El derecho a la protección de datos personales y la implementación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

José Guillermo Petricioli Alfaro•

La persona que pierde su intimidad lo pierde todo.

Milan Kundera (1929-) Novelista y ensayista checo

Abstract

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares es una normatividad cuya total implementación ya es una realidad, debido a que a finales de diciembre de 2011 se publicó el Reglamento de la Ley citada. La intimidad, la privacidad y la protección de datos personales eran temas que en México, a pesar de su notorio uso cotidiano y a la avanzada codificación internacional, hasta ahora, con la publicación de la multicitada Ley, empiezan a tener ya una mayor proyección en el Estado Mexicano. La propia norma es explicada para comprender por qué al ser ésta de orden público y de observancia general, la autoridad tiene interés en proteger los datos personales y difundir los principios que aplican a éstos con el fin de regular su tratamiento, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Se hace referencia también a los antecedentes normativos internacionales con el fin de que el lector se familiarice con el desarrollo de los derechos a la privacidad y a la protección de datos personales.

Introducción

El valor de la privacidad es casi intangible. Al querer determinar el valor económico de una identificación oficial, y el costo que pagaríamos porque ciertos

• Licenciado en Derecho por la Universidad Iberoamericana León. Maestro en Derecho por la New York University (NYU). Director de área de investigación en la Dirección General de Verificación de la Secretaría de Protección de Datos Personales del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI).

datos personales no se conocieran en caso de que se extraviara o se nos robara tal identificación, es difícil de cuantificar. Algunos dirían que no tiene valor; otros que cuesta unos pesos o al contrario, miles de pesos y unos más señalarán el costo del material. Sin duda, el valor de un dato personal es subjetivo. Para algunos vale mucho mantener el anonimato, su nombre , su dirección o su edad; sin embargo, también hay casos en que el valor de un dato personal es casi siempre alto, aceptando como un hecho casi incontrovertible por la mayoría de la sociedad, que si extraviamos o se nos sustrae un dato personal sensible, sexual, patrimonial o de salud, haríamos mucho por protegerlo[1].

La gran discusión en torno a la privacidad en México giraba hace unos años en ”qué” se debía proteger, para evolucionar posteriormente a “cuánto” se debía proteger, y el dilema hoy es “cómo” se debe proteger esta privacidad.

El valor de la información de un dato personal es incuantificable y fascinante. Con información suficiente y precisa, se reconocen patrones, conductas, procesos psicológicos; se prevén tendencias; se generan estadísticas; se establecen probabilidades y se crean algoritmos que permitan tener sistemas informáticos y electrónicos casi perfectos. Con información explícita de datos personales, al compararse con otros datos, se pueden generar avances en materia médica, lo mismo que soluciones mediante la implementación de información y datos obtenidos de políticas públicas; incluso, hasta de preferencias y resultados electorales. Sin embargo, es también claro que el uso de tecnologías, de manera tan vertiginosa en últimos tiempos, ha puesto en riesgo los métodos de protección

[1] Artículo 4 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

al derecho a la intimidad y a la privacidad, casi siempre por abuso de los depositarios de estos datos o por decisión propia no consciente del titular del dato personal.

La imposibilidad de permanecer en el anonimato en la libertad de expresión y en la libertad de acción, al ser humano le ha traído consigo el cuestionamiento de cómo se puede permanecer en lo íntimo, sin ser molestado.

Varios referentes trascendentes para mostrar el interés en el tema de la protección de los datos personales los encontramos en la historia, en Alemania, con el extinto Ministerio de Seguridad para el Estado, *Ministerium für Staatssicherheit,* mejor conocido como la *Stasi,* el cual ejercía vigilancia sobre sus ciudadanos al punto de que es secreto a voces las violaciones predilectas a los ciudadanos en una de las posesiones más preciada, la información personal y la intimidad. Ya estamos también familiarizados con el debate y la lucha entre lo público y lo privado, entre la fascinación por conocer la intimidad del otro, sin que éste se de cuenta, o aun contra su consentimiento.

La literatura también lo ha previsto, con el ejemplo por excelencia, *1984* de George Orwell, que como mayor herencia nos dejó el morboso concepto sobre la vigilancia omnipresente del *hermano mayor*. La adaptación a televisión y cine del concepto de privacidad también ha sido prolífica, mencionando como un botón programas como *Big Brother*, o películas como *La Vida de los Otros*[2]*.*

[2] Título original en Alemán *Das Leben der Anderen* del director Florian Henckel Von Donnersmarck.

