CÁMARA DE DIPUTADOS
LXIII LEGISLATURA

DIRECCIÓN GENERAL DE SERVICIOS DE DOCUMENTACIÓN, INFORMACIÓN Y ANÁLISIS
SEDIA

CRV-X-18-17

SERVICIOS DE INVESTIGACIÓN Y ANÁLISIS

DIRECCIÓN

CONGRESO REDIPAL VIRTUAL X

Red de Investigadores Parlamentarios en Línea
Marzo-septiembre 2017

Ponencia presentada por

Sandra Marisela Flores Alonso

"TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES"

Mayo 2017

Av. Congreso de la Unión Nº. 66, Colonia El Parque; Código Postal 15960,
México, DF. Teléfonos: 018001226272; (+52 ó 01) 55 50360000, Ext. 67032, 67034
e-mail: redipal@congreso.gob.mx

TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES

Sandra Marisela Flores Alonso [1]

RESUMEN

El presente trabajo aborda el tema de la transparencia, específicamente el aspecto de la protección de datos personales para tratar de describir la importancia que tiene en la actualidad, a partir de la revisión del marco conceptual, normativo y modelos existentes, así como abordar someramente la aplicación y cumplimiento de los principios y deberes que sustentan al derecho a la protección de información personal en México.

Incluye un planteamiento de los aspectos más relevantes de la relación de la protección de los datos personales con el Internet, los dispositivos móviles, las redes sociales, el *big data* y los motores de búsqueda; con el fin de hacer una reflexión del uso de nuestros datos personales, cuáles son nuestros derechos y cuáles son los deberes a exigir a quienes manejan la información personal.

Así también, un rápido recorrido de los conceptos fundamentales sobre el derecho a la protección de datos personales, una breve referencia a la normativa aplicable en el ámbito federal, algunos ejemplos sobre los retos de este derecho emergente con el uso de las nuevas tecnologías de la información, para finalizar con una reflexión de los desafíos que enfrenta esta disciplina y su importancia en la sociedad actual.

[1]Miembro de la REDIPAL. Licenciada en Comunicación por la Universidad Autónoma de México UNAM; diplomada en Derecho Parlamentario por la UIA; máster en Democracia y Parlamento por la UNAM y la Universidad de Salamanca, España; Titular de la Unidad de Transparencia del Sindicato de Trabajadores de la Cámara de Diputados del H. Congreso de la Unión, Ciudad de México. Correo electrónico: sandra.flores@congreso.gob.mx

I. INTRODUCCIÓN

El derecho a la información muestra siempre dos caras: la publicidad (o transparencia) de la información y la privacidad (opacidad de la información de particulares expresada como "confidencialidad"). Un derecho que por una parte controla, a través de su exhibición, la información pública y por otra protege, a través de su clausura, la información privada.[2]

La protección constitucional de la privacidad es la otra cara normativa del principio de publicidad en el marco del derecho a la información, razón por la cual el presente texto se enmarca en el tema de transparencia y protección de datos personales.

Es importante enfatizar la doble naturaleza del derecho a la información:

a. Un derecho de control democrático de los ciudadanos sobre los poderes públicos y sobre los bienes públicos (como los recursos fiscales y la autoridad pública)
b. Un control que limita la arbitrariedad de los gobernantes y otras autoridades públicas (legisladores, jueces, partidos políticos) así como de particulares relacionados con el interés público.

El control sobre la información pública es, a la vez, una forma de proteger los derechos, los intereses y los bienes privados, que mientras son estrictamente privados, han de estar resguardados y sustraídos de la intromisión de terceros. [3]

Entonces, el derecho a la información a la vez fortalece la privacidad al otorgar protección constitucional a los datos personales, lo que amplía el espacio de acción de los ciudadanos, mientras limita el de las autoridades públicas y los poderes fácticos.

En México esta tensión que prevalece entre el interés público de conocer cierta información y la vulnerabilidad de los ciudadanos ante el uso indiscriminado de datos personales, que son puestos a merced del marketing comercial y político o en manos de la delincuencia, se ve también reflejada en las competencias del órgano constitucional autónomo y especializado en la materia, ya que estos dos temas convergen en el ámbito de competencia del INAI[4], que es el órgano responsable de garantizar el cumplimiento de

[2] INAI (2016), *Curso Sensibilización para la Trasparencia y la Rendición de Cuentas.*
[3] *Idem.*
[4] En mayo de 2015 el Instituto Federal de Acceso a la Información Pública (IFAI) dejo de existir y dio paso al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Además del nombre, el INAI renovó su misión, visión y objetivos, para ejercer sus nuevas funciones y atribuciones legales.

los derechos de acceso a la información pública y la protección de datos personales, en congruencia con el camino avanzado hasta ahora en transparencia.

Estos temas resultan aún poco conocidos para la población en general, ya que es reciente la reforma constitucional en materia de transparencia,[5] de la que se desprende una ley reglamentaria: la Ley General de Transparencia y Acceso a la Información Pública[6] y también la creación del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, aunque en los hechos se ha difundido más la parte referida a la transparencia.

