TFJA

TRIBUNAL FEDERAL
DE JUSTICIA ADMINISTRATIVA

LA PROTECCIÓN DE DATOS PERSONALES REVISIÓN CRÍTICA DE SU GARANTÍA EN EL SISTEMA JURÍDICO MEXICANO

Guillermo A. Tenorio Cueto
(Coordinador)

Centro de Estudios Superiores en materia de Derecho Fiscal y Administrativo

COLECCIÓN DE ESTUDIOS JURÍDICOS

La protección de datos personales
Revisión crítica de su garantía en el sistema jurídico mexicano

Guillermo A. Tenorio Cueto
(Coordinador)

México
2018

TFJA

TRIBUNAL FEDERAL
DE JUSTICIA ADMINISTRATIVA

2018
ISBN: 978-607-8140-26-8
Publicación editada por el Tribunal Federal de Justicia Administrativa con domicilio en Insurgentes Sur 881, Torre "O", Col. Nápoles, Del. Benito Juárez, C. P. 03810, Ciudad de México, www.tfja.gob.mx.

ÍNDICE

PRIMERA PARTE

La protección de datos en el sistema jurídico mexicano

CAPÍTULO PRIMERO
La autodeterminación informativa y sus principios

Guillermo A. TENORIO CUETO[1]

SUMARIO

I. INTRODUCCIÓN

El presente trabajo busca proponer una fundamentación de los principios que irradian del derecho a la autodeterminación informativa previsto en nuestra Constitución Política y que ha dado origen legal al tratamiento de datos personales tanto en lo público como en lo privado.

Ha pretendido hablar en un primer momento del derecho a la vida privada como origen y motor de este nuevo derecho para contextualizar al lector sobre todo el andamiaje previo que ha supuesto la construcción del derecho que nos ocupa. He partido de la base que el derecho a la vida privada no puede ser soslayado por todo aquel que aborda los temas de protección de datos personales.

A partir de ello, he tratado de proponer una revisión de cada uno de los principios que refieren los ordenamientos jurídicos en materia de protección de datos,

[1] El autor es actualmente Director del Posgrado de la Escuela de Gobierno y Economía de la Universidad Panamericana. Autor de diversos libros en materia de libertades informativas. Miembro del Sistema Nacional de Investigadores de México.

esperando que al lector le pueda servir como una referencia importante para el desarrollo de los múltiples aspectos que de ellos se derivan.

II. EL DERECHO A LA VIDA PRIVADA Y LA AUTODETERMINACIÓN INFORMATIVA

La vida privada es aquella que no está dedicada a una actividad pública[2] y, que por ende, es intrascendente y sin impacto en la sociedad de manera directa[3]; en donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan, no son de su incumbencia ni les afecta. Ella se encuentra protegida desde diversas perspectivas dentro de los diferentes marcos constitucionales[4], pero la más importante es donde se protege la misma de cara a los posibles abusos que puedan existir por parte del poder o bien de los abusos que puedan tenerse por parte de otros particulares[5].

Hoy en día cuando nos referimos a la vida privada en los marcos constitucionales también hablamos de la autodeterminación informativa como un derecho constitucional inserto a la vida privada y que, sin lugar a dudas, con el advenimiento de las nuevas tecnologías, completa el cuadro de protección del derecho que referimos.

La vida privada se excluye del principio de máxima publicidad, principio rector de la política de transparencia y del derecho de acceso a la información contenido en las constituciones que prevén dicho derecho. Una de las típicas excepciones al principio de máxima publicidad es el ámbito de la confidencialidad, es decir, el ámbito que tiene toda persona para mantener en reserva su información sin que nadie pueda utilizarla sin su consentimiento[6].

---

2 Habermas, Jürgen, *Historia y crítica de la opinión pública,* Barcelona, Gustavo Gili, 2004, p. 50.

3 Carrillo, Marc, *El derecho a no ser molestado*, Navarra, Thomson Aranzadi, 2003, p. 44. Refiere el autor que: "… es la potestad del titular a vivir solo y a no ser molestado, que permite al individuo decidir soberanamente sobre su independencia personal".

4 En el caso mexicano, protegido en el Artículo 16 constitucional.

5 Carrillo, Marc, *op. cit*., p. 44.

6 Desantes Guanter, José María, *Derecho a la información*, Valencia, Fundación Coso, 2004, p. 230. Así, el autor refiere que: "… en ningún caso se puede penetrar en la intimidad de las personas contra su voluntad…".

Dentro de la esfera que denominamos "vida privada" se desarrolla otro derecho que ha cobrado fuerza en materia de autodeterminación informativa que es el llamado "derecho a la intimidad". Este derecho es aquel centrado en lo más profundo de la persona, donde se desarrollan sus pensamientos, aficiones, preferencias sexuales, preferencias políticas, creencias religiosas y demás situaciones que solo le pertenecen a la persona pudiéndolas compartir con un número muy reducido de personas[7]. El derecho a la intimidad encontrará fuerte relación con la autodeterminación informativa pues dentro de ella, cuando hablamos de datos sensibles, nos referiremos a aquellos datos vinculados a esta esfera íntima de la persona.

Tanto el derecho a la vida privada, como el derecho a la intimidad adquieren relevancia en la autodeterminación informativa al constituir el núcleo central de la administración, de la información personal que solo por voluntad es susceptible de ser compartida. Normalmente, en los marcos constitucionales democráticos estos derechos estarán en franca oposición con la publicidad de la información, la cual siempre deberá velar por la protección de ambos y no solo ello, cuando llegan a colisionar, permitirá que estos en la mayoría de las ocasiones triunfen sobre la publicidad.

Existen otros derechos que pueden violentarse con la invasión a la vida privada y a la intimidad como son: el "derecho al honor" y el "derecho a la propia imagen" los cuales, en conjunto de la vida privada formarán lo que la tradición civilista ha denominado los "derechos de la personalidad", y que han cobrado especial preponderancia cuando hay tratamientos inadecuados de datos personales[8].

[7] El derecho a la intimidad significará: "… la absoluta soledad, en donde la persona vive íntegra y absolutamente su vida auténtica". *Ibidem*, p. 229.

[8] En ese sentido, la Suprema Corte de Justicia de la Nación en su criterio "DERECHO A LA VIDA PRIVADA. SU CONTENIDO GENERAL Y LA IMPORTANCIA DE NO DESCONTEXTUALIZAR LAS REFERENCIAS A LA MISMA", ha referido un catálogo enunciativo de derechos conexos con la vida privada como lo son: "… el derecho de poder tomar libremente ciertas decisiones atinentes al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular". Tesis 1a. CCXIV/2009, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXX, diciembre de 2009, p. 227.

Es por ello que es de esencial importancia que los retos fundamentales del derecho a la privacidad hoy en día estarán en proteger a este conjunto de derechos.

III. LA CONFIDENCIALIDAD DE LA VIDA PRIVADA Y LA AUTODETERMINACIÓN INFORMATIVA

De manera complementaria habría que decir que la vida privada tiene en la confidencialidad a su principal atributo[9]. En el caso de la información que guarda especial relación con la vida privada o íntima de las personas, la limitación a la publicidad se presenta como natural al manejo de aquella. En este caso, es preciso que dicha información sea clasificada con tal naturaleza de confidencial, por tratarse de un bien jurídico que en ponderación con lo público no participara de dicho elemento. La información confidencial no es por esencia información pública y en nada abona a lo público. La confidencialidad conlleva un no hacer (la divulgación) y un hacer (el manejo sigiloso de la información).

A pesar de lo anterior, puede darse el caso que a partir de la información confidencial obtengamos datos estadísticos que nos sirvan para la decisión pública, pero dicha utilización de la información estará supeditada a un proceso de disociación[10] en donde la vida privada o íntima no sea menoscabada.

La información confidencial no podrá ser revelada, salvo que medie consentimiento del particular que la proporcionó. Es más, para efectos de este tipo de información, el poder público deberá en todo momento asumir una serie de mecanismos de seguridad para el debido resguardo y protección siendo que, desde su obtención, se deberá informar al titular de la información que se hará con ella, para que fines se obtiene, si será susceptible de divulgación y como se efectuará su

[9] Según el Diccionario de la lengua de la Real Academia Española, la confidencia obedece a "la acción de confiar reservada o secretamente algo a una persona de confianza". En ese sentido el carácter de guardar la confidencialidad corresponderá a quien se le entregó la información.

[10] Cabe recordar que en la Ley Federal de Datos Personales en Posesión de los Particulares, la disociación se encuentra contemplada en el Artículo 3o., fracción VIII, en donde se refiere como un mecanismo aceptable para la divulgación de datos estadísticos que se nutren en primer lugar de datos de la vida íntima o privada de las personas. En ese sentido dicho proceso de disociación involucrará un desgajamiento entre la información que le da origen y el dato que nos interesa publicar y en donde sería imposible identificar a las personas que nutren en su conjunto el dato estadístico.

almacenamiento[11]. Lo mismo sucede en el ámbito privado donde la información entregada con el sello de confidencial asumirá un tratamiento específico en los llamados responsables.

En el caso del poder público, la protección de información personal por parte del Estado debe ser garantizada, más no como una limitación del derecho del acceso a la información, sino como una prerrogativa fundamental derivada del derecho a la vida privada a partir de lo que se denomina "autodeterminación informativa" siendo que dicha protección deberá de cubrir, todas las previsiones de seguridad de la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados[12]. De igual manera en el ámbito privado, la garantía al cuidado de la información estará llamada a respetar no solo la vida privada, la intimidad y la autodeterminación informativa, sino también los derechos al honor y en ocasiones la propia imagen.

Esta llamada autodeterminación informativa garantizará al ciudadano una serie de derechos que son conocidos por su acrónimo como los derechos ARCO, esto es: *a)* Acceso, *b)* Rectificación, *c)* Cancelación y *d)* Oposición. Acompañando a estos derechos constituirán obligaciones de todos los sujetos obligados, la institucionalización de medidas de seguridad en tres vías para el aseguramiento de un tratamiento adecuado. Por un lado, habrá estándares de seguridad técnicas destinadas a la protección y resguardo seguro de la información, las medidas de seguridad física las cuales asegurarán un tratamiento de la información contenido en soporte tradicional y las medidas de seguridad administrativas las cuales estarán destinadas a proponer mecanismos o procedimientos que irradien a todo el enramado organizacional para el debido cuidado de la información de carácter personal.

---

[11] Villanueva, Ernesto, *Derecho de acceso a la información pública en Latinoamérica*, México, IIJ-UNAM, 2003, p. LXXIV. Así se encuentra contemplado tanto en la Ley Federal de Acceso a la Información Pública como en la Ley Federal de Datos Personales en Posesión de Sujetos Obligados.

[12] *Idem*. En el ordenamiento jurídico mexicano la defensa a la vida privada encontrará, tanto en el Artículo 6o. como en el 16 de la Constitución, manifestaciones claras de protección, es por ello que tanto la Ley Federal de Transparencia y Acceso a la Información como la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados reforzarán el carácter confidencial de la información que goza de esta característica.

Ello implicará no solo un deber de cuidado sino una responsabilidad que, en el caso de ser incumplida, implicará una sanción para el funcionario público tratándose de información otorgada a los órganos del Estado o bien a los responsables del tratamiento, tratándose de entidades de naturaleza privada que traten datos.

En el caso de los sujetos obligados de naturaleza pública que trabajen con datos personales y busquen proteger el derecho de acceso a la información, deberán realizar acciones que por un lado, potencien dicho derecho pero que por otro salvaguarden la información personal. En ese sentido tanto la disociación, es decir, la separación de datos de un conjunto, como las versiones públicas, en otras palabras, el ocultamiento de datos personales de los documentos, resolverán tal situación.

Cuando existe un órgano garante de la materia, éste estará llamado a velar por la protección de ambos derechos exigiendo por un lado la vivencia del principio de máxima publicidad y por otro deberá garantizar la protección y no injerencia en la vida privada de los ciudadanos que pudieran verse afectados[13].

Como ya adelantamos, entenderemos que la clasificación de la información por razón de la confidencialidad estará vinculada a la protección de los datos personales concernientes a personas identificadas o identificables. Está referida información confidencial a diferencia de la información clasificada como reservada, no se encontrará sujeta a ninguna temporalidad, es decir, que en todo momento deberá permanecer con el carácter privativo de su naturaleza específica.

Esta información en primer lugar, es aquella donde los particulares entregan a los órganos del Estado con ese carácter, pero también se considera como información confidencial aquella como: *a)* los secretos bancario, fiduciario y bursátil; *b)* secreto industrial y comercial; *c)* secreto fiscal y postal.

---

[13] Sabemos que la existencia de un órgano garante en materia de transparencia y acceso a la información constituye "… otra de las piedras angulares para hacer efectivo el derecho de acceso a la información". *Cfr*. *Ibidem*, p. LXIV; pero, ¿dicho órgano debe también atender la protección de datos? Resulta curioso que quien proteja el principio de máxima publicidad en materia de derecho de acceso a la información deba también atender el principio de máxima privacidad en materia de autodeterminación informativa. Es por ello que en otros países, como Argentina o España, existan agencias especializadas en la materia, situación que en México es una realidad lejana.

A la par, esta confidencialidad no supone que existan casos en que por las necesidades propias del interés público, esta información en ocasiones sea susceptible de ser divulgada. En ese sentido el consentimiento del titular de la información quedará en un segundo término por la relevancia de la información como es el caso de: *a)* la información que se encuentre en registros públicos o fuentes de acceso público; *b)* aquella que por mandato de alguna ley tenga el carácter de pública; *c)* aquella que se vea afectada por una orden judicial o bien; *d)* aquella que es divulgada por razones de seguridad nacional o para proteger derechos de terceros.