Sin embargo, aterrizándolo ya al abordaje legal en México, el tema era abundante, aunque disperso, desde hace años; la pugna de derecho entre privacidad y seguridad, privacidad e inteligencia militar, privacidad y espionaje, privacidad y vida en sociedad, privacidad y políticas públicas, y privacidad y desarrollo, por mencionar algunas, solo habían sido abordadas en el ámbito de la información de datos personales de servidores públicos por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en cuanto a la información generada y custodiada por la autoridad y el gobierno, por lo que el enfoque de este breve trabajo es acercarnos ahora a esas pugnas, con la expectativa de que ahora sean menos difusas, cuando intervienen en conflicto los datos personales de los particulares con las obligaciones de cuidado de esos datos por parte de los mismos particulares, especialmente en posesión de comerciantes, empresas y negocios.

Por lo anterior, es de celebrarse la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, ya que al ser éstos instrumentos públicos que obligan a la autoridad a vigilar que se implementen medidas de seguridad técnicas, administrativas y técnicas suficientes para proteger los datos personales contra su mal uso y destrucción, este tópico empieza ya a discutirse en los más diversos foros académicos, políticos y jurídicos, siendo menester que la sociedad en general empiece a interesarse en la trascendente temática que aborda de cómo ejercer sus derechos para proteger la privacidad.

Se advierte al lector que el contenido del presente trabajo es sólo una mera explicación breve de las disposiciones de la mencionada Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que busca que el objetivo o propósito sea una sencilla familiarización con sus conceptos y no un profundo trabajo de investigación, del cual de antemano se ofrece una disculpa al lector por ser éste un escrito tan simple.

DESARROLLO

El derecho a la protección de datos personales, ya ha sido abordado desde la legislación internacional, ya fuere en convenios, resoluciones y leyes locales de otros países; sin embargo, debe hacerse breve referencia a los siguientes instrumentos internacionales por ser los más conocidos que normativizan el derecho a la privacidad:

- Artículo 12 de la Declaración Universal de los Derechos del Hombre que dispone *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 ataques.*
- Artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre que expone que *toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar*, previendo por tanto el derecho a la protección a la honra, la reputación personal y la vida privada y familiar.

- Artículo 8 del Convenio para la protección de los derechos humanos y las libertades fundamentales, consistente en los siguientes puntos relativos al derecho al respeto a la vida privada y familiar:

  1 Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

  2 No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

- Artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, que dispone de manera similar a los ordenamientos previos lo siguiente:

  1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

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

- Artículo 11 apartado 2 de la Convención Americana sobre los Derechos Humanos, conocido como Pacto de San José. Esta disposición, en la cual quiero hacer hincapié, es la relativa a la Protección de la Honra y de la Dignidad, que expresa: *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.

Tal disposición tiene relación con los artículos 1.1 (Obligación de respetar los derechos) y 2 (Deber de adoptar disposiciones de derecho interno) de la misma Convención. Estos artículos son el ejemplo perfecto para poder implementar la protección de datos personales en México, aun si no tuviéramos reconocimiento constitucional o ley alguna, en razón de la novedosa facultad de todas las autoridades de ejercer control de convencionalidad y control difuso de normas, para darle verdadera validez al derecho internacional y a las sentencias generadas por tribunales internacionales, que sería materia de otro trabajo.

Este último instrumento citado, a mayor abundamiento, prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas, como la de sus familias, sus domicilios o sus correspondencias. La Corte Interamericana de Derechos Humanos, con sede en San José, Costa Rica, ha sostenido que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. Aunque las conversaciones telefónicas no se encuentran expresamente previstas en el artículo 11 de la Convención Americana de Derechos Humanos, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección del derecho a la vida privada.

En la última década, más de 30 países han adoptado leyes estrictas de protección de datos personales, las cuales determinan que el poder para la transmisión de estos datos, en gran medida, recae en los consumidores. Sorprendentemente Europa, y no Estados Unidos, ha liderado este esfuerzo y ha establecido los estándares en el temas a nivel global, desafiando la dominación norteamericana en el mercado internacional regulatorio.

El derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados, siempre que las injerencias no sean abusivas o arbitrarias; por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad; es decir, deben ser necesarias para legitimar los actos de autoridad en una sociedad democrática, tal y como aconteció en la pugna entre el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), al solicitar al Servicio de Administración Tributaria, el (SAT), dependiente de la Secretaría de Hacienda y Crédito Público (SHCP), de ordenar a la última, difundiera datos sobre créditos fiscales.

Evidentemente, a nivel nacional existía una base clara en el primer párrafo del artículo 16 constitucional desde hace décadas, el cual, recordaremos, protege al gobernado contra actos de molestia de la autoridad, aunque no es sino hasta la inclusión del segundo párrafo de ese mismo artículo, a mediados del año 2009, que determina que *"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", cuando existe una inclusión de un derecho fundamental, con reconocimiento constitucional, a la protección explícita de los datos personales.

Desde el año 2001 se presentaron las primeras iniciativas de leyes de protección de datos personales, contando ya con cierta regulación sectorizada en circulares de bancos, en sociedades de información crediticia, o en protección del consumidor, pero no fue sino casi 10 años después, cuando se publicó la normatividad que ya lo regula de manera clara.

Otro ejemplo en la vasta normatividad del sector público lo encontramos en la Norma Oficial Mexicana (NOM) del Expediente Clínico que *establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud*, en donde la propia Ley General de Salud y el Reglamento de Insumos para la Salud son ejemplos vinculados, que se relacionan en un tema específico, el de la salud, en cuanto al alcance de la regulación de los datos personales, ya sea para proteger contra su tratamiento, o para desarrollar tal uso.

No obstante lo anterior, la normativa más clara de protección a los datos personales la encontramos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFDPPP) la cual es el referente de la reglamentación del derecho humano constitucional de la protección de datos personales, la cual será materia de nuestra discusión de ahora en adelante.

CONCEPTOS DE LA LEY Y EL REGLAMENTO

Para comprender la protección de datos personales, hay que empezar por su concepto, el cual la Ley refiere como *datos personales* a *cualquier información concerniente a una persona física identificada o identificable.*

Otro concepto trascendente es el de *datos personales sensibles*, los cuales la Ley define como *aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida puedan dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual*.

Un concepto más es el del **Responsable** el cual se entiende como la *persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.*

ENCARGADO DESIGNADO POR EL RESPONSABLE

La figura de ”encargado”, igualmente importante, es la de *la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.* El encargado, normalmente aunque no de forma obligatoria, puede ser el responsable, o un empleado de éste.

Sus obligaciones son fundamentalmente las siguientes:

I. Tratar los datos personales conforme a las instrucciones del responsable;

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;

III. Implementar las medidas de seguridad conforme a la normatividad aplicable;

IV. Guardar confidencialidad respecto de los datos personales tratados;

V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable;

VI. Abstenerse de transferir los datos personales (salvo el responsable lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente).

Al familiarizarnos con algunos de los conceptos que desarrolla la ley, encontramos un avance para determinar cuál es el bien jurídico protegido, los principios a los que sujetan tales datos y con posterioridad, los métodos para protegerlo.

PRINCIPIOS

La ley define también principios de observancia obligatoria por los responsables para proteger los datos personales, los cuales consisten en:

1. *Responsabilidad*, relativa al deber de cuidado de los datos, privilegiando los intereses del titular y la expectativa razonable de privacidad.
2. *Información*, concerniente al proceso de transmitir las razones por las cuales se obtienen datos con la debida.
3. *Proporcionalidad*, consistente en tener los datos necesarios para la finalidad y obtener la mínima cantidad de información necesaria para llegar a tal finalidad.
4. *Calidad*, traducida en veracidad y exactitud en la obtención y uso del dato. Se presume cuando la información es proporcionada directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.
5. *Lealtad*, para que el dato no se obtenga por medios engañosos o fraudulentos. Establece también la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.
6. *Finalidad*, consistente en el porqué del uso u obtención de datos personales. Busca que se cumpla con los objetivos establecidos en el aviso de privacidad debiendo éstos ser determinados, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales.

7. *Licitud*, significa que la información sea recabada y tratada bajo el marco de la legalidad y obligando al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.
8. *Consentimiento*, para que previo al tratamiento de datos personales, se obtenga la aprobación y permiso del titular de éstos.