La redacción del artículo sexto constitucional coloca la información que se refiere a la vida privada y los datos personales, dentro de los principios y bases del derecho a la información, pero nos remite a una legislación secundaria diferente, en este caso dos leyes referidas a la protección de datos personales.

Es evidente que el derecho de acceso a la información se encuentra más desarrollado en nuestro país, partiendo del análisis de la configuración constitucional de estos derechos y de su desarrollo en el ámbito local y en la legislación secundaria. Sin embargo, es un avance definitivo la incorporación en el artículo 16 constitucional el que toda persona tiene derecho a la protección, acceso, rectificación y cancelación de sus datos personales, así como a manifestar su oposición al uso de los mismos.

II. CONCEPTOS FUNDAMENTALES SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

La protección de datos personales es un derecho humano que les da a los individuos el poder de controlar su información personal, decidir con quién se comparte y para qué la utilizan terceros, así como el derecho a que sus datos se traten de forma adecuada, para permitir el ejercicio de otros derechos y evitar daños a su titular.

Cuando hablamos de datos personales nos referimos a toda aquella información relativa a una persona física que la identifica o la hace identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, por ejemplo le da identidad a una persona o la describe su origen, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Pero

[5] Publicada en el Diario Oficial de la Federación el 7 de febrero de 2014.
[6] Publicada en el Diario Oficial de la Federación el 4 de mayo de 2015.

también los datos describen aspectos más sensibles o delicados, como su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros aspectos. [7]

Entonces los datos personales son cualquier información que se refiera a una persona física que pueda ser identificada a través de los mismos. Dichos datos se pueden expresar en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, como por ejemplo: nombre, apellidos, CURP y RFC[8], estado civil, lugar y fecha de nacimiento, domicilio, número telefónico, correo electrónico, grado de estudios y sueldo, entre otros.

Dentro de los datos personales hay una categoría que se denomina "datos personales sensibles", que requieren especial protección, ya que se refieren a información que afecta a la esfera más íntima de una persona o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave, como la información genética, el estado de salud presente y futuro, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, origen racial o étnico y preferencia sexual.[9]

Los datos personales son necesarios para que una persona pueda interactuar con otras o con una o más organizaciones sin que sea confundida con el resto de la colectividad y para que pueda cumplir con lo que disponen las leyes. Asimismo, hacen posible la generación de flujos de información que redunda en crecimiento económico y el mejoramiento de bienes y servicios.

No obstante, el uso extensivo de las tecnologías de la información y las telecomunicaciones ha permitido que en muchas ocasiones, los datos personales sean tratados para fines distintos para los que originalmente fueron recabados, así como ser transmitidos sin el conocimiento del titular, rebasando la esfera de privacidad de las personas y lesionando en ocasiones, otros derechos y libertades.

Derechos ARCO

En México el derecho a la información está garantizado por el Estado bajo ciertos principios y bases establecidos en el artículo sexto constitucional, donde sobresale, para la interpretación de este derecho, el principio de máxima publicidad. Al respecto, cuando se habla de "la información" se refiere a toda la información en posesión de cualquier autoridad,

[7] Grupo de Trabajo del artículo 29 (2007), Dictamen 4/2007 sobre el concepto de datos personales.
[8] Clave Única de Registro de Población y Registro Federal de Contribuyentes.
[9] Artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

entidad, órgano y organismo federal, estatal y municipal, la cual es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. Así, cualquier persona, sin necesidad de acreditar interés alguno, o justificar su utilización, tendrá acceso gratuito a la información pública, sus datos personales y la rectificación de éstos.

La protección de datos de carácter personal, recoge una serie de derechos fundamentales de los ciudadanos conocidos como derechos ARCO (acrónimo que designa los derechos de acceso, rectificación y cancelación de los datos de particulares, así como el de oposición al uso de los mismos). El Derecho de rectificación se caracteriza porque permite corregir errores, modificar los datos que resulten ser inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento. El derecho de cancelación permite que se supriman los datos que resulten ser inadecuados o excesivos. El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo.

En tanto que el derecho de acceso permite al ciudadano conocer y obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento.

Asimismo el derecho de información consiste en que en el momento en que se procede a recolectar los datos personales, el interesado debe ser informado previamente de modo expreso, preciso e inequívoco de la existencia de un archivo, de la posibilidad de ejercitar sus derechos y del responsable del tratamiento, entre otros puntos.

