sectores interesados y sabedores en el tema que garantice una verdadera transparencia y efectividad en las actuaciones. En suma, habría que hacer una verdadera reestructuración del IFAI y no sólo cambiarle de nombre, en adecuaciones meramente cosméticas, o en su caso pensar en otra autoridad encargada de velar el cumplimiento de esta ley, y en caso de ser necesario crearla, dada la importancia del tema; de todos modos, las sanciones económicas, de por si excesivas y con un destino no adecuadamente clarificado, dando pauta a un autofinanciamiento, que evitaría considerar a dicho ente como un lastre.

Aunque deseamos que sea lo contrario, no podemos decir que vaya a ser una buena ley y desafortunadamente la autoridad no es la indicada porque tenemos duda si realmente quiere o sabrá cumplir su encomienda, sería una lástima que luego de tanto tiempo de espera en nuestro país, esto haya sido infructuoso dilapidando experiencias nacionales e internacionales en esta materia.

Cabe decir que en su momento, en el dictamen favorable a ésta ley en la Comisión de Gobernación de la Cámara de Diputados, se establece que la autoridad responsable de la protección de datos recaería en el entonces Instituto Federal de Acceso a la Información y Protección de Datos, partiendo de dos argumentos centrales:

La experiencia del IFAI en materia de protección de datos personales en posesión de entes públicos, y cuestiones de orden presupuestal.

Sin embargo, creemos que ambos argumentos son insuficientes, ya que por una parte, la referida experiencia de dicho Instituto es limitada y se tendría que partir prácticamente de la nada en cuanto a la aplicación del procedimiento administrativo sancionador que prevé la ley debido a que eventualmente se sancionaría a particulares, fundamentalmente empresas en donde el IFAI no tiene ningún grado de experiencia al respecto teniendo que crearse una estructura nueva dentro de dicha institución y capacitar los recursos humanos encargados del procedimiento administrativo sancionador. Por otra parte, el argumento de orden presupuestal resulta endeble, ya que se ha sostenido que existen limitaciones presupuestales para crear una autoridad nueva encargada de la protección de datos personales en posesión de particulares (v.gr; Agencia de Protección de Datos Personales en España), sin embargo, al determinar que sea el IFAI se le

tendrían que dotar de recursos presupuestales adicionales para crear la estructura administrativa necesaria para la aplicación de la ley, por tanto no existe argumentación lo suficientemente sólida para que se haya decidido que estas atribuciones recaigan en dicho Instituto, ya que bajo estos planteamientos, prácticamente lo mismo daría crear una nueva institución encargada de la protección de datos personales o bien delegarla a un organismo protector de los derechos humanos (de acuerdo a algunas experiencias internacionales), situaciones que por lo visto no se valoraron adecuadamente en su momento.

Finalmente, respecto los artículos transitorios, el artículo segundo señala que el Ejecutivo Federal expedirá el reglamento de la ley un año después de su entrada en vigor, por su parte, el artículo tercero establece que los responsables designarán a la persona o departamento de datos personales que dispone la ley a más tardar un año después de la entrada en vigor de dicha ley y por su parte, el artículo cuarto dispone que los titulares podrán ejercer ante los responsables sus derechos de acceso, rectificación, cancelación y oposición, así como el procedimiento de protección de derechos, en un plazo de *dieciocho meses después* de la entrada en vigor de la ley y a su vez el artículo quinto que abroga o en su caso deroga las disposiciones locales en materia de protección de datos personales en posesión de los particulares que se opongan a la presente Ley.

Todo esto nos parece preocupante y podría constituir una simulación la materialización o aplicación operativa del segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, al establecer una *vacatio legis* en cuanto a la aplicación de la ley tan extendida que prácticamente a pesar de exista una disposición constitucional vigente en materia de protección de datos personales en posesión de particulares, haga nugatorio el ejercicio de este derecho fundamental al introducir dichas disposiciones transitorias , particularmente el artículo cuarto.