Estos principios, al estar contenidos en ley, podrán ser materia de mayor reglamentación al momento que el IFAI emita las recomendaciones para implementar medidas de seguridad para proteger datos personales, al marcar las mejores prácticas que se generarán en torno a que la ley sea verdaderamente ejecutable y no letra muerta.

AVISO DE PRIVACIDAD

Posteriormente, la ley menciona el aviso de privacidad, el cual se define como un **"***documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley".*

Dicho aviso de privacidad deberá contender las finalidades del tratamiento, los medios para que los titulares limiten el uso o la divulgación de los datos, y la forma en que ellos pueden ejercer los derechos de acceso, rectificación, cancelación u oposición, entre otros puntos de adhesión a las obligaciones autoimpuestas por el

responsable del tratamiento de los datos. El aviso de privacidad deberá contener, al menos:

- Identidad y domicilio del responsable que los recaba
- Finalidades del tratamiento de datos
- Opciones y medios que el responsable ofrece a los titulares para limitar el uso o divulgación de los datos
- Los medios para ejercer los derechos ARCO
- Si hay transferencias de datos
- Procedimiento para comunicar cambios al aviso de privacidad

El aviso deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.

Para la difusión de los avisos de privacidad, el responsable podrá valerse de formatos físicos, electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

MEDIDAS DE SEGURIDAD

Otro elemento trascendente es cómo el responsable del tratamiento de los datos garantizará que se cumpla con las medidas de seguridad técnicas, físicas y administrativas para proteger los datos personales, lo cual es posible a través de la implementación de un documento o política de seguridad.

El Reglamento de la Ley es precisamente el que da la pauta para los estándares de tal documento, al imponer la obligación al IFAI para que emita lineamiento de medidas de seguridad físicas, técnicas y administrativas mínimas a implementar para que los responsables protejan datos personales.

Interesante es el parámetro de que las medidas de seguridad para proteger datos personales no serán menores a aquellas que mantenga el responsable para el manejo de su información, sin referirse a qué información, contable o financiera por ejemplo, lo cual significaría empezar con el pie derecho en los estándares que los responsables implementarán en el cuidado de datos personales.

MEDIDAS DE SEGURIDAD ADMINISTRATIVAS

Consisten en el conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal en materia de protección de datos personales.

MEDIDAS DE SEGURIDAD TÉCNICAS

Son el conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados

b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones

c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y

d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales

MEDIDAS DE SEGURIDAD FÍSICAS

Consisten en el conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:

a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información

b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones

c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y

d) Garantizar la eliminación de datos de forma segura

Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) de los titulares de los datos

Consiste en que el titular puede conocer sus datos personales, así como información relativa a las condiciones y generalidades del tratamiento en poder del responsable de cuidar sus datos.

RECTIFICACIÓN

Consiste en que pueden modificarse datos inexactos o incompletos.

CANCELACIÓN

Se ejecuta al bloquear y suprimir el dato de las bases del responsable.

OPOSICIÓN

Procede al momento de que el titular del dato, por causa legítima, solicita al responsable que no se de uso ni tratamiento a sus datos.

PROCEDIMIENTO DE PROTECCIÓN DE LOS DERECHOS ANTE EL IFAI

Procede en contra de las inconformidades derivadas del ejercicio de los derechos ARCO, entre otras, cuando:

1. No se haya recibido respuesta por parte del responsable
2. No se otorgue acceso a los datos personales solicitados o lo haga en un formato ilegible o incomprensible
3. El responsable se niegue a efectuar rectificaciones a los datos personales
4. El titular no se conforme con la información entregada por considerar que es incompleta
5. El responsable se niegue a cancelar los datos personales
6. El responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición

SOBRE EL PROCEDIMIENTO DE VERIFICACIÓN

Procede al momento de que el IFAI investiga, ya sea por denuncia o de oficio, posible incumplimiento a la ley. Este proceso debe cumplir no solamente con la

normatividad relativa a visitas de verificación que contempla la Ley Federal del Procedimiento Administrativo, sino que tiene sus particularidades, toda vez que requiere un mayor término que el que ordinariamente otras autoridades administrativas usan para verificar el cumplimiento de obligaciones de carácter administrativo. Se asemeja, en la complicación y el fondo de su procedimiento, a una visita domiciliaria para verificación de cumplimiento de obligaciones fiscales o en materia de comercio exterior, pero no se sujeta a tales estándares de reglas.