Otro de los conceptos fundamentales a tener en cuenta es la figura del Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales, que no debemos confundir con el concepto de Titular: Persona física a quien corresponden los datos personales, o con la figura del Encargado: Persona física o jurídica que sola o conjuntamente con otras trata datos personales por cuenta del responsable.[10]

Tres de los términos más usados en el tema de la protección de datos personales son:

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

Consentimiento: Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

[10] Artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Aviso de Privacidad: Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos.[11]

III. MODELOS E INSTRUMENTOS INTERNACIONALES

En México nos retroalimentamos con lo que sucede en el ámbito internacional, particularmente en Europa, donde el derecho a la protección de datos personales es considerado un derecho fundamental a título propio, distinto al del derecho a la intimidad. El 28 de enero de 1981, muchos años antes del *boom* de las nuevas tecnologías y el uso de redes sociales, se firmó el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Con este parámetro inició el debate internacional sobre el papel del Estado como garante en la protección de datos de las personas.[12]

A fin de equilibrar las fuerzas entre las personas y aquellas organizaciones –públicas o privadas- que recaban o colectan datos de carácter personal, surge en Europa el concepto de la protección de datos personales. Un concepto similar surgió en los Estados Unidos de América (el concepto de "privacidad") aunque con alcances distintos.

Bajo el concepto de protección de datos personales, el titular (o dueño) de dichos datos es la propia persona, lo que implica la libertad de elegir qué se desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información. En naciones avanzadas, la protección de datos personales es quizá el más nuevo de los derechos que goza un ciudadano.

Los países suscriptores del mencionado Convenio 108 se comprometen a realizar las reformas necesarias en su legislación interna para implementar los principios contenidos en el Convenio, en primer término, que los datos personales deben recolectarse y tratarse con fines legítimos; que no deben conservarse más tiempo de lo estrictamente necesario de acuerdo con el fin para el cual fueron recolectados; que sean verdaderos, y que no sean excesivos. Asimismo, prevé que deberá garantizarse la confidencialidad de los llamados datos sensibles y reconoce el derecho de las personas para tener acceso y en su caso, solicitar la corrección de su información.

[11] Artículo 3 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.
[12] Red por la Rendición de Cuentas (2016) Boletín semanal del 24 al 31 de enero 2016.

A partir del 2006, el Comité de Ministros del Consejo de Europa decretó el 28 de enero como el Día Internacional de la Protección de Datos personales y en México se empezó a conmemorar este día bajo el auspicio del entonces IFAI a partir del 2009. Desde entonces, el objetivo ha sido sensibilizar a servidores públicos, instancias de seguridad y empresas públicas y privadas sobre las mejores prácticas en la materia, así como las implicaciones y riesgos de compartir datos con terceros.

La relevancia de los instrumentos internacionales consiste en el establecimiento de un marco armonizado de protección de datos personales a nivel global, con el fin de garantizar que el desarrollo del comercio a nivel mundial resulte compatible con la protección de los derechos de las personas, especialmente en lo que se refiere a la protección de la información que les concierne.

La legislación mexicana federal en materia de protección de datos personales cumple con los principales estándares establecidos en instrumentos internacionales en materia de privacidad y protección de datos personales. El que se reconozca como un derecho humano, con independencia de la nacionalidad o residencia, es para proteger la privacidad en un mundo sin fronteras y caracterizado por las transferencias internacionales de información, en el que resulta necesario que los Estados aprueben las leyes adecuadas para no perjudicar los intercambios de datos personales y la puesta en práctica de una protección de datos efectiva y global.

Existen diversos modelos de regulación en el ámbito de la protección de datos personales en el mundo, aquí sólo mencionaré brevemente algunos: el modelo estadunidense de autorregulación pura, que significa en concreto sin participación de la autoridad. En esta materia se observa que existen países que no tienen propiamente una legislación sobre protección de datos personales y que, en su mayoría, dejan este tema en manos de los particulares, lo que conocido como autorregulación pura. Este modelo se caracteriza por tener un marco jurídico muy flexible en materia de protección de datos personales, en el cual se le deja a las empresas actuar conforme a sus necesidades. Dicho marco se compone de las mejores prácticas de las empresas, acompañados de profesionales que desarrollan diversas prácticas para promover la cultura de la privacidad.[13]

Algunos países como Australia cuentan con una legislación sobre protección de los datos personales que reconoce y fomenta la adopción de mecanismos de autorregulación en el texto legal. Esto a su vez puede significar el otorgamiento de efectos jurídicos variados

[13] Prosoft (2014) *Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI*.

a los mecanismos de autorregulación, México se encuentra dentro de esta categoría de Modelo Mixto o Integrado de la Autorregulación en Materia de Datos Personales.

En España existen los Códigos Tipo o Códigos Deontológicos o de conducta, que constituyen un instrumento de autorregulación, es decir, la capacidad de las organizaciones y entidades para regularse a sí mismas. En el ámbito de la protección de datos de carácter personal esa capacidad está orientada a la adopción de reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por quienes se adhieran al código tipo o lo promuevan y a facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de la normativa.[14]

La Privacidad por Diseño o Privacy by Design (PbD por sus siglas en Inglés) es un concepto reconocido como estándar global de privacidad, donde idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización. El objetivo de la privacidad por diseño es asegurar la privacidad, obtener control personal de la información propia, y para las organizaciones, y obtener una ventaja competitiva sostenible.