Es importante referir que la negativa de acceso a la información en las causales de confidencialidad no significa que en ocasiones no pueda entregarse el resto de la información que completa una solicitud. Para la protección de la confidencialidad el servidor público podrá en su caso, eliminar cualquier rastro de dato que comprometa la privacidad y en su caso podrá entregar el resto de la información en un ánimo de potenciar el principio de máxima publicidad.

IV. LOS DIVERSOS TIPOS DE DATOS QUE EMERGEN DE LA VIDA PRIVADA

Los datos personales los podemos definir como cualquier información[14] concerniente a una persona física identificada o identificable, esto significa que no es necesario que la vinculación directa entre el dato y el conocimiento o identificación de la persona, sino que basta la referencia de un dato que permita una posible identificación, para que en su caso deba protegerse y resguardarse. Para ello puede servirnos precisar que una persona física es identificable cuando su identidad pueda determinarse, directa o indirectamente, mediante cualquier información. De igual manera, será necesario precisar que si para dicha identificación es necesario un plazo o actividades desproporcionadas lo común es que ese dato ya no se considere como alguno que vulnere la vida privada de las personas.

[14] "Esto significa que puede tratarse de información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo en la medida en que concierna a una persona física e identificable". *Cfr.* Téllez, Julio, *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México*, México, IIJ-UNAM, 2013, p. 134.

En casi todos los sistemas jurídicos donde se han contemplado regulaciones en materia de protección de datos encontramos que, los mismos suelen clasificarse en tres grandes grupos, más allá que luego podamos encontrar clasificaciones particulares. Así encontramos: *a)* datos de identificación; *b)* datos sensibles; y *c)* datos patrimoniales[15]. En cada uno de estos grupos encontraremos efectos diversos sobre su tratamiento e inclusive sobre los efectos de las sanciones respecto a una posible violación de los mismos.

El primer gran grupo es el de los datos de identificación. Ellos son los que, afectando la vida privada, no inciden en la vida íntima, que en principio y solo en principio, no darían pie a ningún tipo de discriminación. En ese sentido y únicamente por citar algunos ejemplos encontraremos: nombre, domicilio, teléfono, código postal, edad o correo electrónico. En principio con la obtención de cada uno de estos datos no estaríamos en presencia de ningún tipo de vulneración a la vida íntima de las personas. Con su tratamiento obtenemos información relativa a la identificación de la persona y que si bien conciernen a su vida privada no requerirán un consentimiento expreso para su tratamiento. Ello no significa que su vulneración pueda ser sancionable o que sobre dichos datos no se actualicen los derechos ARCO por el contrario, como cualquier dato es susceptibles de protección en todas sus dimensiones y solo estarían sujetos al tratamiento a partir de lo que en la ley mexicana se conoce como consentimiento tácito.

El segundo grupo de datos es el concerniente a los datos de naturaleza sensible. Este grupo tiene la peculiaridad de que, con motivo de su tratamiento afectan a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este[16]. En particular, se consideran

[15] *Idem*. Llama la atención que en el caso mexicano encontremos expresamente referidas las dos primeras categorías pero respecto a la tercera, es decir los datos patrimoniales solo los encontremos a partir de la referencia que ella hace a los mismos dentro del articulado de la norma. De cualquier manera la misma ley mexicana asume que datos patrimoniales y datos personales sensibles deberán tener el mismo tratamiento.

[16] En ese sentido, Pablo Lucas Murillo de la Cueva refiere que el derecho a la intimidad está identificado "con la pretensión del individuo de excluir del conocimiento ajeno cuanto guarda relación con sus relaciones sexuales, conyugales, paterno-filiales y familiares, con su cuerpo, con

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. La definición en la ley mexicana "es jurídicamente desafortunada, pues contiene términos no jurídicos, equívocos y subjetivos"[17].

El tercer grupo de ellos son los datos de naturaleza patrimonial. Este grupo diferenciado agrupa a aquellos datos que revelen la información de carácter económica o patrimonial de una persona. Solo para ilustrar sirvan como ejemplos: datos de la cuenta bancaria, datos de ingresos o egresos, bienes muebles o inmuebles, inversiones o monto de pólizas de seguros.

Con esta distinción hecha entre los distintos tipos de datos, es necesario también hacer una distinción entre los diversos tipos de tratamientos de datos. En ese sentido cuando se habla de tratamiento nos estamos refiriendo a:

a) Obtención;
b) Uso;
c) Divulgación; y/o
d) Almacenamiento de datos personales, por cualquier medio.

El uso abarca cualquier acción de acceso, manejo, aprovechamiento o disposición de datos personales. Por su parte, la obtención se referirá a cualquier proceso en donde el dato sea captado tanto de manera directa como indirecta. En el caso de la divulgación, estaremos en presencia de toda acción tendiente a difundir, compartir o transferir los datos a cualquier entidad externa al responsable sea de naturaleza pública o privada y en donde los datos del titular puedan ser susceptibles de nuevas finalidades de tratamiento o bien, de finalidades análogas a las que realizaba el responsable originario. Por último cuando hablamos de almacenamiento nos referimos a todo proceso dentro de la organización que tiende a guardar, conservar, retener los datos del titular en algún soporte físico, electrónico y que suponga

su salud, con su muerte, con sus pensamientos, creencias, aficiones y afectos" *Cfr*. Lucas Murillo de la Cueva, Pablo, "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta. Cuadernos de Derecho*, Donostia-San Sebastián, núm. 20, 2008, p. 46.

[17] *Idem.*

la custodia de la información, por el tiempo que sea necesario para cumplir, con las finalidades del tratamiento o con el tiempo extraordinario que el responsable deba guardar la información, ajeno a la temporalidad de las finalidades, ya sea para el cumplimiento de obligaciones impuestas por otras legislaciones o bien, por la utilidad que le representa el dato. Todo ello nos aproxima a entender que la protección de datos es integral y no solo queda reducida a un espectro limitado de acción y protección.

V. LOS PRINCIPIOS ORIENTADORES DE LA AUTODETERMINACIÓN INFORMATIVA

El establecimiento de principios en materia de protección de datos en todos los sistemas orientados a su protección, es de capital importancia pues, ilustra de manera ordenada el quehacer rector para su salvaguarda, es decir, que más allá del tipo de dato o del tipo de tratamiento, los responsables o los sujetos obligados estarán vinculados a una serie de deberes de manejo y conservación de la información. En ese sentido encontramos una serie de principios comunes en casi todos los ordenamientos que trabajan con datos personales los cuales son: *a)* licitud; *b)* consentimiento; *c)* información; *d)* calidad; *e)* finalidad; *f)* lealtad; *g)* proporcionalidad; y *h)* responsabilidad. Cada uno de ellos orientará una forma de tratar los datos.

El principio de licitud, obliga al responsable que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación doméstica y el derecho internacional. Para algunos autores, como Noe Riande, el principio de licitud "… indica que al sujeto de los datos se le debe advertir que se han (están o serán) recolectados sus datos, el fin para el cual se requieren sus datos, el tipo de datos necesarios para dicha finalidad, las operaciones y transmisiones que se realizarán con ellos, el tiempo por el que se conservarán, y dónde terminarán los datos cuando ya no se necesiten (a menos que el procesamiento, lo ordene o autorice un mandato de ley o de autoridad judicial competente)"[18]. Sin lugar a equívocos, el principio de licitud responde a una sujeción a la ley, a todos aquellos responsables y sujetos obligados que traten datos personales. Ordena, sistematiza, impone deberes, obligaciones y

[18] *Cfr*. Riande Juarez, Noé Adolfo, "El derecho a la autodeterminación informativa", *Revista Praxis de la Justicia Fiscal y Administrativa*, México, número 21, julio-diciembre de 2017, p. 11.

sobre todo orienta en el debido cumplimiento del tratamiento de datos a partir del marco constitucional y legal que rodea a la materia.

El segundo de ellos, es el principio de consentimiento[19]. Para cualquier tratamiento de datos, la regla general será que, el responsable obtenga el consentimiento del titular a menos que por mandato de ley no sea exigible con arreglo a lo previsto en el Artículo 10 de la Ley. La solicitud del consentimiento deberá en todo caso ir referida a una finalidad o finalidades determinadas, previstas en el documento que hemos llamado aviso de privacidad. Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento. En las diversas legislaciones que contemplan tratamiento de datos, hemos encontrado diversas formas de referirse al consentimiento. En algunas hemos encontrado expresiones del mismo de manera lisa y llana, en otras hemos encontrado distinciones dentro del mismo consentimiento encontrando dos tipos del mismo: expreso y tácito.

Cuando el consentimiento está asociado a datos de identificación, los efectos más notables, los vincularemos al tipo de consentimiento que la persona nos tiene que dar para el tratamiento que hagamos de los mismos. En ese sentido, hablaremos de un consentimiento tácito, es decir, que la persona que nos proporcione dichos datos simplemente no se opondrá al tratamiento. Por el tipo de dato que el titular está entregando al responsable, se presume que no existirá posible discriminación y por ello solo acudiremos a una aceptación del documento llamado aviso de privacidad sin una expresión afirmativa palpable más que el otorgamiento de los datos, esto es, que para este tipo de consentimiento no es necesario una firma, en donde se autorice el tratamiento de los datos o una huella digital que avale el

[19] "Principio rector y de una trascendencia fundamental en el ámbito del derecho de autodeterminación informativa… el cual tiene una íntima relación con el poder de control sobre nuestros datos personales. Siempre el tratamiento de datos personales debe estar amparado en un título que habilite su utilización. Es por ello que resulta esencial el consentimiento del titular de los datos. En consecuencia este principio se constituye en el eje central en el derecho de autodeterminación informativa y supone que el titular de los datos es el único que tiene derecho a decidir quien, como, cuando y para que se tratan sus datos". *Cfr.* Orrego, César Augusto, "Una aproximación al contenido constitucional del derecho de autodeterminación informativa", *Anuario de Derecho Constitucional Latinoamericano*, Bogotá, año XIX, 2013, p. 326.

tratamiento, o cualquier signo inequívoco donde quede plasmado el consentimiento, basta con la simple y llana entrega de los datos personales.

Para el caso de otro tipo de consentimiento, no podemos hablar de una simple aceptación de tratamiento, por el contrario al tratarse de datos sensibles y patrimoniales el consentimiento tendrá que ser expreso, es decir, que la persona que nos proporcione dichos datos deberá dejar de manifiesto que consiente que los datos entregados y puedan ser tratados por el calibre o magnitud de la información que dichos datos arroja, en su caso podrían generar un tipo de discriminación. Como ya hemos adelantado este tipo de consentimiento debe manifestarse con signos inequívocos que reflejen la voluntad del titular de los datos.

Como ya habíamos adelantado, para los casos en los que la legislación doméstica solo se refiere al consentimiento sin hacer diferencias entre tácito y expreso, el mismo deberá obtenerse de manera indubitable, y como siempre ocurre con un tratamiento de datos, quedará en todo momento el titular en la posibilidad de acceder a los mecanismos de protección previstos en la legislación.

Otro de los principios prototípicos en materia de autodeterminación informativa es el denominado principio de información[20]. Sabemos que el responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento, que serán sometidos sus datos personales a través de un documento que se llama aviso de privacidad. El aviso de privacidad deberá contener, al menos, la siguiente información:

a) La identidad y domicilio del responsable que los recaba;
b) Las finalidades del tratamiento de datos;
c) Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
d) Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;

[20] El principio de consentimiento del cual habíamos hablado supone la característica de ser informado y esto supone que el titular "debe tener la posibilidad de conocer y reflexionar en torno a los beneficios y eventuales desventajas que acarrea el tratamiento de datos". *Idem.*

e) En su caso, las transferencias de datos que se efectúen;
f) El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley; y
g) En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de ese tipo de datos.

Resulta medular saber, que el aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, con una estructura y diseño que facilite su entendimiento. Es necesario recordar que, para la difusión de los avisos de privacidad, el responsable puede valerse de formatos físicos, electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular. De igual manera es muy importante recordar que no todos los avisos de privacidad son iguales. Sabemos que existen diversos avisos de privacidad en formatos con espacio limitado, en los cuales es común en diversas legislaciones que se contemplen solo como datos a otorgar al titular:

a) Nombre del responsable;
b) Finalidades para las que se recaban; y
c) Mecanismos para acceder al aviso de privacidad, integral o completo.

No debemos olvidar que, prácticamente todas las legislaciones en materia de datos, el aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de manera previa al tratamiento, cuando la captación de los mismos se hace de manera directa, y cuando se realiza de manera indirecta, es decir, que se obtienen los datos por un tercero, el aviso de privacidad se hará de manera inmediata en tanto se tengan los datos.

Sobre este último punto, es importante tener en cuenta que el responsable deberá observar lo siguiente para la puesta a disposición del aviso de privacidad:

a) Cuando los datos personales, sean tratados para una finalidad prevista en una transferencia consentida o se hayan obtenido de una fuente de acceso público, el aviso de privacidad se deberá dar a conocer en el primer contacto que se tenga con el titular; o

b) Cuando el responsable, pretenda utilizar los datos para una finalidad distinta a la consentida, es decir, vaya a tener lugar un cambio de finalidad, el aviso de privacidad deberá darse a conocer previo el aprovechamiento de los mismos.

No debemos olvidar que para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable[21].