Al día de hoy, el IFAI, a diferencia de otras dependencias que desarrollan verificaciones en materia administrativa en los diferentes niveles de gobierno, no cuenta con grandes facultades de inmovilización de equipos o levantamiento de los mismos para ser analizados en laboratorios o incautados como parte de un proceso criminal; sin embargo, la ventaja de esta verificación es que tiene el carácter de sorpresa y alerta[3].

Por las complejidades de este acto de verificación, no solo se requieren abogados expertos en derecho administrativo, sino fundamentalmente se requieren ingenieros, informáticos y técnicos en sistemas computacionales.

SANCIONES

Las sanciones van desde cinco mil pesos hasta 18 millones de pesos en caso de reincidencia. La infracción se basa en los principios del derecho administrativo sancionador.

[3] Ver: Visitas de verificación. La ley Federal de Procedimiento Administrativo no requiere que se entiendan forzosamente con el interesado, y en caso de no encontrarlo, dejarle citatorio para el día hábil siguiente. Registro IUS 176772

POSICIÓN JUDICIAL SOBRE EL DERECHO A LA PRIVACIDAD EN LOS ESTADOS UNIDOS DE AMÉRICA

En los Estados Unidos de América, el gran referente es el voto disidente del Ministro de la Suprema Corte de Justicia, Louis Brandeis, quien hace más de ochenta años, en el caso *Olmstead v. United States*, condenó la intrusión del gobierno en la privacidad de las personas, acuñando la famosa frase de que una persona tiene "el derecho de ser dejada en paz y a solas, el más fundamental de los derechos y el más valorado por los hombres civilizados".

Tal sentencia argumentó que la habilidad del gobierno hoy en día de poder utilizar sofisticados artefactos tecnológicos de vigilancia, como un sistema de posicionamiento global, *conocido como GPS*, pone en relieve que en verdad el gobierno se convierte en el *big brother* al constantemente estar invadiendo la privacidad de los gobernados.

Ya en el caso *Kyllo v. United States*, decidido hace más de diez años, la Suprema Corte de Justicia de los Estados Unidos decretó que el uso de un detector térmico que pueda verificar el calor que emana desde el interior de una casa, requería forzosamente una orden o permiso especial de un juez, y no podía ser utilizada en simples métodos de investigación policial.

Incluso en otro caso, como el de *United States v. Knotts,* la Suprema Corte de Justicia de los Estados Unidos dijo que el que la policía insertara un sistema de rastreo en un vehículo y seguirlo, no era exactamente una invasión a la privacidad,

porque el auto era conducido en público, y cualquiera podía ver los movimientos de tal automóvil. Vemos que incluso en un país de avanzada, en los temas de tecnología, los límites a la privacidad también son difusos.

CRÍTICA GENERAL A LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES

La ley parece ser insuficiente en regular figuras como las siguientes:

1. *Phishing y pharming*[4]*,* que consisten en obtener datos personales de los usuarios de internet, así como datos de carácter sensible o relativo a aspectos económicos (tarjetas de crédito).
2. *Social spammer* y *spam*[5]*,* que consisten en el uso de las redes sociales como plataformas para el envío de correos electrónicos no deseados.
3. *Suplantación o robo de identidad,* se refiere a que la "identidad digital" de una persona ya está siendo utilizada en redes sociales.
4. *Instalación y uso de cookies*[6] *sin conocimiento del usuario,* que permitan a la plataforma [7]conocer cuál es la actividad del usuario dentro de internet.

CONCLUSIÓN

El tema que realmente preocupa a las personas en relación con su información personal no es el acto de compartir la información en sí, pues la mayoría entiende

[4] Obtención ilegal de datos mediante páginas de internet falsas.
[5] Envío masivo de correo no deseado.
[6] Término informático para información sobre un usuario almacenada de forma local.
[7] Protección de datos de carácter personal Alfonso I. López-Bello Moreno* publicada en "El mundo del Abogado" Diciembre 2011. México.

que esto es crucial para la vida social, sino la distribución inadecuada e indebida de la información[8].

La información debe ser distribuida y protegida de acuerdo a las normas que rigen los distintos contextos sociales, ya sea lugar de trabajo, servicios de salud, escuelas, o entre la familia y amigos. Las distinciones básicas entre lo público y lo privado muchas veces tienen el efecto de oscurecer, más que aclarar, las políticas públicas.