Privacy by design es el modelo canadiense de protección de datos personales que promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios y que sus principios pueden ser aplicados a todos los tipos de información personal, con especial a los datos delicados tales como información médica y datos financieros.[15]

IV. LA NORMATIVIDAD APLICABLE EN MÉXICO

En México, el reconocimiento al derecho de protección de datos personales tuvo un proceso paulatino y se fue configurando desde el debate de qué es la información y qué son los datos. Al desarrollarse el derecho de acceso a la información pública gubernamental, se reparó en el hecho que se contaba con datos de personas es específico como es el nombre, domicilio, edad, teléfono, religión, patrimonio, dependientes, fotografía, huellas digitales, etc. y que esa información se encontraba en archivos públicos y cualquiera podría conocerla, afectando la vida privada de las personas.

En el año 2000 se empezaron a promover diversos proyectos legislativos sin que ninguno fructificara. En 2007, el Congreso de la Unión aprueba una reforma al artículo 6º

[14] Agencia Española de Protección de Datos (2016) *Ley orgánica 15-1999.*
[15] Privacy by Design (2016) Los “7 principios fundamentales”.

constitucional por la que se incorpora la protección a los datos personales y la información relativa a la vida privada, así como el derecho de acceder y corregir los datos que obren en archivos públicos.

Otro antecedente es la resolución emitida por la Suprema Corte respecto a lo que es la vida privada y el derecho a preservarla del conocimiento público, lo que eventualmente se incorporó al artículo 16 de la Constitución como protección de datos personales,[16] porque precisamente son esos datos los que merecen un trato especial y privilegiado. Así quedó reconocido el derecho de toda persona a la protección de sus datos personales, lo cual es de gran relevancia en virtud de éstos datos se encuentran en manos tanto de gobiernos como de particulares (empresas, organizaciones y profesionistas).

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".

Otra reforma constitucional[17] que impactó este derecho es la del artículo 73, fracción XXIX, inciso O) que dota de facultades expresas al Congreso General para legislar en materia de protección de datos personales en posesión de particulares y así llegamos al 2010 con la expedición de la Ley Federal de Protección de Datos Personales en Posesión de Particulares,[18] donde destacan los siguientes aspectos:

a) Modelo híbrido que equilibra los principios de protección de datos personales internacionalmente reconocidos, permitiendo el libre flujo de la información personal para el crecimiento económico, con las garantías necesarias para el titular de que el tratamiento de sus datos se lleve a cabo de manera lícita e informada.
b) Prevé los mecanismos para el ejercicio de los derechos ARCO ante una autoridad independiente y las sanciones para los sujetos regulados.

[16] Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden al artículo 16, publicado en Diario Oficial de la Federación, 1 de junio de 2009.
[17] Publicada en el Diario Oficial de la Federación el 30 de abril de 2009.
[18] Publicada en el Diario Oficial de la Federación el 5 de julio de 2010.

c) Satisface los elementos básicos que garantizan la protección de los datos personales: principios, derechos, procedimientos (ante el responsable y ante la autoridad), definición de autoridades reguladora y garante; así como un catálogo de infracciones y de sanciones relacionadas con las mismas.
d) Otorga una amplia protección a los datos sensibles, lo que colocó a la ley a la vanguardia de la protección de derechos de tercera generación.
e) Ampliación de la protección de los datos personales al ámbito privado, contando con una autoridad que resuelve quejas en este rubro.
f) Prevé que el consentimiento del titular de los datos sea tácito (opt-out) para casi la totalidad de tratamientos, excepto en el caso de datos sensibles; no se prevé la obligación de solicitar al órgano garante la autorización de las transferencias internacionales; prevé mecanismos de conciliación y establece la posibilidad de impugnar las resoluciones del órgano garante.

Al pasar los años se expidió otra reforma constitucional en el mismo artículo 73, fracción XXIX, pero ahora en el inciso S) que dota de facultades expresas al Congreso General para expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno.[19]

Al promulgarse la Ley General de Transparencia y Acceso a la Información Pública se estableció que en tanto no se expida la ley en materia de datos personales, permanecería vigente la normatividad federal y local en la materia, en sus respectivos ámbitos de aplicación. Esto es que los datos personales en posesión de los órganos gubernamentales eran materia local, mientras que los datos personales en posesión de sujetos privados como bancos, aseguradoras, proveedores y tiendas comerciales, son materia federal.

Así, la Ley Federal de Datos Personales en Posesión de los Particulares permaneció vigente, en tanto concluyó el proceso de aprobación de la nueva Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.[20]

Esta nueva ley es reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de

[19] Publicada en el Diario Oficial de la Federación el 7 de febrero de 2014.
[20] Nueva Ley publicada en el Diario Oficial de la Federación el 26 de enero de 2017.

datos personales en posesión de sujetos obligados y tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los siguientes sujetos obligados: en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Aquí vale la pena puntualizar que los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares.

V. DATOS PERSONALES EN INTERNET

El marco jurídico vigente enfrenta una serie de retos para su aplicación práctica, aunque definitivamente es un gran avance hablar de un derecho humano, de un ámbito de libertad que la Constitución reconoce a las personas frente al Estado. Pero por otro lado tenemos las malas prácticas de empresas de tecnología y compañías basadas en Internet que representan todo un reto a superar debido a que esas malas prácticas son acciones que van en contra de la ética y en algunas ocasiones de las normas legales. Por ejemplo las redes sociales y motores de búsqueda como compañías presentan prácticas engañosas, no en el sentido del precio engañoso, porque son gratuitas, pero sí lo son porque atraen a las personas con un servicio señalando todos los beneficios, pero no se mencionan claramente los costos adicionales, que en este caso es la pérdida del control de los datos personales.