Por su parte, el principio de calidad, obligará a que los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados. Este principio presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados 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. El responsable deberá adoptar los mecanismos que considere necesarios para procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

Otro de los principios es el de finalidad, el cual supone que los datos personales solo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en los documentos llamados avisos de privacidad. Lo anterior obliga a que la finalidad o las finalidades establecidas en dicho documento de privacidad deberán ser determinadas, 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. Lo normal en toda legislación en materia de protección de datos es que

[21] *Ibidem*, p. 327.

existen dos tipos de finalidades: Finalidades que dieron origen a la relación jurídica y finalidades secundarias o que no son necesarias para la relación jurídica.

El principio de lealtad, establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad. Este principio ordenará a que, no se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales. De hecho, como sabemos, este principio es el origen de la actividad delictuosa contemplada en la misma ley y en donde se señala como un tipo penal especial justamente el recabar datos de manera engañosa.

De igual manera, el principio de proporcionalidad cobrará vida al entenderse que solo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido. Este principio ha generado toda una gama de posibilidades en relación con los principios de consentimiento e información respecto a las finalidades para las cuales se recaban datos. Esto significa que este principio orienta el establecimiento de finalidades primarias y secundarias dentro del aviso de privacidad y sobre todo las vincula con la proporción del objeto del tratamiento.

Por último, el principio de responsabilidad supondrá una la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo custodia o posesión de cualquier responsable de protección de datos, se encuentren o no en el territorio de donde surja la restricción. Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines. Este principio encuentra su concreción en la legislación a partir de lo que llamamos medidas de seguridad las cuales son: medidas de seguridad físicas, medidas de seguridad administrativa y medidas de seguridad técnicas.

VI. A MANERA DE CONCLUSIÓN

Los principios en materia de la autodeterminación informativa se encuentran directamente ceñidos a la voluntad del titular de los datos, el ejercicio ordenado y adecuado del responsable del tratamiento. Cada uno de ellos cobra sentido a partir de la protección de la vida privada, así como de la vida íntima de la persona. Desde luego la confidencialidad y la secrecía que supone la vida privada no pueden romperse a menos que su titular lo consienta.

Cada uno de los principios que hemos revisado en este apartado constituye la tierra fértil en la cual se construye nuestro derecho a la autodeterminación informativa pero también cada uno de ellos produce los frutos adecuados para un sano ejercicio de aquel derecho. Como hemos observado de cada uno de ellos se desprenden acciones concretas que lo materializan por lo que es indispensable su estudio y observancia de manera permanente y no su desdeño o poca valoración.

VII. FUENTES DE INFORMACIÓN

CARRILLO, Marc, *El derecho a no ser molestado*, Navarra, Thomson Aranzadi, 2003.

DESANTES GUANTER, José María, *Derecho a la información*, Valencia, Fundación Coso, 2004.

HABERMAS, Jürgen, *Historia y crítica de la opinión pública,* Barcelona, Gustavo Gili, 2004.

LUCAS MURILLO DE LA CUEVA, Pablo, "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta. Cuadernos de Derecho,* Donostia-San Sebastián, núm. 20, 2008.

ORREGO, César Augusto, "Una aproximación al contenido constitucional del derecho de autodeterminación informativa", *Anuario de Derecho Constitucional Latinoamericano,* Bogotá, año XIX, 2013.

RIANDE JUAREZ, Noé Adolfo, "El derecho a la autodeterminación informativa", *Revista Praxis de la Justicia Fiscal y Administrativa*, México, número 21, julio-diciembre de 2017.

Semanario Judicial de la Federación, Novena Época, t. XXX, diciembre de 2009.

TÉLLEZ, Julio, *Lex Cloud Computing. Estudio jurídico del cómputo en la nube en México*, México, IIJ-UNAM, 2013.

VILLANUEVA, Ernesto, *Derecho de acceso a la información pública en Latinoamérica,* México, IIJ-UNAM, 2003.

CAPÍTULO SEGUNDO
El consentimiento en materia de protección de datos

Cynthia CRUZ CHAVEZ[22]

SUMARIO

I. INTRODUCCIÓN

La importancia del consentimiento radica en la representación de la voluntad de la persona, etimológicamente proviene del verbo activo transitivo "consentir" y del sufijo "miento" que indica acto, estado y efecto de[23]. En términos generales, se puede entender como autorizar, aceptar y que tiene como consecuencia que la persona se vincula jurídicamente con otro. De ahí que se haga necesario el hacer un alto para analizar el consentimiento *per se* para posteriormente analizarlo en protección de datos.

Como señalé, el consentimiento es un requisito *sine qua non* para vincularse con el otro; sin embargo, no todas las personas tienen el mismo nivel cultural, socioeconómico, etc. Lo cual puede ser una desventaja para alguna de las partes. En

[22] Licenciada en Derecho por la Universidad Panamericana. Maestra en Tecnologías de la Información por el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC). Docente en diversas universidades de nuestro país. Experta en materia de Tecnologías de la Información, Telecomunicaciones y Propiedad Intelectual.

[23] Véase: *https://definiciona.com/consentimiento/*.

ese tenor, De la Peza, establece un atinado señalamiento en el origen del consentimiento:

> …
>
> Conviene, sin embargo, hacer una importante distinción, pues si bien es cierta e indiscutible la igualdad ontológica de todos los seres humanos, en la realidad social es evidente la desigualdad de condición de los hombres por razones morales, culturales, económicas, sanitarias, etc., que han dado lugar a que se sostenga con razón, que la justicia impone la necesidad de tratar igual a los iguales y desigual a los desiguales, principio que debe informar a la ley positiva[24].

En este sentido el Código Civil Federal (CCF) prevé tal situación, denominada en la doctrina como la lesión y que se encentra en su Artículo 17, que más adelante se detallará.

El consentimiento es la única forma de establecer una relación jurídica entre personas, de ahí que tenga una importancia vital, que exista un entendimiento de los involucrados, respecto a qué derechos y obligaciones están aceptando. Una vez que se otorga el consentimiento esos derechos y obligaciones solo podrían ser anulados mediante el ejercicio de la acción y la invocación del vicio del consentimiento de que se trate.

La regulación mexicana ha establecido diferentes formalidades para otorgar el consentimiento, dependiendo de la relevancia del acto jurídico, así tenemos en materia médica, en materia civil, mercantil y en protección de datos.

En todos los casos la *ratio legis* es proteger a la persona, como lo señalaba De la Peza, al existir una variedad de diferencias en los individuos, se trata de evitar un abuso, engaño o simplemente de brindarle claridad a la persona de las implicaciones que tiene el otorgar su consentimiento.

II. EL CONSENTIMIENTO EN EL CÓDIGO CIVIL FEDERAL DE MÉXICO

El motivo de abordar en un inicio el consentimiento en el CCF, obedece a que es ahí, de donde emanan los preceptos que en la Ley Federal de Protección de Datos

[24] De la Peza, José Luis, *De las obligaciones*, México, McGraw-Hill, 1997, pp. 23 y ss.; al referirse a la obra de Planiol y Ripert, t. VI, primera parte.

Personales se establecen. Es una razón que atiende básicamente a la fuente original de las disposiciones normativas.

El CCF en su Artículo 1803 establece que el consentimiento puede ser expreso o tácito y distingue:

> I. Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y
>
> II. El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente.

El Código en su generalidad, establece cualquier forma posible para otorgar el consentimiento, de forma expresa o por presunción con la salvedad de que por ley o acuerdo entre las partes sea distinto.

En el punto número I, señalamos los vicios del consentimiento, que son una forma de no cumplir con la obligación contraída. Los citados vicios del consentimiento son:

a) El error y éste puede ser de derecho o de hecho y de cálculo;
b) El dolo; y
c) La violencia.

Cuando se alega un vicio en el consentimiento, de acuerdo al Código Civil citado, genera diferentes consecuencias, dependiendo de que vicio se trate. Para el error de hecho o derecho la invalidez del contrato y de cálculo, solo la rectificación. Cuando el vicio del consentimiento fue con dolo o violencia, se decreta la nulidad del contrato.

A manera de recordatorio, el dolo se prevé en el Artículo 1815 del citado Código como cualquier sugestión o artificio que se emplee para inducir a error o mantener en él a alguno de los contratantes; y por mala fe, la disimulación del error de uno de los contratantes, una vez conocido, a su vez la violencia se define en el 1819 cuando se emplea fuerza física o amenazas que importen peligro de perder la vida, la honra, la libertad, la salud, o una parte considerable de los bienes

del contratante, de su cónyuge, de sus ascendientes, de sus descendientes o de sus parientes colaterales dentro del segundo grado.

Aunado a lo anterior, existe la denominada "lesión", que justamente se trata de evitar lo que De la Peza comentaba, el abuso de una de las partes por diferencias de diversas índoles. El Artículo 17 establece que:

> Cuando alguno, explotando la suma ignorancia, notoria inexperiencia o extrema miseria de otro; obtiene un lucro excesivo que sea evidentemente desproporcionado a lo que él por su parte se obliga, el perjudicado tiene derecho a elegir entre pedir la nulidad del contrato o la reducción equitativa de su obligación, más el pago de los correspondientes daños y perjuicios.

La lesión no está contenida dentro de los vicios del consentimiento y pudiera ser que se debe a que cuando existe lesión en el consentimiento no es posible que se ratifique el acto, conlleva la nulidad del contrato, simple y llanamente, por lo demás no encuentro alguna justificación que amerite estar fuera de los catalogados vicios del consentimiento que prevé el CCF.

La lesión como claramente se advierte, es protectora para el consumidor que derivada de la diferencia notoria de la ignorancia y/o miseria entre aquel y el vendedor. Hay una anotación que realiza el Maestro Sánchez Medal al respecto y ayuda a clarificar cómo opera la lesión dentro de un acto jurídico:

> La lesión no está reglamentada en nuestro derecho dentro de los vicios del consentimiento, sino al principio del Código civil en las "disposiciones preliminares", pero a pesar de ello, debe considerarse la de lesión (17) como un vicio del consentimiento, que se integra con un elemento *objetivo* (obtener un lucro excesivo que sea evidentemente desproporcionado a lo que por su parte se obligue el perjudicado, pero sin señalar el monto o la cuantía de tal desproporción), y por otro elemento *subjetivo* (explotar la suma ignorancia, notoria inexperiencia o extrema miseria de otro)[25].

Como establecí, la intención del legislador es proteger al que por su condición puede ser víctima o abusado de su propia situación y creo que en ese sentido es que marca la disparidad entre las partes, a diferencia de los vicios del consentimiento,

[25] Sánchez Medal, Ramón, *De los contratos civiles*, México, Porrúa, 1993, p. 57.

que no obedecen a una situación de disparidad entre las partes, sino más bien a diferentes situaciones, pero partiendo de la base que las partes están justamente *"a la par"*.

De los efectos jurídicos de los contratos cuando existe un vicio del consentimiento la Dra. Fernández señala:

> La mayoría de la doctrina moderna[8] no contrapone ambos términos, sino que entienden que su ámbito de actuación se produce en planos diferentes. Así, consideran la invalidez como causa de ineficacia, como una clase de ineficacia en los supuestos en los que ésta obedece a una sanción del ordenamiento, y que esta última sería el género y la invalidez la especie[9].
>
> En definitiva, que todo contrato inválido es ineficaz, pero no todo contrato ineficaz es inválido.
>
> Esta premisa considera que la invalidez incluye la nulidad y la anulabilidad. Pero en los casos en el que surgen nuevas formas de sanción, que son híbridos entre las anteriores, la concepción de la invalidez no queda tan nítida. Ello ocurre en las nuevas leyes especiales que prevén nuevas formas de ineficacia y que al contemplar formas de sanción particular para el incumplimiento de los actos y contratos no van a encontrar encaje entre la invalidez.
>
> Se establece para estos casos de inexistencia o nulidad absoluta una misma acción imprescriptible con legitimación para interponerla cualquier interesado, incluso, declararla de oficio los tribunales…[26]

Por último, me gustaría destacar que el consentimiento se encuentra en la parte de los contratos de nuestra legislación vigente y que pudiera parecer que no todas las manifestaciones de la voluntad encuadrarían en un contrato, sino que se trataría de una declaración de la voluntad que no involucra un derecho u obligación para quien otorga ese consentimiento. En este sentido, nos ilustra el Maestro Sánchez Medal[27].

> Suelen distinguirse dos clases de declaraciones de voluntad en un negocio jurídico: las declaraciones *recepticias*, que para producir la eficacia que le es pro-

---

[26] Fernández Ramón, Francisca, "Conceptualización de la ineficacia, invalidez e inexistencia en el Derecho español", *Revista chilena de Derecho Privado*, Santiago de Chile, número 19, diciembre de 2012, *http://dx.doi.org/10.4067/S0718-80722012000200003*.

[27] Sánchez Medal, Ramón, *op. cit.*

pia deben estar dirigidas a una determinada persona (notificación al deudor acerca de la cession de un crédito, oferta contractual, desistimiento, etc.) y las declaraciones *no recepticias* que para producir sus efectos no requieren de un destinatario concreto o determinado (promesa al público, el testamento) (Trabucchi).

El consentimiento, en su segunda acepción, esto es, como *acuerdo de voluntades*, no existe cuando no hay coincidencia en las dos voluntades, lo que ocurre principalmente en los casos del llamado *error-obstáculo*, que corresponde al *"error in corpore"* o error sobre el objeto-cosa…

III. EFICACIA DEL CONSENTIMIENTO

Se ha establecido el consentimiento y las consecuencias jurídicas de otorgarlo, cuando se presenten vicios del consentimiento o la lesión y los requisitos (la formalidad), que en algunos casos, la ley impone para manifestar el consentimiento.