Es de reconocer en México que la ley es un avance, y sobre todo la asignación presupuestal para que el Estado vigile la protección de estos datos, a través de darle tal encargo al IFAI, aprovechando su experiencia en regular los datos personales en posesión del Estado, para ahora vigilar un mundo desconocido para éste, el de los particulares.

El propio universo de sujetos regulados es diverso en su cumplimiento, aplica a cualquier persona moral o física que en el curso de sus actividades utiliza datos personales. Según la Secretaría de Economía, hay 5.1 millones de empresas que manejan bases de datos, y esto sin contar particulares, profesionistas abogados, consultores, médicos, etc. que manejan también bases de datos personales.

[8] Helen Nissenbaum. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* (*Privacidad en Contexto, tecnología, política pública y la integridad de la vida social)* Estados Unidos: Stanford Law Books.

Los deberes de los responsables, en general, y lo que podemos exigir como titulares de datos personales, son entre otros:

- Implementación de medidas de seguridad físicas, técnicas y administrativas para prevenir vulneraciones.
- Confidencialidad en el tratamiento de datos.
- Tener aviso de privacidad.
- Contar con un encargado de tratamiento de datos.
- Describir claramente cláusulas de transferencias de datos.
- Cumplir al titular de los datos para que se le facilite el acceso a sus datos, a su rectificación, cancelación y al procedimiento de oposición a ciertos tratamientos de los mismos.

Incluso en los diccionarios jurídicos mexicanos, aún es difícil encontrar conceptos tales como privacidad, intimidad, o datos personales. Es más, hoy sólo llegan a mezclarse éstos con el derecho a la información, o como una más de las actividades del derecho administrativo.

Ahora, como consumidores, cuando nos den el aviso de privacidad y nos recaben datos personales, se nos tiene que comunicar qué va a pasar con esa información, para cambiar la cultura con la cual se venía manejando los datos por parte de las empresas, ya que la perspectiva es que ellas eran dueñas de las bases de datos, pero ahora, como su nombre lo dice, solo los poseen, ya que los usuarios seguimos siendo los propietarios de nuestra información, no las empresas.

Al día de hoy, la obligación del Estado es la de orientar los esfuerzos a promover el cuidado de los datos personales, los cuales, evidentemente son información, y por lo tanto un bien, propiedad y posesión personalísima, la cual, no por la complejidad de su cuidado debe de ser difícil de proteger; por el contrario, por su valor, se debe iniciar de manera orquestada una fuerte política pública para poder acceder a un bien mayor como es que la sociedad tenga control de su intimidad, y que detrás, el Estado, orientado por el interés público de un derecho humano, proteja este bien jurídico tal como cualquier otro.

BIBLIOGRAFÍA

1. Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el Diario Oficial de la Federación el 5 de julio de 2010.
2. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación el 22 de diciembre de 2011.
3. Araujo Carranza, Ernesto (2009) *El derecho a la información y la protección de datos personales en México,* Ed. Porrúa, México.
4. Muñozcano Eternod Antonio (2010) *El derecho a la intimidad frente al derecho a la información,* Ed. Porrúa, México, 2010.
5. Ratcliff, Ronald E. (2008). *What Does Privacy Mean in an Age of Virtual Transparency?* [9]Tesis Doctoral, Estados Unidos: Salve Regina University.
6. Newman Abraham L. (2008). *Protectors of Privacy: Regulating Personal Data in the Global Economy*[10]*.* Estados Unidos: Cornell University Press.
7. McThomas, Mary Beth (2007) *The Right to Privacy: Individual Liberty, Property Interests and the Dual System of Privacy Rights in the United States*[11]*.* Tesis Doctoral, Estados Unidos: University of California, Los Angeles.

[9] ¿Qué significa la privacidad en la era de transparencia virtual?
[10] Protectores de privacidad, regulando datos personales en la economía global.
[11] Libertad individual, intereses de propiedad y el sistema dual de derecho a la privacidad en los Estados Unidos.

8. Newman, Abraham L. (2006) *Creating Privacy: The International Politics of Personal Information*[12]*.* Tesis Doctoral, Estados Unidos: University of California, Berkeley.

[12] Creando privacidad, políticas internacionales de la información personal.