Otras prácticas engañosas pueden ser las falsas promesas de limitar la privacidad, porque con ello también limitan el servicio. También está la venta bajo presión, que se da cuando la empresa a fin de vender sus productos, manipula, presiona y prácticamente obligar al consumidor a realizar la compra. No se paga con dinero, se paga con algo más valioso: nuestros datos, que al final del día se traduce en valor económico. Un claro ejemplo de lo anterior es cuando se insiste constantemente en bajar una *app*; dar un *click* para mejorar la experiencia del servicio; valerse de mentiras para convencer de ir a otro sitio web; permitir accesos a fotos o contactos, etcétera.

Otro tema es la venta de información del cliente, que sucede cuando la información que recaban las empresas de sus usuarios, las venden a otras empresas o a terceros, sin que el cliente de su consentimiento e incluso sin que se entere, afectando su derecho a la privacidad.

Cuando las empresas brindan información falsa, en este caso las vueltas sin fin en los *links* de políticas de privacidad, en donde señalan determinadas características que posee su servicio, que en realidad no son ciertas. Promesas no cumplidas, publicidad no solicitada... en fin, un enorme mercado donde la competencia es feroz y el usuario o consumidor parece cautivo.

VI. POLÍTICAS DE PRIVACIDAD EN DISPOSITIVOS MÓVILES Y REDES SOCIALES

El objeto de mencionar este apartado es comprender cómo tratan los datos personales los proveedores de aplicaciones para dispositivos móviles y eso lo podemos constatar revisando las políticas de privacidad y/o condiciones de uso y analizando a qué datos personales accede cada aplicación. Por ejemplo en un teléfono inteligente con aplicaciones básicas como *Whatsapp, Waze*, agenda, cámara, música, video y una aplicación de salud, encontramos que se tiene acceso a: número de teléfono, nombre de usuario, contactos, reconocimiento de voz, grupos, actividad, archivos, historial y copia de seguridad. Datos personales que pueden ser utilizados por Facebook con fines comerciales, salvo que nosotros nos opongamos expresamente a ello. Localización GPS del dispositivo, rutas, velocidad, frenado en seco, tiempos de trayectos, todo en tiempo real. Historial de ubicaciones. Chats y relaciones del *username* con los de otras aplicaciones, búsquedas, calendario. Fotografías y videos que sirven para identificar los lugares y personan con los que has estado. El software de seguimiento capta imágenes sin que el portador del dispositivo lo sepa. Recopilar, editar, agregar y almacenar datos médicos en línea, frecuencia cardiaca, pasos realizados peso, estatura, etc. Preferencias y contenidos, listas de reproducción, compras de música. Colección de vídeo y alquiler o compras de películas y episodios de televisión. Horas de uso e historial. Todo ello sin contar que muchas veces tenemos en el teléfono aplicaciones bancarias y acceso a nuestro correo electrónico personal y de trabajo, con toda la información sensible e íntima que eso conlleva.

Por otro lado tenemos las redes sociales donde destaca Facebook que al parecer trata pocos datos personales: nombre, usuario, contraseña y dirección de correo electrónico, pero que basa su éxito en la generación de contenido por parte de sus usuarios.

Esto es el mejor ejemplo de los llamados *prosumers o* prosumidores (acrónimo formado por la fusión de las palabras *producer* y *consumer*) que al final del día no son dueños de lo publicado en Twitter o Facebook, empresa que tienen acceso a fotos, contactos, reconocimiento de voz, actividad, archivos, historial, copia de seguridad y que también puede registrar y transmitir la dirección IP. Lo que no alcanzamos a leer en la letra chiquita de la política de privacidad es que se otorga una licencia no exclusiva, transferible, con posibilidad de ser subotorgada, libre de regalías y aplicable globalmente para utilizar cualquier contenido de IP que publiques en Facebook o en conexión con Facebook.

Sobre el tema de las redes sociales, la privacidad y la protección de datos personales se ha escrito mucho, por lo que únicamente señalo los principales riesgos en el uso de redes sociales, que pueden identificarse en el cuadro 1.

VII. INTERNET DE LAS COSAS Y BIG DATA

El internet de las cosas (IdC o loT, por las siglas en inglés de *Internet of Things*) es una revolución de la relación entre objetos y personas, incluso entre objetos que se conectan directamente entre ellos y con la red y ofrecen datos en tiempo real. Es sencillamente el punto en el tiempo cuando se conectaron a Internet más "cosas u objetos" que personas.[21]

El impacto que tiene el Internet de las cosas en la vida privada, lo podemos ver directamente a través de los aparatos que utilizamos diariamente y que tienen conexión a Internet para proporcionarnos una serie de servicios y aplicaciones inteligentes sin precedentes: *Smartphone, Smart TV*, consola de videojuegos, computadora, cámaras, *Iwatch,* refrigerador inteligente, lavadora, calzado deportivo, ropa inteligente, juguetes, autos, tabletas, edificios, mobiliario, dispositivos GPS, artículos de limpieza personal y objetos de oficina.