Para que el consentimiento sea eficaz, debe pasar la revisión de tres puntos: *a)* la capacidad de los contratantes; *b)* la ausencia de vicios; y *c)* la forma de manifestarse[28]. El Maestro Rojina Villegas añade un elemento más y que se refiere a que el acto tenga un fin, motivo, objeto y condición lícitos. Llamamos a este elemento: *d)* licitud del acto jurídico[29].

a) Capacidad de los contratantes. Esto se refiere a que los contratantes no deben ser personas de las referidas en el Artículo 450 del CCF; es decir, menores de edad y los declarados en estado de interdicción y que el Artículo 23 del CCF lo señala como una restricción a la personalidad juridicial.

Ahora bien, no deberá confundirse con la falta de legitimación, como serían prohibiciones para determinadas personas que por su cargo o nacionalidad, no pueden contratar, como por ejemplo la prohibición de los servidores públicos de formar parte del Jurado Ciudadano que establece el Artículo 60 de la Ley Orgánica del Poder Judicial Federal.

---

[28] De la Peza, José Luis, *op. cit.*, p. 225.

[29] Rojina Villegas, Rafael, *Compendio de Derecho Civil*, 26ª. ed., México, Porrúa, 1995, t. I, pp. 120-131.

b) Ausencia de vicios. En el punto anterior, detallamos cuáles son los vicios del consentimiento que establece el CCF en donde consisten y a manera enunciativa son, error de derecho, hecho o cálculo, el dolo, la violencia o intimidación y establecido en un Artículo aparte el dolo.

c) Forma de manifestar el consentimiento. Se pueden distinguir varias formas de la manifestación del consentimiento: un escrito privado, escrito privado firmado ante testigos, escrito privado ratificado ante un fedatario público y escritura pública.

Dependerá de la exigencia de la ley para que el acto jurídico revista a formalidad requerida y pueda ser eficaz, siempre y cuando cumpla con las otras condiciones.

En todos los casos, se requiere un documento escrito, que se hace necesario para el caso de un desacuerdo posterior entre los contratantes, se exhiba como documento base de la acción.

d) La licitud del acto jurídico. Esto se refiere a que cuando las partes consienten un acto, debe tener un objeto lícito, para lo cual el Artículo 1825 del CCF establece como debe ser: *i)* existir en la naturaleza; *ii)* ser determinada o determinable en cuanto a su especie; *iii)* estar en el comercio.

Por último, el CCF establece claramente que los contratos que no cumplan con la formalidad requerida, no serán válidos, aunque permite la posibilidad de convalidar el acto, cuando la ley exija determinada forma para un contrato, mientras que esté no revista esa forma no será válido, salvo disposición en contrario; pero si la voluntad de las partes para celebrarlo consta de manera fehaciente, cualquiera de ellas puede exigir que se dé al contrato la forma legal.

El CCF ya ha incorporado, para algunos casos, los medios electrónicos como forma de manifestar la voluntad, según lo establece el Artículo 1834, se tendrán por cumplidos mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta.

De acuerdo a la opinión de Bacigalupo, el ámbito de eficacia del consentimiento depende, en gran parte, del poder de decisión que el orden jurídico otorgue sobre el mantenimiento del bien jurídico al particular que es titular del mismo, reconociendo validez al consentimiento otorgado sobre la posesión, la propiedad, el patrimonio, y, en general, la libertad personal y la integridad corporal[30].

En efecto, si analizamos lo previsto anteriormente, la eficacia de los actos emana de la ley ya que en ella se establecen los requisitos para la validez de los contratos, la formalidad y los vicios del consentimiento.

IV. EL CONSENTIMIENTO EN LA PROTECCIÓN DE DATOS EN MÉXICO

Es importante señalar, que la protección de datos está protegida en la Carta Magna, en el Artículo 6o., apartado A, fracción III establece, la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

Es justamente la *ratio legios* de protección, lo que da origen a la formalidad que dispone la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), la cual señala, en primer término, la definición de consentimiento como manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

La LFPDPPP en su numeral 8, establece como presupuesto para el tratamiento de datos personales el consentimiento del titular, salvo las excepciones previstas en esa misma Ley.

A mayor abundamiento, define lo que es el consentimiento expreso como la voluntad de manifieste verbalmente o por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, así como por signos inequívocos (misma definición que en CCF, Artículo 1803), y en el tácito se establece que habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición (que es la esencia del tácito señalado en el referido 1803).

---

[30] Bacigalupo Zapater, Enrique, *Principios de Derecho Penal. Parte general*, 2ª. ed., Madrid, Akal, 1990, p. 156.

En los Artículos 12 y 13 del Reglamento de la LFPDPPP se establecen las "características" (que no es otra cosa sino la eficacia del consentimiento), los cuales cito a continuación:

> Artículo 12. La obtención del consentimiento tácito o expreso deberá ser:
>
> I. Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;
>
> II. Específica: referida a una o varias finalidades determinadas que justifiquen el tratamiento; y
>
> III. Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.
>
> El consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.
>
> Artículo 13. Salvo que la Ley exija el consentimiento expreso del titular, será válido el consentimiento tácito como regla general, conforme a lo dispuesto en el artículo 11 y 12 de este Reglamento.

Respecto a la fracción I, no son otra cosa que los vicios del consentimiento establecidos en el Artículo 1803 del CCF, sin embargo, el legislador olvidó que la lesión puede dar origen también a una nulidad total del acto, dada la gravedad con que se establece la disparidad de las partes. En este sentido, parece relevante plantearse, si la lesión podría alegarse en la protección de datos, aunque la Ley no establezca como supletoriedad el CCF.

Por lo que se refiere a la fracción II, relativa a que el consentimiento debe ir referido a una o varias finalidades determinadas que justifiquen el tratamiento, me parece que es un consentimiento limitado o restringido a la finalidad; es decir, yo otorgo mi consentimiento para que mis datos personales puedan ser utilizados para ser tratados en el caso de estudios médicos, pero si el responsable los utiliza además para publicidad, estaría utilizándolos más allá para lo que fueron otorgados En este caso, salta la duda si se estaría en presencia de un acto ilícito en virtud de que los datos personales en posesión de terceros, salvo autorización, no podría comerciar con dichos datos o bien tendría como consecuencia la ineficacia del con-

sentimiento por lo que se refiere a la parte no consentida. El legislador no señala los efectos en los vicios del consentimiento, por lo que obliga ir a la fuente que dio origen tales disposiciones y que es el CCF.

El inciso III del ordinal 12, establece lo que hoy se conoce como un consentimiento informado y que se refiere a que el titular tenga conocimiento del aviso de privacidad, que se le entrega previo al tratamiento de sus datos personales. Desde mi punto de vista, este consentimiento informado adolece de un elemento esencial y que es que el titular de los derechos *comprenda* "las consecuencias de otorgar su consentimiento" como lo señala la citada fracción y no solo tenga conocimiento del aviso.

Es evidente la diferencia entre tener conocimiento del aviso de privacidad y entender las consecuencias del mismo, ya señalaba el Maestro De la Peza las diferencias sociales, económicas, culturales de las personas en una sociedad, si se trata de proteger como bien jurídico tutelado los datos personales de una persona, tendría que existir el entendimiento del consentimiento y no solo saber que me dieron a conocer el aviso de privacidad. En este sentido, me parece que el legislador sí debió establecer como "característica" del consentimiento la comprensión de las consecuencias jurídicas.

En su último párrafo, el Artículo 12 establece como regla general que el consentimiento tácito y nuevamente me parece que no se está logrando proteger a cabalidad los datos personales del titular de que se trate. La parte que de alguna forma, salva esa protección es que la única prueba que tendría el responsable del consentimiento es un documento en donde conste el mismo, pues desde un ámbito procesal, me parece un tanto complicado acreditar el consentimiento tácito, sin un documento, aunque si bien es cierto, existen otras pruebas que lo pudieran acreditar, lo más sencillo es la existencia de ese documento y que es lo que hasta ahorita ha prevalecido en la práctica el tratamiento de datos personales.

Por lo que se refiere a la formalidad del consentimiento, el Reglamento de la LFPDPPP establece en su numeral 15 que será expreso cuando: "I. Lo exija una ley o reglamento; II. Se trate de datos financieros o patrimoniales; III. Se trate de datos sensibles; IV. Lo solicite el responsable para acreditar el mismo; o V. Lo acuerden así el titular y el responsable".

En consecuencia, si un responsable está haciendo tratamiento de mis datos financieros o patrimoniales, sin mi consentimiento expreso, ¿se entendería que hay una ineficacia?, ¿podría en su caso, esta situación convalidarse en cualquier momento? Al respecto la Ley en cuestión es omisa, por lo que se hace relevante ir al CCF y a la doctrina.

La LFPDPPP y su Reglamento, sancionan pecuniariamente a los responsables en los tratamientos de datos personales cuando no se cumplan las formalidades o el consentimiento no cumpla con las "características" establecidas, pero existe una omisión total de las consecuencias del acto *per se*. En este sentido, me inquieta pensar que el titular de los datos personales que se hubiese visto afectado por el incumplimiento del responsable, deba recurrir a otra instancia para solicitar daños y perjuicios en su caso, y no sea el propio Instituto Nacional de Transparencia, Acceso la Información y Protección de Datos Personales la autoridad competente, quien tendría todos los elementos para evaluar si existió o no la vulneración a las disposiciones aquí indicadas, en virtud de los procedimientos que aquel realiza.

Por último, no menos importante es la excepción a recabar el consentimiento del titular de los datos personales y que se establece en el Artículo 10 de la LFPDPPP y se refiere a las siguientes:

I. Esté previsto en una Ley;

Por ejemplo, el Artículo 59 del CCF dice: "Cuando el nacido fuere presentado como hijo de matrimonio, se asentarán los nombres, domicilio y nacionalidad de los padres, los nombres y domicilios de los abuelos y los de las personas que hubieren hecho la presentación". En este caso, existe un claro tratamiento de datos personales sin consentimiento, es por mandato de ley, que dichos datos deben estar asentados.

II. Los datos figuren en fuentes de acceso público;

La misma LFPDPPP establece la definición de fuente de acceso público como aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación y en el Reglamento detalla en el Artículo 7o. que son considerados como fuentes:

I. Los medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté

concebido para facilitar información al público y esté abierto a la consulta general; como ejemplo, tenemos cualquier buscador, léase google, safari, etc.;

II. Los directorios telefónicos en términos de la normativa específica; que ahora ya se encuentran de forma virtual; verbigracia, la sección amarilla.

III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;

IV. Los medios de comunicación social; léase Facebook.

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

Esto se refiere a que como resultado de ese proceso, el titular de los datos no sea identificable y que generalmente se utiliza para fines estadísticos.

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

Es evidente de que se trata del cumplimiento o ejecución de un contrato.

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

Como podría ser el caso de desalojar a las personas en caso de una situación grave y que exista la necesidad de realizar el tratamiento de datos personales.

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

Este caso, pudiera ser cuando hay un accidente en la calle y deba prestarse el servicio.

VII. Se dicte por resolución de autoridad competente.

Si bien es cierto, la LFPDPPP y su reglamento tratan de formar detalladamente el consentimiento en la protección de datos, no menos cierto es que debe mejorarse la técnica jurídica, establecer como supletorio el CCF para que se establezca perfectamente y de forma jerárquica las consecuencias de los vicios del consentimiento, además de agregarse el dolo como un elemento más en la validez del consentimiento y por último, hacer mención expresa al tratamiento de datos personales de los menores, que si bien por regla general, recae ese consentimiento en sus padres o tutores, debiera estar previsto, ya que hay muchos datos personales de menores, que tienen un tratamiento, principalmente por escuelas privadas, hospitales, laboratorios y médicos particulares principalmente.

El hecho de que el titular de los derechos *comprenda* las implicaciones jurídicas del aviso de privacidad, debería ser piedra angular en el otorgamiento del consentimiento y en ese momento, si se estaría hablando de un consentimiento informado.

V. LA PROTECCIÓN DE DATOS EN EL ÁMBITO INTERNACIONAL

Ahora bien, no podría estar completo este trabajo, si no señalo de una forma breve pero concreta la Directiva 95/46 (Unión Europea, UE), que si bien es cierto está muy cerca de perder vigencia, aún la tiene, el Reglamento que la sustituye (UE) 2016/679 también será objeto de mención.

Por lo que se refiere a la Directiva 95/46 de la UE, en su Artículo 3o. dispone que, el consentimiento del interesado, es toda manifestación de voluntad libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

En el Reglamento que le sustituye, el 2016/679, añade dos elementos que a mi parecer, protegen aún más al titular de los datos personales, dispone que el consentimiento del interesado, es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una *declaración o una clara acción afirmativa*, el tratamiento de datos personales que le conciernen. Considero que estos elementos son para el titular, candados valiosísimos para que el responsable no pueda sin el consentimiento de aquel tratar sus datos.

El Artículo 7o. de la Directiva 95/46 establece los lineamientos en los que el consentimiento debió darse para poder tratar los datos personales, los que son: *a)* el interesado ha dado su consentimiento de forma inequívoca; *b)* es necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación de medidas precontractuales adoptadas a petición del interesado; *c)* es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable de tratamiento; *d)* es necesario para proteger el interés vital del interesado; *e)* es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos; *f)* es necesario para la satisfacción del interés le-

gítimo perseguido por el responsable del tratamiento, por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección.

Como es evidente, este numeral es la base para el establecimiento en la LFPDPPP.

Ahora bien, comparado con la parte relativa al Reglamento que está por entrar en vigor, el Artículo 7.1 dispone que cuando el consentimiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

Es relevante destacar, que la carga de la prueba la tiene el responsable del tratamiento de datos y que obliga de alguna forma al responsable, el consentimiento otorgado pueda ser probado en juicio, lo que nos lleva a la generalidad del consentimiento plasmado en un documento, lo cual es de alguna forma protector para el titular de los datos personales.