Aunado a lo precedente, si en lapso de la *vacatio legis*, algún ciudadano decidiera ejercer esta garantía constitucional por la vía de los precedentes jurisdiccionales se empezaría a construir el ejercicio de este derecho desde el plano judicial. Y finalmente truncar los logros en la materia en algunas entidades federativas o en su caso municipios, nos parece aberrante al "desconocerles" todos esos logros que la Federación no supo erigir después de décadas de mentiras, traiciones y corrupción.

BIBLIOGRAFÍA

Doctrina:

Burgoa Orihuela, Ignacio. 1984. *Diccionario de Derecho Constitucional Garantías y Amparo.* Editorial Porrúa. México

De Domingo Pérez, Tomás. 2001 *¿Conflicto entre derechos fundamentales? Un análisis desde las relaciones entre los derechos a la libre expresión e información y los derechos al honor y a la intimidad.* Madrid, España. Centro de Estudios Políticos y Constitucionales.

Fernández Rodríguez, José Julio, *Lo público y lo privado en Internet*, Intimidad y libertad de expresión en la red, Editorial Instituto de Investigaciones Jurídicas, Serie Doctrina Jurídica, No. 154, UNAM, México, 2004.

Luhmann, Niklas y Raffaele De Georgi. 1993. *Teoría de la Sociedad.* Universidad de Guadalajara. Universidad Iberoamericana. Instituto Tecnológico y de Estudios Superiores de Occidente. México.

Pérez Luño, Antonio Enrique, *Ensayos de Informática Jurídica*, 2° edición, Editorial Fontamara, México, 2001.

Puccinelli, Oscar, *El Habeas Data en Indoiberoamérica*, Editorial Themis, Colombia. 1999.

Código modelo: Código de Buenas Prácticas y Alternativas para el Diseño de Transparencia y Acceso a la Información Pública en México, www.ifai.org.mx.

Declaración Universal de los Derechos Humanos., (Documento web), Asamblea General de las Naciones Unidas, 10 de diciembre de 1948 en: http://www.un.org/spanish/aboutun/hrights.htm

Dictámenes de Discusión de las comisiones unidas de puntos constitucionales; y de estudios legislativos, el que contiene proyecto de decreto que adiciona un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos., http://www.senado.gob.mx/gace.php?sesion=2008/12/04/1&documento=71

Diputado Luis Gustavo Parrra Noriega. Avances y Retos en la Legislación en materia de Protección de Datos Personales *"Avances y Propuestas Legislativas en materia de Protección de Datos Personales"* 25 de febrero de 2009.

http://www3.diputados.gob.mx/camara/content/download/210061/515613/file/DIP.%20LUIS%20GUSTAVO%20PARRA%20NORIEGA.ppt

García Ramírez, Sergio. *En torno a la seguridad pública. Desarrollo penal y evolución del delito. Cit. por* Arellano Trejo Efrén. "Definición". en Seguridad Pública, (Documento web), Centro de Estudios Sociales y de Opinión Pública. Febrero. 2006. en: http://archivos.diputados.gob.mx/Centros_Estudio/Cesop/Comisiones/dtseguridad%20publica1.htm

"Obligaciones del Estado en materia de Protección de Datos Personales", (Documento web), Instituto Federal de Acceso a la Información, en: http://www.senado.gob.mx/comisiones/LX/cyt/content/seminarios/tecnologias/Lina_Ornelas.pdf

Ley de Seguridad Nacional. México. 31 de enero. 2005. última reforma publicada en el DOF: 26 de diciembre, 2008. en: http://www.cddhcu.gob.mx/LeyesBiblio/pdf/LSegNac.pdf

¿Seguridad, Privacidad, Confidencialidad? El desafío de la protección de datos personales, Ediciones Trilce, Goethe-Institut Montevideo, Montevideo, 2004.

Legislación:

Constitución Política de los Estados Unidos Mexicanos.

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

Ley de Transparencia y Acceso a la Información del Estado de Nuevo León.