Con el Internet de las Cosas se aprovecha para medir ciertos parámetros externos (como por ejemplo temperatura, energía, actividad, luz, humedad, errores, etc.), de forma automática y sin la interacción del ser humano. Y esos datos viajen a un centro de procesamiento para que se tomen decisiones en tiempo real, por lo que se sabe exactamente la ubicación, el consumo y las compras de productos en todo el mundo, porque al final para eso se quieren los datos: para vendernos cosas… o bien para convertir esa información en conocimiento, según el enfoque que se le quiera dar.

[21] De acuerdo al Grupo de soluciones empresariales basadas en Internet de Cisco, Evans Dave (2011) Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo.

La información que comparten entre sí los dispositivos nos lleva a la invasión de nuestra privacidad. Toman decisiones por nosotros, ven nuestros datos, hacen un perfil y seleccionan qué necesitamos basado en ese análisis, a veces sin que interfieras en ello. Por ejemplo, creemos no tener información en *la nube*[22], porque no lo hemos realizado nosotros mismos, pero los dispositivos se conectan entre sí como lo vemos con *Dropbox y Icloud* que hacen respaldos automáticos de los teléfonos en *la nube*. Otro ejemplo típico es que sí tienes cuenta de correo en Google, Hotmail, o Yahoo, tienes información en *la nube*.

No basta con ser conscientes de lo que está sucediendo con nuestros datos, debemos tomar acciones como navegar anónimo o de incógnito en internet, en redes sociales cambiar la configuración de seguridad, cambiar contraseñas periódicamente, uso de *Smart Privacy* o privacidad inteligente, que significa un amplio espectro de medidas de protección de datos personales para administrarlos en forma adecuada.

Por otro lado tenemos un rápido vistazo a las repercusiones del tratamiento de información personal por parte de las empresas que utilizan *Big Data*.

El concepto de Big Data (datos masivos o metadatos) aplica para toda aquella información que no puede ser analizada utilizando procesos o herramientas tradicionales. Big Data son los grandes conjuntos de datos que tienen tres características principales: volumen, velocidad y variedad. Volumen de información ya que se habla en términos de petabytes y exabytes, además existe una gran variedad de datos que requieren velocidad de respuesta al realizar un análisis basado en el uso de algoritmos para obtener información correcta, en el momento preciso, para la toma de decisiones.

La cantidad y la velocidad a la que se producen los datos en el entorno digital nos llevan a su adecuado almacenamiento, lo que sucede en *la nube*, al contratar servicios especializados como los de Microsoft, Google y Amazon, que son los grandes proveedores del servicio y que atienden tanto a empresas como al sector público que administra bases de datos de censos, registros médicos, impuestos y demás información. Es aquí cuando nos empieza a hacer sentido la necesidad de protección de datos personales en este entorno digital, y entonces pensamos en las transacciones financieras realizadas en línea, en la información sobre clientes, proveedores y facturas, o bien en lo publicado en redes sociales y la ubicación geográfica mediante GPS.

La reflexión es que los seres humanos estamos creando y almacenando información en cantidades astronómicas, lo que implica una nueva forma de ver la información, que

[22] Computación en la nube es una metáfora empleada para hacer referencia a servicios que se utilizan a través de Internet.

antes era difícil de extraer o que estaba oculta, por lo que debemos cuestionar qué información es la que se debe analizar y enfocarnos en el gran valor social y económico asociado a los datos, que son transformados en materia prima para la producción, llegando incluso al concepto “minería de datos” (Data Mining).

VIII. PROTECCIÓN DE DATOS PERSONALES EN LOS MOTORES DE BÚSQUEDA

Los buscadores como Google, Safari, Bing, etcétera, tratan datos personales al indexar la información publicada en la red (aparte de los datos personales que tratan a través de las cookies), además estos buscadores hacen un respaldo de la información conocido como memoria caché, lo cual también puede ser considerado como tratamiento de datos personales.

En Europa se permite el ejercicio del derecho de cancelación y oposición ante los buscadores a raíz del caso de Mario Costeja, con una sentencia del Tribunal de Justicia europeo que obligó a Google España a eliminar enlaces de su buscador, aunque la información sigue disponible en los sitios web donde fue publicada originalmente. Sin embargo, es prudente hacer algunas precisiones ya que este tema se relaciona con el llamado “derecho al olvido” que como tal no es una figura jurídica y lo sí existe es el derecho de cancelación y de oposición.

En México, de acuerdo a las recientes resoluciones del INAI no es posible cancelar u oponerse al tratamiento de los datos personales ante Google, debido a que los servicios del motor de búsqueda no es prestado por Google México, sino por Google Inc, el cual tiene su sede en Estados Unidos y la Ley Federal de Protección de Datos Personales en Posesión de Particulares no puede ser aplicada de manera extraterritorial, por lo tanto, no hay competencia para ordenarle nada a Google Inc.