También prevé el caso de que el consentimiento se hubiese dado para varios asuntos, en el cual el responsable debe presentar la solicitud del consentimiento de forma que se distinga del resto de los asuntos, de forma inteligible y de fácil acceso, utilizando un lenguaje claro y sencillo, estableciendo como consecuencia, que la declaración no es vinculante, si el consentimiento se otorga violentando la citada Directiva.

Por último, hay una disposición que me pareció interesante, ya que delinea la forma de evaluar si el consentimiento se otorgó libremente, dispone también que se tomará en cuenta para dicha evaluación, si dicho consentimiento se supeditó para la prestación de un servicio o la ejecución de un contrato y que dichos datos no eran necesarios para los citados supuestos. En este sentido, está señalando las ventas atadas y es verdaderamente afortunada el que esta disposición prevea tal situación.

En este ordenamiento, el numeral 8 establece el consentimiento, tratándose de niños, "de servicios de la sociedad de la información" y contempla que será lícito cuando el niño haya dado su consentimiento y sea mayor de 16 años, o bien

si es menor a esa edad, lo otorgaron sus padres o tutores, y que los Estados parte podrán establecer otra edad, pero nunca menor de 13 años.

Al respecto, me parece atinada dicha prevención, pero considero que un niño de 13 años no tiene la madurez para entender las consecuencias jurídicas del acto jurídico que realiza al otorgar su consentimiento, en mi experiencia con niños de esas edades, inmersos en un mundo digital, con situaciones económicas favorables, no son lo suficientemente capaces de discernir los beneficios o no de otorgar su consentimiento, pues ellos lo que les interesa es *bajar* el juego o la aplicación sin ningún otro interés más.

Después de comparar los dos ordenamientos, existe un avance en el Reglamento que entrará en vigor en el 2018 y que valdría la pena que la LFRPPP y su reglamento, tomaran las partes en las que fueron omisas en pro del titular de los datos y de los menores.

VI. CONCLUSIÓN

La protección de datos es, una materia relativamente nueva y ha sido impulsada por la Comunidad Europea a través de sus distintas normativas al respecto.

Paradójicamente el consentimiento, en nuestra tradición jurídica existe desde el Derecho Romano y se ha ido transformando de acuerdo a las situaciones económicas y culturales de los países, hasta llegar al más novedoso consentimiento informado. En ese tenor, no es muy claro que es realmente esté informado, por lo menos en lo que se refiere a la legislación mexicana, ya que solo requiere que el titular de los datos tenga conocimiento del aviso de privacidad, pero no establece que el titular haya entendido las consecuencias jurídicas de haber otorgado su consentimiento el en tratamiento de datos.

No pasa desapercibido el tema de los menores, que fue olvidado por el legislador y, en su momento, es imperante que se establezca, ya que la niñez está con acceso a las TIC's y eso pone en riesgo sus datos personales. Si bien es cierto, debemos estar a lo establecido en el Código Civil Federal, cuya suplencia no se establece en la LFPDPPP, resulta necesaria para resolver este tema.

El consentimiento es la piedra angular en los contratos y el aviso de privacidad, desde mi perspectiva pudiera llegar a ser aun *contrato* entre particulares, cuya

formalidad está prevista en la ley respectiva, que si bien es cierto no se le da ese tratamiento en la LFPDPPP ni en su Reglamento, tiene todos los elementos de un contrato y añadiría de "adhesión" ya que generalmente los avisos de privacidad son entregados al titular de los datos para que puedan ser tratados sus datos para el objeto planteado. No es tema de este artículo ahondar en la naturaleza jurídica del aviso de privacidad.

La cuestión respecto a si el consentimiento realmente está siendo informado y consecuentemente, si el aviso de privacidad es un instrumento real para proteger los datos personales, tendrá que medirse y evaluar su eficacia con el paso del tiempo.

Por último, me parece que el tema del consentimiento en la legislación federal de protección de datos en posesión de terceros, está basada en el Código Civil Federal y en la Directiva 94/46, pero que aún puede y debe ser mejorada con los resultados de la aplicación de la Ley e incluir las omisiones ya indicadas.

VII. FUENTES DE INFORMACIÓN

1. *Bibliografía*

BACIGALUPO ZAPATER, Enrique, *Principios de Derecho Penal. Parte general, 2ª.* ed., Madrid, Akal, Madrid, 1990.

DE LA PEZA, José Luis, *De las obligaciones*, México, McGraw-Hill, 1997.

Diccionario de la lengua española, Real Academia Española, *https://definiciona.com/consentimiento/.*

FERNÁNDEZ, Ramón Francisca, "Conceptualización de la ineficacia, invalidez e inexistencia en el Derecho español", *Revista chilena de Derecho Privado*, Santiago de Chile, número 19, diciembre de 2012, *http://dx.doi.org/10.4067/S0718-80722012000200003.*

ROJINA VILLEGAS, Rafael, *Compendio de Derecho Civil,* 26ª. ed., México, Porrúa, 1995, t. I.

SÁNCHEZ MEDAL, Ramón, *De los contratos civiles,* México, Porrúa, 1993.

2. *Legislación*

Código Civil Federal.

Directiva 95/46 de la Unión Europea.

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

Reglamento 2016/679 de la Unión Europea.

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

CAPÍTULO TERCERO
El principio de información en materia de protección de datos personales en México

María RIVERO DEL PASO[31]

SUMARIO

I. INTRODUCCIÓN

El derecho a la protección de datos, garantiza que la información personal que de cada individuo sea conocida, ya sea con la autorización de ésta o de manera circunstancial, destinada únicamente para los fines que se deban y en todo momento sea tratada conforme fue autorizado o conforme a lo que es permitido por las leyes respectivas y por la misma persona; protegiendo así la vida privada[32].

Este derecho está integrado por distintos principios, dentro de los que se encuentra el de información, mismo que en este artículo se analiza.

[31] Es Licenciada en Derecho así como Maestra en Derecho de la Empresa por la Universidad Panamericana con honores. Sus áreas de experiencia son enfocadas en el Derecho Corporativo, contratos, logística y transporte, Tecnologías de la Información, cumplimiento normativo, anticorrupción, privacidad y protección de datos personales. Autora de diversas publicaciones en materia de protección de datos. Socia del despacho Sesma & McNeese abogados.

[32] Villanueva, Ernesto, *Derecho de acceso a la comunicación pública en Latinoamérica*, México, UNAM, 2003, p. XXV.

Para la salvaguarda y ejecución del principio de información, en materia de protección de datos personales, es requisito que para el tratamiento de dichos datos y previamente a que el titular de los datos otorgue su consentimiento en caso de ser requerido, le sean comunicados por parte del responsable del tratamiento los elementos suficientes y necesarios para que con pleno conocimiento sobre la forma en que se llevará a cabo su tratamiento, pueda otorgar o negar su autorización para el uso de los mismos. Es aquí donde cobra relevancia el principio de información para la protección de datos personales.

A continuación, se analiza el concepto, aplicación, obligaciones y relación con otros principios, del principio de información en materia de protección de datos personales en México.

II. CONCEPTO DE PRINCIPIO DE INFORMACIÓN

El principio de información, es el derecho del titular de la información, a ser informado de sus datos personales, con la finalidad de que conozca los sujetos, la forma y métodos, el propósito y demás particularidades que pudieran existir sobre la recolección, uso, salvaguarda y transferencia de dicha información[33].

La salvaguarda y protección de este principio, faculta al titular de los datos personales a conocer precisamente el tratamiento que se le dará a su información, así como los medios que le permitan ejercer los derechos y acciones disponibles para garantizar su autodeterminación informativa.

Este principio es aplicable para aquellos casos en que los datos personales sean recabados o conocidos al ser obtenidos directamente de su titular, terceros, así como a través de fuentes o registros públicos. En este último caso, debe comunicarse e informarse al titular de los datos por medio del responsable del archivo, la fuente de la que los datos han sido obtenidos, la finalidad de su recolección y los derechos disponibles de los titulares en relación con sus datos[34].

Con lo anterior, se garantiza el derecho del titular de la información de tener el control sobre sus datos personales, independientemente si estos están o no

[33] Rivero del Paso, María, *Principios rectores para la protección de los datos personales,* México, Universidad Panamericana, 2008, p. 78.

[34] *Informe sobre protección de datos a nivel internacional*, noviembre 2004 pp. 47 y 48, *www.ifai.org.mx.*

contenidos en archivos de acceso público, es decir, el principio de información, es aquél por el que se garantiza que el titular de los datos personales conozca con precisión, claridad y de forma oportuna qué datos se tratarán, para qué serán tratados, por quién, por cuánto tiempo, si serán transferidos, cómo podrá oponerse a su tratamiento o revocar, en su caso, el consentimiento que sobre su tratamiento pudiera haber otorgado con anterioridad y cualquier otra particularidad relativa a su tratamiento.

El debido cumplimiento de este principio es crítico y primordial para una completa y debida protección de los datos personales.

III. MATERIALIZACIÓN Y APLICACIÓN PRÁCTICA DEL PRINCIPIO DE INFORMACIÓN

1. *Principio de información y las obligaciones para entes privados*

En atención a la protección de la autodeterminación informativa, derecho mediante el cual, los titulares deben tener la facultad de conocer el estado de su información personal, por medio del principio de información, a partir de la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en 2011, se ha impuesto a los particulares responsables, del tratamiento de datos personales, la obligación de emitir un comunicado mediante el cual se informe a los titulares, la información esencial sobre el tratamiento de sus datos personales. Dicho comunicado es denominado aviso de privacidad. Este es el 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[35].

El aviso de privacidad tiene como finalidad que los responsables del tratamiento de datos personales, comuniquen a los titulares de los datos, su identidad, domicilio, datos que se recabarán, finalidades, medios y procedimientos para ejercer sus derechos de acceso, rectificación, cancelación y oposición. De esta forma, los titulares conocen y están informados sobre el tratamiento que se le dará a sus datos personales.

[35] Artículo 2o., párrafo primero, Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

El contenido, tipos y requisitos para la comunicación del aviso de privacidad se encuentran regulados por la Ley antes mencionada, su Reglamento y los Lineamientos del aviso de privacidad.

De acuerdo con los Lineamientos del aviso de privacidad, este deberá contener los siguientes elementos:

I. Identidad del responsable. Debe incluirse el nombre o en su caso la denominación social completa, ya que dentro de los casos de sanciones impuestas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, otrora Instituto Federal de Acceso a la Información y Protección de Datos Personales, en ejercicio de sus facultades de revisión, se encuentra la imposición de multas por el uso del nombre comercial de un responsable, omitiendo en su lugar la denominación social[36].

II. Domicilio del responsable. La dirección puede ser en cualquier plaza de la República Mexicana y no requiere tener relación con algún domicilio en específico, es decir, no es necesario que coincida con el domicilio fiscal, ubicación de oficinas y tampoco es requerido que se encuentre en la misma entidad donde se recaban los datos. No obstante, atendiendo al propósito del principio de autodeterminación informativa, es conveniente que el domicilio del responsable sea accesible para los titulares y permitir a éstos mantener el control sobre su información, evitando obstáculos para las comunicaciones entre el titular y el responsable en relación con el tratamiento de los datos personales.

III. Datos que se recaban, identificando aquéllos que sean sensibles. Deberá incluirse un listado sobre la información que se tratará. Dicho listado deberá ser limitativo, es decir, deberá incluir la totalidad de la información que se recabará.

IV. Finalidades del tratamiento de los datos personales. Una descripción de los propósitos con los que se tratarán los datos personales recabados. Dicha descripción debe ser clara, limitativa y acorde a la relación entre el respon-

[36] Resolución de fecha 3 de diciembre de 2012, por más de dos millones de pesos a la empresa Pharma Plus, S.A. de C.V., Operadora de Farmacias San Pablo.

sable y el titular. En todo caso, deberá distinguirse en el aviso de privacidad aquellas finalidades que son necesarias a raíz de la relación entre el titular y el responsable y aquellas que sean distintas. En caso que las finalidades varíen, deberá informarse a los titulares previamente y, cuando así se requiera, será necesario obtener su consentimiento para las nuevas finalidades.

V. Consentimiento del titular para aquellos casos que así se requiera. En relación con este requisito debe considerarse que para el tratamiento de datos sensibles o patrimoniales, el consentimiento debe otorgarse de forma expresa, mientras que para las finalidades que requieren consentimiento, siempre y cuando no se trate de datos sensibles o patrimoniales, el consentimiento puede otorgarse de forma tácita. Asimismo, debe tomarse en cuenta que corresponde al responsable la carga de la prueba sobre la obtención del consentimiento para aquellos datos o fines que lo requieran.

VI. Medios para que el titular pueda solicitar la limitación del uso o divulgación de sus datos. Señalar un medio que sea viable y acorde al perfil de los titulares. Sobre este elemento vale la pena destacar que los medios deben ser aquellos que efectivamente permitan una comunicación entre el responsable y el titular.

VII. Las transferencias de datos personales que en su caso se efectúen; el tercero receptor de los datos personales y las finalidades de las mismas, incluyendo la opción para que el titular exprese su consentimiento o rechazo a la transferencia, cuando así se requiera.

VIII. Los medios y el procedimiento para ejercer los derechos de Acceso, Rectificación, Cancelación y Oposición.

IX. Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento para el tratamiento de sus datos personales.

X. Las opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de sus datos personales.

XI. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología que permitan recabar

datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso.

XII. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

El Reglamento profundiza en la regulación sobre el aviso de privacidad, identificando distintos tipos de los mismos, tomando en consideración la forma en la que se recaban los datos, la finalidad y la naturaleza de los mismos. De este modo, el aviso de privacidad puede ser integral (completo) o simplificado (corto).