Lo anterior se desprende de una larga historia de desencuentros del INAI con Google, que inicia con la solicitud de un empresario mexicano para que se eliminen enlaces del buscador Google México, donde aparece su nombre. Google se negó y el empresario solicitó la protección del INAI y luego vino toda el proceso donde intervienen, además del órgano constitucional autónomo y la poderosa compañía de tecnología, muchos abogados, periodistas, activistas de derechos humanos, académicos y jueces mexicanos. El asunto es que Google México fue omiso en atender la solicitud de ejercicio de derechos de oposición y cancelación del Titular y durante el procedimiento y sólo a instancias del INAI, negó el ejercicio de los derechos referidos y se abstuvo de cancelar y dejar de tratar los datos en

cuestión, todo ello sin causa justificada y sin acreditar que el servicio de motor de búsqueda lo presta una empresa diversa.

Entonces se emite la resolución del INAI PPD.0094/14 contra Google México, S. de R.L. de C.V. del 26 de enero de 2015, donde destaca la valoración de un acta constitutiva que indica que el servicio de motor de búsqueda es prestado por Google México, sin embargo dicha acta fue modificada por la empresa y ahora no hay forma de acreditar que ese servicio es prestado por Google México. La resolución resolvió ordenar el ejercicio de los derechos de oposición y cancelación en los siguientes términos: 1. Por lo que respecta al derecho de oposición, con fundamento en el artículo 27 de la Ley de la materia, se abstenga de tratar los datos personales del Titular, consistentes en su nombre y apellidos, de tal manera que al ser tecleados en el motor de búsqueda del Responsable, no aparezcan los links o URL'S - indexación- que dicho Titular refirió en su solicitud de ejercicio de derechos ARCO de fecha veintidós de julio de dos mil catorce. 2. En cuanto al derecho de cancelación, con fundamento en los artículos 25, cancele los datos personales del Titular antes mencionados, de modo que no obren en las bases de datos del Responsable.

Al final la resolución queda sin efecto por orden del Tribunal de Justicia Fiscal y Administrativa, que no mandó llamar como tercero interesado a la empresa de comunicación que originalmente publicó la información y como consecuencia obliga a sobreseer el juicio de Google México contra el INAI y realizar un nuevo procedimiento.

La importancia del caso se explica por sí sola y no termina ahí, ya que existen consecuencias a la vista del desencuentro del INAI con Google al involucrarse temas fundamentales como la libertad de expresión, los datos personales y las responsabilidades de los motores de búsqueda en Internet.

IX. CONCLUSIONES

México ha llevado efectivamente a su marco jurídico el conjunto de principios y derechos de la protección de datos personales para su defensa y promoción señalados a nivel internacional. Lo anterior es relevante dado que los datos personales se encuentran en manos tanto de gobiernos como de particulares (empresas, organizaciones y profesionistas) y, porque con el uso indiscriminado de la tecnología, éstos pueden utilizarse para fines distintos de aquellos para los que fueron recabados.

La información relativa al interés público, de acuerdo a nuestra Constitución Política, ha de ser pública y abierta (aun cuando temporalmente y conforme a criterios también

públicos pueda reservarse), mientras que la información privada ha de ser confidencial y estará protegida frente a malos usos o abusos de otros sujetos.

En el artículo 16 constitucional incorpora el derecho fundamental de las personas al adecuado tratamiento y la protección de sus datos personales con la presencia de los derechos individuales de acceso, rectificación, cancelación y oposición.

La debida observancia de estas normas ha quedado sujeto al control de una autoridad independiente que en principio se denominó Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI) y hoy en día es el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI), que no parece incluir en sus siglas la parte de protección a los datos personales, con el sencillo argumento que el acceso a la información incluye los datos personales.

Sin embargo, en la práctica aún existen retos tanto en el ámbito privado como en el público, por lo que es indispensable dar seguimiento a la implementación de la legislación y cambiar el diseño legal e institucional que se requiera para desplegar el más nuevo de los derechos en nuestro país.

Como ejemplo claro de los retos a enfrentar está el robo de identidad, donde no encontramos aún una ruta para la corrección, protección o sanción para este tipo de actividad que es un importante desafío de coordinación entre diversas instituciones, ya que no existe una legislación federal que tipifique este delito, solamente hay en el país 16 entidades que contemplan una regulación para alguna de las variantes del robo de identidad. Sin embargo, las bases de datos con registros de datos personales que manejan instancias públicas y privadas como el INE (más de 85 millones de registros) el IMSS (60.5 millones de derechohabientes) o empresas privadas de telefonía móvil (105 millones de usuarios) obligan a la responsabilidad del buen resguardo y justificación pública del uso de esta información; así como a la existencia de certeza normativa que brinde suficientes garantías de protección a los usuarios.