En caso de que la información se recabe de manera personal, el aviso de privacidad deberá proporcionarse al momento en que se recaben los datos (de forma clara y fehaciente), a menos que el aviso se hubiere proporcionado con anterioridad.

En el supuesto de que los datos sean obtenidos de otra manera (medios ópticos, electrónicos, etc.), en el momento deberán darse a conocer los datos esenciales del aviso de privacidad, es decir, el aviso simplificado, refiriendo al titular el texto completo del mismo.

Asimismo, en caso que se recabe una menor cantidad de datos y que los mismos no sean sensibles, y que por lo tanto no se requiera el consentimiento del titular, puede emitirse el aviso de privacidad corto, con la identificación y domicilio del responsable, finalidades y remisión al aviso de privacidad integral.

El aviso de privacidad siempre deberá emitirse en idioma español, aunque discrecionalmente los responsables podrán elegir acompañar traducciones a distintos idiomas, considerando el origen de los titulares cuya información sea recabada.

Si bien, el aviso de privacidad requiere integrarse por varios elementos, es menester no perder de vista que el propósito de este es informar al titular sobre el tratamiento de su información, para así procurar que su contenido, formato y estructura sean claros, precisos y adecuados para los titulares cuya información se recabe.

2. *Principio de información y las obligaciones para entes públicos*

Promulgada el 26 de enero de 2017, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, regula la salvaguarda de esta información al momento de su tratamiento en el ámbito federal, estatal y municipal, por cualquier

autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Por primera vez, este ordenamiento exige a los sujetos obligados la emisión de un aviso de privacidad, entendiendo como tal el documento a disposición del titular de forma física, electrónica o por 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[37].

Es a través de este ordenamiento, donde se establece el uso de la información personal, que está sujeta al uso limitado de los fines señalados en el aviso de privacidad o aquellos señalados en las atribuciones conferidas en la ley y mediando el consentimiento del titular, salvo cuando se trate de personas reportadas como desaparecidas[38].

El aviso de privacidad debe redactarse y estructurarse de forma clara y sencilla para cumplir de forma eficiente con su función de informar. Asimismo, éste deberá darse a conocer al titular de forma directa, en el entendido que cuando dicha difusión exija esfuerzos desproporcionados, el responsable podrá hacer uso de medidas compensatorias de comunicación masiva, atendiendo en todo caso a los criterios emitidos por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales[39].

Para los sujetos obligados, existen las modalidades de aviso de privacidad simplificado e integral. El aviso de privacidad simplificado debe contener la siguiente información:

I. Denominación del responsable;

II. Finalidades del tratamiento para las cuales se obtienen los datos personales, haciendo una identificación sobre aquéllas que requieran el consentimiento del titular;

---

[37] Artículo 3o., párrafo segundo, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

[38] Artículo 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

[39] Artículo 26 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

III. En los casos en que se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:

a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y

b) Las finalidades de dichas transferencias;

IV. Mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular; y

V. El sitio donde se podrá consultar el aviso de privacidad integral.

La puesta a disposición de este aviso de privacidad no exime al responsable de su obligación, de proveer los mecanismos para que el titular pueda conocer el contenido del aviso de privacidad integral.

El titular debe tener acceso a los mecanismos y medios para manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a que ocurra dicho tratamiento[40].

En cuanto al contenido del aviso de privacidad integral, deben sumarse a los elementos requeridos para el simplificado los siguientes:

I. El domicilio del responsable;

II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;

III. El fundamento legal que faculte al responsable para llevar a cabo el tratamiento;

IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;

[40] Artículo 27 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;
VI. El domicilio de la Unidad de Transparencia; y
VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad[41].

Con esta obligación se protege de forma excepcional y novedosa en el Derecho Positivo mexicano, el principio de información.

IV. RELACIÓN DEL PRINCIPIO DE INFORMACIÓN CON OTROS PRINCIPIOS RECTORES DE LA PROTECCIÓN DE DATOS PERSONALES

De una manera coordinada, la salvaguarda de cada uno de los principios rectores de la protección de datos personales crea un marco a través del cual los datos personales sean protegidos, garantizando la autodeterminación informativa de sus titulares.

En este sentido, el principio de información se encuentra estrechamente vinculado a los principios de autodeterminación informativa, consentimiento y proporcionalidad. De modo que en la medida en que se informe debidamente al titular sobre el tratamiento de sus datos y medios para su protección, este podrá mantener el control que le corresponde sobre su propia información. Asimismo, deberá garantizarse que los datos y fines que se reporten al titular por parte del responsable tengan una relación lógica y proporcional con el propósito último de su tratamiento, de modo que los datos y fines se mantengan alineados y dentro de los parámetros de lo requerido para la relación que exista entre el titular y el responsable.

Cada uno de los principios requiere del cumplimiento de los demás, es por ello que, para cumplir debidamente con el requisito de obtener el consentimiento del titular de la información, para su recolección y manejo es indispensable que dicho titular esté claramente informado y conozca el propósito de la recolección.

[41] Artículo 28 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Esta vinculación de principios se encuentra reconocida en la legislación vigente, estableciendo como requisito previo a la obtención del consentimiento, la obligación a cargo del responsable de poner a disposición del titular el aviso de privacidad, siendo éste el instrumento mediante el cual se comunica al titular de los datos la información relevante sobre su tratamiento.

V. CONCLUSIÓN

El principio de información en materia de protección de datos personales, se traduce en el derecho del titular de los datos y la correlativa obligación del responsable del tratamiento de los mismos, para comunicar debida y oportunamente al titular de los datos personales sobre la información que de éste será tratada, los fines para los que se utilizará la misma y demás condiciones relativas al proceso de su tratamiento y protección. Este principio debe garantizarse independientemente de que la información personal hubiera sido obtenida directamente del titular, de fuentes de acceso público o de algún tercero.

Asimismo, el principio de información debe ejercerse de forma coordinada y relacionada con otros principios rectores en materia de protección de datos personales, pues no basta la comunicación al titular sobre los fines o datos que se traten, si éstos no son proporcionales con los fines y relación que se entable entre el titular y responsable de tratar los datos personales.

VI. FUENTES DE INFORMACIÓN

1. *Bibliografía*

RIVERO DEL PASO, María, *Principios rectores para la protección de los datos personales*, México, Universidad Panamericana, 2008.

VILLANUEVA, Ernesto, *Derecho de acceso a la comunicación pública en Latinoamérica*, México, UNAM, 2003.

2. *Legislación*

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

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos para el Aviso de Privacidad.

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

3. *Otros*

Informe sobre protección de datos a nivel internacional, noviembre 2004, *www.ifai.org.mx.*

CAPÍTULO CUARTO
Las medidas de seguridad en materia de protección de datos personales

Cynthia SOLÍS[42]

"Corría el invierno de 2006 en la Universidad de París,
cuando Monsieur Matthiew entraba al anfiteatro con una contundente pregunta
–¿Qué es la seguridad?–, *varios minutos y participaciones después,*
con mirada profunda e impostando la voz, nos dijo:
"señores, la seguridad es un estado del espíritu".

Ese día comprendí, por primera vez, aquello a lo que solemos llamar seguridad, no es otra cosa que, una forma de sentir y que su mayor aproximación es la minimización del riesgo, este último estado natural de la vida; el Diccionario de la Real Academia Española, define la seguridad como una cualidad, la cualidad de seguro, y a su vez, conceptualiza a lo seguro como algo libre y exento de riesgo, algo que brinda certeza y confianza; es así, que la seguridad depende directamente del riesgo, no existen el uno sin el otro y suelen ser inversamente proporcionales, es decir, a menor riesgo mayor seguridad y viceversa.

[42] Es egresada de la Facultad de Derecho de la Universidad Nacional Autónoma de México, de las Universidades París I Panthéon Sorbonne y París Sud XI; así como de la Universidad Panamericana y cuenta con estudios de Maestría en Traducción del Colegio de México (COLMEX). Doctora en Derecho Privado y Ciencias Sociales por la Universidad de París Saclay. Catedrática de distintas universidades e instituciones educativas nacionales como internacionales, entre las que se destacan el Centro de Estudios Navales de la Secretaría de Marina (CESNAV), el Instituto Politécnico Nacional (IPN) y el Instituto Nacional de Ciencias Penales (INACIPE). Experta certificada en materia de Protección de Datos Personales por Normalización y Certificación Electrónica (NYCE).

Me permito hacer esta anecdótica introducción, porque no hay manera de concebir una medida de seguridad sin una correcta dimensión del riesgo. Por tanto, es un concepto a geometría variable.

Ya entrando en la materia de protección de datos personales, y dentro del contexto de esta obra en la que tengo el honor de compartir y expresar mis reflexiones con tan destacadas figuras expertas en el tema; retomando los conceptos y principios, exquisitamente explicados en los capítulos precedentes, no ahondaré demasiado en ellos.

El tema de la seguridad de la información cobra relevancia, cuando dimensionamos la importancia de salvaguardar la confidencialidad[43] de la misma; en el ámbito de la protección de datos personales, la confidencialidad y la seguridad son dos conceptos íntimamente relacionados cuyo fin es garantizar que no se haga un uso indebido de la información con carácter de dato personal. Sin embargo, aún dentro de la categoría de datos personales, alguna de esta información, requerirá de medidas de seguridad más altas que el resto.

Por ejemplo, ya que un dato personal[44] es toda aquella información concerniente a una persona física identificada o identificable, podemos inferir que dentro del vasto universo que plantea el concepto contenido en nuestra Ley mexicana (Ley Federal de Protección de Datos Personales en Posesión de los Particulares), existe una gran cantidad de información que podría clasificarse como tal, pero no toda ella merece el mismo nivel de confidencialidad, por lo que el dato que corresponde a mi nombre completo no tendría el mismo peso específico que mi historial crediticio o más aún mi historial médico.

---

[43] El término confidencialidad, proviene de confidencia y a su vez de la palabra confianza, es además uno de los dos deberes contemplados en el Artículo 9o. del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; en relación con los Artículos 19 y 21 de la Ley.

[44] Artículo 3o. fracción IX, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

En este nuevo paradigma de la sociedad de la información[45] y la dependencia de las herramientas informáticas[46], es casi un sinónimo de muerte civil no aparecer en los buscadores. ¡Quién eres si no apareces en Google! Si el Internet no "constata" o "relata" tu historia; puede ser muy atractivo para mí ser una persona cuyos resultados de búsqueda se extiendan a diversas páginas, o puede no serlo, eso dependerá de mi nivel de exposición, y de nuevo, el riesgo que esta conlleve, sin embargo, cualquiera que sea el caso, no debe ser un asunto ligero el que se exhiba el historial médico de un individuo y mucho menos sin su consentimiento, la mayoría de las personas podrían sentirse incómodas ante tal situación.

Cada vez se vuelve más difícil guardar el equilibrio entre lo público y lo privado, entre la exposición y la discreción, sobre todo cuando la seducción de la aparente fama nos impide visualizar potenciales riesgos, eso lo saben muy bien los cientos de personas que han sido "linchadas virtualmente" gracias a un irresponsable uso de las tecnologías de la información y la comunicación.

Las medidas de seguridad que, por Ley[47], deben acatar los responsables que traten datos personales, no pueden de ninguna manera definirse sin antes conocer a detalle el nivel de riesgo, y por ello se entiende un análisis holístico de este concepto.

Delimitar el nivel de riesgo conlleva la puesta en marcha de toda una metodología de análisis[48], que comienza con la identificación de los datos personales

---

45 Sociedad de la información, es un término que fue introducido desde 1973 por el sociólogo Daniel Bell, quien formula *que el eje principal de esta será el conocimiento teórico y advierte que los servicios basados en el conocimiento habrían de convertirse en la estructura central de la nueva economía y de una sociedad apuntalada en la información, donde las ideologías resultarían sobrando.* Bell, Daniel, *The coming of Post-Industrial Society. A venture in social forecasting*, Harmondsworth, Peregrine, 1976; citado por Torres, Rosa María, *Sociedad de la información/Sociedad del conocimiento*, Universidad de Barcelona, 21 de abril de 2005, *http://www.ub.edu/prometheus21/articulos/obsciberprome/socinfsoccon.pdf.*

46 La informática se considera una gran amenaza para la privacidad porque permite una vigilancia omnipresente, bases de datos gigantescas y una veloz distribución de la información en el globo entero. Nissenbaum, Helen, *Privacidad amenazada,* trad. de Enrique Mercado, México, Océano, 2011, p. 21.

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

48 *Gestión de riesgos, análisis y cuantificación, http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf.*

que se tratan, el propio alcance del tratamiento, pasando por los medios de almacenamiento y llegando hasta la capa más vulnerable que es la humana, es decir, todas aquellas personas que por motivo de su empleo o de su encargo, tendrán acceso a esa información.

Después de llevar a cabo un levantamiento de toda la información que se encuentra en posesión de un responsable y de todas aquellas partes relacionadas directa o indirectamente con este, como es el caso de los empleados, recursos humanos externos, practicantes, servidores sociales, encargados[49] y terceros; debe procederse a una clasificación de la misma, es decir, del hiperónimo conocido como información habrá que categorizarse toda aquella de identifique o vuelva identificable a una persona física; posteriormente, atendiendo al nivel de riesgo de daño o discriminación que conlleva el tratamiento de esos datos, se determinará si estamos en presencia de datos considerados por la Ley como sensibles o no.

El resultado de todo este examen es el famoso inventario de datos, más que un requerimiento legal, es un activo básico para el establecimiento de los procesos de seguridad de la información, que detallaremos más adelante.

El deber de seguridad, se encuentra establecido y relacionado con otros principios, en diferentes Artículos de la Ley y su Reglamento[50], por ejemplo:

> Artículo 19[51]. *Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas* que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
>
> *Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información*. Asimismo, se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

---

[49] Se entiende por encargado a la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable, esta figura debe ser ajena a la organización del responsable, en términos del Artículo 3o. fracción IX, de la LFPDPPP y del Artículo 49 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP).

[50] RLFPDPPP.

[51] LFPDPPP.

El cumplimiento cabal y estricto de este deber de seguridad es tan importante y trascendental, que, todo aquel responsable, encargado o tercero, que provoque una vulneración de seguridad, será acreedor a una sanción, la cual puede llegar incluso a ser de carácter penal.

Es el RLFPDPPP, el que define de manera precisa, lo que se entiende por medidas de seguridad, su alcance, funciones, factores a tomar en cuenta para su determinación, acciones a seguir, actualizaciones, vulneraciones, comunicación de las vulneraciones y medidas correctivas en su capítulo III.

> Artículo 57. *El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales*, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá́ por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales.
> *Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.*

Del Artículo transcrito, se desprende que la obligación de establecer y mantener todo tipo de medidas de seguridad, no solo se limita a la figura del responsable sino a la del encargado, y aunque no lo menciona este precepto, hay que recordar que, en la mayoría de los casos, el tercero se convierte posteriormente en responsable y además de ello, el responsable al llevar a cabo la transferencia debe verificar, al menos por contrato, que el tercero también se encuentra en cumplimiento de la legislación en materia de protección de datos personales.

Lo anteriormente expuesto, conlleva una especie de cadena segura de manejo de información, que idealmente debe estar estandarizada en todas aquellas fases del ciclo de vida del dato, es decir, que de nada serviría que el responsable de los datos personales se encontrara en estricto cumplimiento si el encargado de los datos personales no está en la misma circunstancia, y por lo tanto, es éste último el eslabón vulnerable por donde puede haber fuga de información o acceso no autorizado a bases de datos personales, incluso sensibles.

Pensar en seguridad es pensar en minimización de riesgos, para conocer el riesgo es importante entender no solo la naturaleza del dato sino la naturaleza de los medios de almacenamiento de la información y sus vulnerabilidades propias.

Cada soporte o medio de almacenamiento de la información es susceptible de sufrir tal o cual desastre natural o ser más apto para sufrir un ataque interno o externo; el papel es sensible al agua, a la humedad, al fuego, no es trazable, es fácil de traspapelar, es delicado para conservar; en el caso de los medios informáticos, son sensibles a otro tipo de circunstancias o ataques, si bien son trazables y su manipulación es fácil de identificar, es cierto que pueden ser objeto de ataques informáticos gestados incluso desde el interior de la empresa o ataques externos, a veces de países lejanos, son susceptibles al borrado accidental, a la copia no autorizada, a la extracción de información ilícita, al cifrado[52] que los pueda volver inaccesibles, en ocasiones pueden ser editables sin conocimiento del titular de la información, etc.

Hablando de medios magnéticos u otro tipo de cintas donde vivan datos relacionados con cámaras de video vigilancia, llamadas telefónicas, registros de voz, imágenes, datos, etc. de igual manera son vulnerables a otras condiciones meteorológicas, físicas, etc.

Hablar de medidas de seguridad es hablar de un sistema de seguridad, es decir, no de medidas y procesos aislados que no servirían de nada cuando de disminuir riesgos se trata, la seguridad de la información por naturaleza está basada en procesos, actividades y medios físicos que prevengan la modificación, alteración, destrucción, acceso o copia no autorizados, en pro de garantizar la famosa triada de la información: integridad, confidencialidad y disponibilidad[53], sea cual sea el formato en el que se haya la información y el soporte donde radica.

Para determinar correctamente las medidas de seguridad, el Reglamento de la Ley, en su Artículo 60, menciona los factores que debe tomar en cuenta para ello, los cuales se citan a continuación:

---

[52] Consultar: *https://www.certsuperior.com/Blog/que-es-el-cifrado-y-para-que-funciona-medida-de-seguridad-primordial-para-tu-empresa.*

[53] Muñoz, Néstor, *Qué es la triada CIA o CID*, *https://es.linkedin.com/pulse/qué-es-la-triada-cia-o-cid-néstor-muñoz.*

> Artículo 60. El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:
> I. El riesgo inherente por tipo de dato personal;
> II. La sensibilidad de los datos personales tratados;
> III. El desarrollo tecnológico, y
> IV. Las posibles consecuencias de una vulneración para los titulares.
> De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:
> I. El número de titulares;
> II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;
> III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
> IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

Estimar el nivel de riesgo de seguridad de cierta información catalogada como dato personal, se vuelve casi un cálculo matemático que además tome en cuenta los avances tecnológicos tanto para el tratamiento de la información como aquellas nuevas amenazas que se hayan desarrollado con motivo de estos.

La delincuencia organizada ha migrado hacia el robo de información de manera creciente, por lo tanto, los mecanismos de acción se han vuelto cada vez más sofisticados, cada año existen nuevas tendencias en materia de ciberdelitos, los virus y troyanos que conocíamos a principios del año 2000, no se parecen en nada a los nuevos gusanos que se esparcen de manera casi instantánea utilizando técnicas de ingeniería social para gestar un ataque de *ransomware*[54] y parar las actividades de servicios críticos como hospitales, transporte público, entre otros.

Además de conocer la calidad de la información que fluye por nuestra organización, el número de usuarios de quienes manejamos esa información, los medios en los que esta reside, su potencial valor; ahora es indispensable conocer las nuevas tendencias de seguridad[55] en función de los avances tecnológicos dispo-

[54] *http://cnnespanol.cnn.com/2017/05/15/que-es-un-virus-ransomware-y-como-actua/*.

[55] Sullivan, Brian *et al*., *Tendencias de seguridad cibernética en América Latina y el Caribe*, Washington DC, Symantec-Organización de los Estados Americanos, 2014.

nibles, las nuevas tendencias criminales y el grado de vulnerabilidad de nuestra empresa u organización ante estos nuevos ataques.

Desde la entrada en vigor de la Ley en 2010, la mayoría de los responsables y sus empleados se preguntaban acerca de una guía o recomendaciones que les ayudaran a cumplir cabalmente con sus obligaciones, es importante recordar que esta Ley le aplica tanto a personas físicas como a personas morales de carácter privado independientemente de su tamaño y estatus económico. Es de hace constar que aun y cuando el Capítulo III del Reglamento de diciembre de 2011, de las medidas de seguridad, en términos del Artículo Cuarto Transitorio no entró en vigor hasta 18 meses después, las empresas debían empezar a aceitar motores en el tema a efecto de no ser sancionadas.

Cualquiera podría pensar que las grandes corporaciones, incluso desde antes de la entrada en vigor de la Ley, se encontraban en perfecta aptitud para enfrentar toda clase de vulneraciones en la seguridad de la información, sin embargo, a la fecha vemos que no es así, pues no se trata de una fuerte inversión de dinero en consultores o herramientas tecnológicas de vanguardia, sino en saber lo que guardamos y en función de ello aplicar las medidas idóneas, no es un aspecto cuantitativo sino cualitativo, asimismo, por desgracia, vemos que siete años después hay una gran cantidad de profesionales independientes que desconocen esta Ley o no se encuentran correctamente implicados o asesorados para su correcto cumplimiento.

Es por ello que la publicación de su reglamento vino a esclarecer un poco el tema, así como las recomendaciones emitidas por el INAI[56].

Las medidas de seguridad, en términos del Reglamento de la Ley, se clasifican de la siguiente manera:

[56] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

	Referencia	Definición	Ejemplos
Medidas de seguridad administrativas	Artículo 2o., fracción V del RLFPDPPP	**Medidas de seguridad administrativas**: 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.	En este rubro podemos encontrar todos aquellos procesos, procedimientos, políticas, normas internas, buenas prácticas documentadas, reglamentos internos, contratos y cláusulas de confidencialidad, contratos con encargados y de transferencia a terceros, capacitación, certificación, normas y estándares internacionales en materia de seguridad de la información como es el caso de la familia ISO 27000, la adhesión y certificación con base en los parámetros de autorregulación y todas aquellas acciones de carácter administrativo que permitan minimizar riesgos para la seguridad de la información.
Medidas de seguridad físicas	Artículo 2o., fracción VI del RLFPDPPP	**Medidas de seguridad físicas**: 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.	Dentro del marco de las medidas de seguridad física podemos encontrar un amplio catálogo de alternativas. Estas opciones pueden en sí mismas tener embebida alguna medida tecnológica o no. Podemos ir desde las medidas más rudimentarias y por todos conocidos como los cerrojos, candados, gavetas con seguridad, cajas fuertes, bloqueadores físicos de puertos USB, puertas de seguridad, cajas de seguridad en bancos, bóvedas subterráneas, hasta incluso la presencia de personal de seguridad controlando los accesos, hasta medidas mucho más sofisticadas como pueden ser las cámaras de video vigilancia, sensores de movimiento, cerraduras con reconocimiento biométrico, cerraduras inteligentes electrónicas, etc.

Medidas de seguridad técnicas	Artículo 2o., fracción VII del RLFPDPPP	**Medidas de seguridad técnicas:** 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.	Por último, tenemos a las medidas de seguridad que implican la aplicación de algún tipo de tecnología. Este tipo de mecanismos de seguridad, comúnmente sobrevalorados, tienen como finalidad el monitoreo, idealmente en tiempo real del flujo de la información así como el acceso que tienen a ella los usuarios con motivo de sus funciones para poder identificar a tiempo comportamientos atípicos que revelen una posible intrusión o alteración por parte de personas ajenas a la operación habitual y autorizada; dentro de las opciones más conocidas y económicas encontramos a los antivirus, anti programas espía, muros de fuego, bloqueo de cookies, y podemos ir subiendo el estándar de precio y sofisticación para llegar a soluciones de seguridad más robustas como los famosos DLP, o *Data Loss Prevention, o Data Leak Prevention*[57] (sistemas de prevención de pérdida de información), *sandbox*[58], hasta soluciones específicamente creadas para prevenir ataques de tipo *ransomware.* Sin olvidar nunca que el usuario suele ser la parte más débil del eslabón y para ello habrá que monitorear y controlar su actividad en los sistemas de la empresa, evitando que navegue por sitios inseguros, descargue aplicaciones y archivos no permitidos o actualizaciones apócrifas de programas de cómputo.

[57] Consultar:*https://www.isaca.org/KnowledgeCenterResearchDeliverables/Pages/Data-Leak-Prevention.aspx.*

[58] Consultar: *http://blog.smartekh.com/sandbox-porque-paraque.*

Como podemos observar, las opciones de los tres tipos de medidas exigidos por la Ley y su Reglamento, son diversas y mientras podamos demostrar que éstas son eficaces y obedecen a las circunstancias de nuestra organización, podremos dormir más tranquilos.

Así como existen diferentes tipos de medidas de seguridad, existen diferentes tipos de amenazas, las cuales en general se dividen en internas y externas, por desgracia en innumerables ocasiones ya sea por imprudencia o dolo, los empleados, colaboradores o miembros de la organización están implicados en las vulneraciones de seguridad de la empresa, y en otros más, se trata de ataques gestados desde fuera con amplio conocimiento del ADN de la compañía, como aquellos en los que un exempleado rencoroso que conoce mejor que nadie los puntos débiles de la empresa, una vez fuera de ella organiza un ataque informático valiéndose del amplio conocimiento que tiene de las deficiencias de seguridad o abusando de la información a la que tuvo acceso.

Sorpresivamente los ataques externos no dirigidos son los menos frecuentes, es decir, la mayoría de los delincuentes, sobre todo los delincuentes informáticos, previo al incidente de seguridad, lo han planeado con meses y hasta años de anticipación estudiando a detalle cada movimiento, cada punto débil, cada brecha de seguridad para elevar la tasa de éxito de su encomienda y para dejar el menor número de huellas de su fechoría.

Lo que es un hecho innegable es el enorme compromiso que recae en el responsable que decide sobre el tratamiento de los datos personales de los titulares, respecto del correcto manejo de la información que se le ha confiado, pero en gran medida depende de las buenas prácticas que deben ser parte del día a día de cada empresa y profesionista en el mundo, al respecto el Dr. Rubén Vázquez en el libro intitulado "Seguridad y defensa en el ciberespacio"[59], en su capítulo respecto de las buenas prácticas comenta lo siguiente: "… es necesario que cada persona haga

[59] Vázquez, Rubén, "Buenas prácticas para reducir los impactos de amenazas y riesgos de la información en el ciberespacio", *Seguridad y defensa en el ciberespacio,* México, Centro de Estudios Superiores Navales, 2015, p. 248.

conciencia sobre su seguridad y la de su información, así como los riesgos y amenazas que pudiera enfrentar, de manera que pueda saber cómo reducir, evitar o transferir los riesgos existentes". Es así pues que las buenas prácticas, deben ser la pieza angular de nuestro pensamiento y comportamiento en el día a día para evitar exponernos a riesgos innecesarios o saber lidiar con ellos al momento de que por alguno de ellos nos veamos implicados en un incidente de seguridad.

Estimado lector, tal y como lo aprendimos hace más de diez años, la seguridad es un estado del espíritu, sustentado en la tranquilidad de saber qué es lo que tenemos, cuánto vale, y sobre todo cómo lo protegemos; en este caso, la tan valiosa información. La seguridad existe en la medida de la conciencia del riesgo.