La venta de ese tipo de bases de datos en los llamados mercados negros de la información, vuelve a los países poco competitivos, pues eleva los costos de sus transacciones y además carga con la penalización a las conductas violatorias de la debida protección de los datos personales, sin contar con que el uso indebido de datos personales sensibles (incluida la información genética) puede tener efectos socio-económicos importantes.

El ser humano a lo largo de su vida va dejando una enorme estela de datos personales que se encuentran dispersos y con el uso de la tecnologías *como big* data, la

velocidad del análisis e interpretación son muy sencillas, lo que puede llevar a crear un perfil determinado de la persona y por ende ser objeto de manipulaciones e interferencias en su vida, en el mejor de los casos. En este punto es donde resalta la asimetría que existe entre los titulares del dato versus el poder de a) las corporaciones que son las que colectan la información sobre las personas y b) los gobiernos que sin una adecuada atención de la privacidad debilitan la democracia, porque es clara la desventaja del titular del dato, que carece de posibilidades de influir en los mecanismos de colecta y procesamiento de sus datos. De ahí que la discriminación pasa a ser un problema de privacidad, en una sociedad en que cada vez más decisiones se toman teniendo como base análisis estadísticos.

Al final tenemos que el aumento en la cantidad de personas y dispositivos interconectados digitalmente ha revolucionado la manera de generar, compartir y acceder al dato, el cual es el oro del siglo XXI.

X. FUENTES CONSULTADAS

Agencia Española de Protección de Datos (2016) *Ley orgánica 15-1999*. Recuperado desde: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia (2014). Recuperado de: http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014

Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden al artículo 16 (2009) México, Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf

Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos (2009) Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf

Evans Dave (2011) *Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo*. Recuperado de: www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf

Facebook (2015) *Política de Datos*, EUA, recuperado de: https://es-es.facebook.com/about/privacy

Google (2016) *Te damos la bienvenida a la Política de privacidad de Google*, EUA, recuperado de: https://www.google.com/policies/privacy/

Grupo de Trabajo del artículo 29 (2007), *Dictamen 4/2007 sobre el concepto de datos personales,* Unión Europea, Directiva 95/46/CE.

INAI, Instituto Nacional de Acceso a la Información Pública y Protección de Datos Personales (2016) *Curso Sensibilización para la Trasparencia y la Rendición de Cuentas,* México, Recuperado de: http://cevifaiprivada.ifai.org.mx/swf/cevinaiv2/cevinai/campus.php

LGTAIP, Ley General de Transparencia y Acceso a la Información Pública (2015), México, Cámara de Diputados. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/index.htm

LFTAIP, Ley Federal de Transparencia y Acceso a la Información Pública (2016), México. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/index.htm

LFPDPPP Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010), México. Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/index.htm

LGPDPPSO, LEY General de Protección de Datos Personales en Posesión de Sujetos Obligados, (2017) México, Recuperado de: http://www.diputados.gob.mx/LeyesBiblio/index.htm

*Las Tres Leyes de la Robótica y los Tiempos de Smartphones Actuales (*2015). Recuperado de: http://revistaprotecciondatos.com/2015/09/17/las-tres-leyes-de-la-robotica-y-los-tiempos-de-smartphones-actuales/

Microsoft (2016) *Declaración de privacidad de Microsoft*, recuperado de: https://privacy.microsoft.com/es-es/privacystatement

Navas Navarro, Susana (2015) *Computación en la nube: Big Data y protección de datos personales,* Recuperado de: http://www.indret.com/pdf/1193_es.pdf

Open Things Lab (2015) VIDEO: *"Internet de las cosas*". Recuperado de: https://youtu.be/542oTWpKPlE

Privacy by Design, (2016) *Los "7 principios fundamentales"* Recuperado desde: https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf

Protección de datos personales, compendio de lecturas y legislación (2010) México, IFAI, Cámara de Diputados, Tiro Corto Editores.

Prosoft Secretaría de Economía (2014) *Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI,* México. Recuperado desde: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_04.pdf

Pulido J. M. (2011). *Convergencias y divergencias: acceso a la información y la tutela de los datos personales*. En "Retos de la protección de los datos personales en el sector público" (pp. 79-102). México. Recuperado de http://docplayer.es/7114112-Www-infodf-org-mx-2011-instituto-de-acceso-a-la-informacion-publica-y-proteccion-de-datos-personales-del-distrito-federal.htmlRRC (2016)

Red por la Rendición de Cuentas, *Boletín semanal* del 24 al 31 de enero 2016, México, recuperado de: http://rendiciondecuentas.org.mx/wp-content/uploads/2016/02/5to-boletin-enero-2016.pdf

Twitter (2015) *Política de Privacidad*, Recuperado de:

http://www.twitterenespanol.net/privacy_policy.php

Vázquez, Rubén (2015), Conferencia "*La amenaza del Internet de las cosas*" en Campus Party México, Recuperado de: https://youtu.be/QKrFNQA99qw

VIDEO *Conversaciones en la azotea: Big Data. Normativa, uso y derecho al olvido (1)*)

Waze (2016) *Sobre nosotros*, recuperado de: https://www.waze.com/es-419/about.