FUENTES DE INFORMACIÓN

1. *Bibliografía*

Gestión de riesgos, análisis y cuantificación, *http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/4AnalisisycuantificaciondelRiesgo%28AR%29_es.pdf.*

MUÑOZ, Néstor, *Qué es la triada CIA o CID*, *https://es.linkedin.com/pulse/qué-es-la-triada-cia-o-cid-néstor-muñoz.*

NISSENBAUM, Helen, *Privacidad amenazada,* trad. de Enrique Mercado, México, Océano, 2011.

REYES, Alfredo, "Ciberespacio y sociedad", *Seguridad y defensa en el ciberespacio,* México, Centro de Estudios Superiores Navales, 2015.

SULLIVAN, Brian *et al*., *Tendencias de seguridad cibernética en América Latina y el Caribe*, Washington DC, Symantec-Organización de los Estados Americanos, 2014.

TENORIO, Guillermo, *Los datos personales en M*éxico, perspectivas y retos, México, Porrúa-Universidad Panamericana, 2012.

TORRES, Rosa María, *Sociedad de la información/Sociedad del conocimiento*, Universidad de Barcelona, 21 de abril de 2005, *http://www.ub.edu/prometheus21/articulos/obsciberprome/socinfsoccon.pdf.*

VÁZQUEZ, Rubén, "Buenas prácticas para reducir los impactos de amenazas y riesgos de la información en el ciberespacio", *Seguridad y defensa en el ciberespacio,* México, Centro de Estudios Superiores Navales, 2015.

2. *Legislación*

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

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

3. *Sitios de Internet*

https://www.certsuperior.com/Blog/que-es-el-cifrado-y-para-que-funciona-medida-de-seguridad-primordial-para-tu-empresa.

https://www.isaca.org/KnowledgeCenter/Research/ResearchDeliverables/Pages/Data-Leak-Prevention.aspx.

http://blog.smartekh.com/sandbox-porque-paraque.

http://cnnespanol.cnn.com/2017/05/15/que-es-un-virus-ransomware-y-como-actua/.

CAPÍTULO QUINTO
Los derechos ARCO

Jorge SALES BOYOLI[60]
Rodrigo Francisco MARTÍNEZ VERGARA[61]

SUMARIO

I. INTRODUCCIÓN

Hoy en día son ya numerosos los trabajos académicos en México que abordan el régimen jurídico de los datos, en particular los que se ocupan de un análisis descriptivo y pedagógico de los denominados derechos ARCO; ello hace evidente el interés que en la era digital despiertan, más allá de la muy importante intimidad y privacidad. Pero también obliga a presentar un abordaje diferente respecto a esta facultad rectificadora que deje de lado aspectos tradicionales del núcleo toral, a nuestro juicio, en la protección de datos. Todos estamos hambrientos de información y al mismo tiempo saturados de la misma.

[60] Socio Director de Bufete Sales Boyoli, S.C., egresado de la Universidad Panamericana.
[61] Asociado del área de Derecho Administrativo del Bufete Sales Boyoli, S.C., egresado de la Escuela Libre de Derecho.

Las nuevas tecnologías superan la capacidad humana para procesar y asimilar tantos datos a una velocidad vertiginosa; por ello es muy sencillo que las personas constantemente y en cuestión de segundos podamos tener acceso a la información de casi cualquier individuo, sin distinguir donde termina su protección y donde comienza la información pública. El Internet (por usar un término genérico) ha revolucionado la forma de comunicar y el tráfico de información, de la cual en algunas ocasiones contamos o no con el consentimiento del titular de los datos, sin detenernos a reparar en ello. Las redes sociales han cambiado la forma en la que las personas tienen control sobre su información; en muchas ocasiones ni ellas mismas saben que en efecto cuentan con mecanismos legales para ser guardianes de su propia información que los identifica o los hace identificables. La acepción moderna de privacidad implica la función dinámica de *controlar* la circulación de información relevante de cada sujeto, ahí es donde entran los derechos instrumentales de acceso, rectificación, cancelación y oposición de datos personales mejor conocidos en nuestro país por el acrónimo ARCO.

Consecuentemente, frente a la actual sociedad de la información, resulta necesario concibamos a la privacidad como un derecho activo de control sobre el flujo de la información que afecta a cada sujeto y no solamente como un estatus negativo en donde las personas tienen la facultad de repeler intromisiones arbitrarias en su esfera privada.

El rango constitucional de los derechos ARCO hace patente su importancia en el orden jurídico nacional, que ha replicado acertadamente otros ordenamientos internacionales. Si bien, los principios en materia de datos personales son la columna vertebral del andamiaje jurídico en la materia[62], la forma de hacerlos valer frente a las autoridades y frente a los particulares, son realmente la mejor muestra de su eficacia; un derecho ineficaz y de ello tenemos muestras abundantes, se mide por la buena aplicación y la manera de hacerlo valer con la seguridad de las consecuen-

[62] Los principios en materia de protección de datos personales en posesión de los particulares los encontramos en el Artículo 6o. de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley), y son licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

cias particulares. Ello le permite al titular de los datos controlar la cantidad, calidad y el uso de los datos personales que trate el responsable.

Describiendo a los derechos ARCO, el acceso a los datos personales implica la posibilidad del titular de conocer, qué clase de información tiene el responsable y cómo la está utilizando, éste cumplirá con su obligación cuando ponga a disposición de aquél sus datos personales mediante copias, documentos electrónicos, medios ópticos, sonoros, visuales, holográficos o cualquier otro mecanismo que se prevea en el aviso de privacidad[63].

La rectificación de los datos personales encuentra su fundamento dentro del principio de calidad. La información inexacta, incompleta, incorrecta o desactualizada puede generar perjuicios de difícil o inclusive imposible reparación para el titular del dato. Una información con alguna de estas características simplemente será información falsa al no ser congruente con la realidad. Pensemos en un consumidor reclamando la devolución de un pago indebido a un proveedor y no pueda proceder porque este último tenga incorrecta su Clave Bancaria Estandarizada (CLABE) o una mujer viuda exigiendo a la seguridad social el pago de la pensión de su marido sin poder cobrarla porque su registro federal de contribuyentes es inexacto.

La cancelación tiene lugar cuando el titular de los datos personales considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la legislación secundaria[64]. La mera presunción de un trato indebido del dato es suficiente para que el titular pueda solicitar su eliminación definitiva.

Finalmente, el derecho de oposición se traduce en una facultad del titular de los datos de solicitarle al responsable que gestione un listado de exclusión derivado de la negativa al tratamiento de su información personal[65]. Los ejemplos más tangibles se dan cuando los datos son objeto de tratamiento para actividades vinculadas con la publicidad y la prospección comercial.

---

63 Artículo 102 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Reglamento).

64 Artículo 106 del Reglamento.

65 Artículo 110 del Reglamento.

II. LOS DERECHOS ARCO EN EL CONTEXTO CONSTITUCIONAL MEXICANO

El 20 de julio de 2007, se publicó en el Diario Oficial de la Federación, el Decreto por el que se adicionó un segundo párrafo, con siete fracciones, al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos. Algunos autores como Miguel Carbonell[66] la han calificado como una reforma "histórica" al dotar a los mexicanos de herramientas jurídicas para el ejercicio de su derecho fundamental de acceso a la información pública de manera uniforme en todo el territorio nacional. Si bien esta adición al texto constitucional estaba orientada a sentar los principios en esta materia, dos de sus fracciones hicieron una primera aproximación a los derechos de *acceso y rectificación* de datos personales solamente.

En efecto, las fracciones II y III, respectivamente, señalan: "… La información que se refiere a la vida privada y los *datos personales* será protegida en los términos y con las excepciones que fijen las leyes… 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…*". De esta forma observamos que los derechos ARCO nacieron limitados a nivel constitucional al acceso y a la rectificación de datos personales. En esa primera etapa, hace poco más de una década, los incipientes derechos ARCO solo podían ser ejercidos frente a las autoridades mexicanas y no así frente a los particulares como hoy en día es viable. No obstante, somos de la opinión que el legislador tuvo la oportunidad de emitir una ley de protección de datos personales en posesión de los particulares con base en la fracción II del Artículo 6o. antes mencionado; es decir no era necesario posteriormente adicionar un segundo párrafo al Artículo 16 de la Constitución Federal para proteger los datos personales en posesión de los particulares. Si aplicamos la máxima jurídica "donde el legislador no distingue el intérprete no debe distinguir", podemos afirmar que la protección constitucional es de carácter general y también le debería aplicar a los particulares y no solo a las autoridades. Máxime

---

[66] Carbonell, Miguel, *Los derechos fundamentales en México*, 4ª. ed., México, Porrúa, 2011, p. 591.

si tomamos en consideración la naturaleza del derecho a proteger. La información personal de alguien puede ser poseída por cualquier individuo bien sea en el sector público o en el privado. Los nombres, domicilios, fotografías, videos, imágenes, claves únicas de registros de población, huellas digitales, ideologías, preferencias políticas y cualquier otra información que identifique o pueda hacer identificable a una persona debe ser objeto de protección, al tener sentido, alcance y valor para una persona.

Con todo, los derechos fundamentales de protección de datos personales constituyen quizá, el ejemplo moderno más tangible respecto de la prerrogativa del gobernado para oponerse ante los actos considerados violatorios de derechos tanto por autoridades como por los particulares. La naturaleza volátil del derecho en cuestión, permite que los mismos puedan ser poseídos y transferidos en perjuicio del titular de los mismos, por ello resulta plausible su protección mediante un procedimiento sencillo que se ejerza frente al responsable de los datos.

Tuvieron que pasar dos años para que el Constituyente diera un segundo paso y reconociera los derechos de cancelación y oposición de datos personales.

El 1 de junio de 2009, se publicó en el Diario Oficial de la Federación, el Decreto por el que se adiciona un segundo párrafo, recorriéndose en su orden, al Artículo 16 de la Constitución Federal que creó el derecho fundamental a la "*protección de datos personales*" en sentido amplio, incluyendo explícitamente a los derechos ARCO, sentando el principio de que *todas las personas* tienen derecho "*… al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley…*".

Este segundo párrafo venía a complementar para los particulares el derecho que ya tenían las personas de acceso y rectificación ante las autoridades del Estado mexicano completando con ello el acrónimo ARCO. El mismo fue pensado para que el Congreso de Unión posteriormente emitiera una Ley de Protección de Datos en Posesión de los Particulares y en posesión de las autoridades. Este derecho fundamental nace con la adición de este segundo párrafo y se distingue de los derechos a la intimidad y a la privacidad como un derecho fundamental autónomo.

Asimismo, aquí se establecieron los límites al ejercicio de los derechos ARCO y que resultan ser constitucionalmente admisibles, siendo la seguridad nacional, las disposiciones de orden público, la protección de derechos de terceros, la seguridad y salud públicas.

A manera de ejemplo, un suscriptor de servicios de telefonía móvil no podría ejercer su derecho de cancelación al uso de su *nombre* por parte de un concesionario de telecomunicaciones en virtud de que el Artículo 190, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión, ordenamiento de orden público, obliga a este último a mantener este dato personal para el caso de tener que colaborar con las instancias de seguridad, administración y procuración de justicia[67]. Esta limitante se considera adecuada, idónea y proporcional para efectos de tutelar los derechos humanos a la vida y la integridad de las personas.

La aptitud para acceder y corregir la información personal, que generalmente se considera un aspecto central de la protección a la privacidad, no es un derecho absoluto. Los derechos ARCO en el ámbito constitucional, entendidos como principios en la materia, permiten abstraer ciertas condiciones necesarias para hacerlos útiles en la vida de las personas, en donde se incluyen temas de cuotas para su acceso y el procedimiento para su obtención. Como presupuesto necesario la persona tendrá que otorgar las pruebas suficientes acreditando contar con interés jurídico para obtener su información personal.

Ahora bien, a través de esta reforma se dota de la más alta jerarquía a los derechos ARCO dentro del ordenamiento jurídico mexicano. Por esta razón consideramos que estos derechos, junto con los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, constituyen la columna vertebral de la legislación en materia de protección de datos personales

---

[67] Artículo 190. Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:
…
II. *Conservar un registro y control de comunicaciones* que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:
a) *Nombre*, denominación o razón social y domicilio *del suscriptor*…

y son el instrumento idóneo para ejercer el derecho a la autodeterminación informativa. Sin estos derechos los principios antes mencionados carecerían de protección. De ahí que algunos autores, como Nelson Remolina Angarita, afirmen que los derechos ARCO son parte del "núcleo esencial" del derecho constitucional de la protección de datos[68].

En este sentido, la forma de proteger la información que identifica o hace identificable a una persona es a través de estas cuatro herramientas esenciales; sin ellas la persona quedaría desprotegida ante el uso indebido de su información personal. El concepto de los derechos ARCO implica una idea de dominio y control sobre la información del titular frente al responsable de la misma. ¿Qué herramienta más eficaz y práctica podría haber que una mera solicitud de eliminación de un domicilio, una petición de rectificación de un registro federal de contribuyentes, la eliminación del nombre de un persona de la lista de condóminos que han incurrido en mora de sus obligaciones *propter rem* o la oposición de una persona al uso de su información personal para cuestiones publicitarias?

En tal virtud, los derechos ARCO encajan en la categoría de los derechos de libertad, entendiéndose esta como una libertad positiva, donde un sujeto tiene la posibilidad de orientar su voluntad hacia un objetivo, de tomar decisiones, sin verse determinado por la voluntad de otro. Es decir, el individuo está dotado de la prerrogativa para ejercer, cuando lo estime conveniente, el control del flujo de su información personal, por estimar que puede ser mal utilizada por alguien más. Lo importante es que esta información ni siquiera tiene que estar catalogada como sensible sino puede ser cualquier información que simplemente haga identificable a la persona. Ello sin perjuicio del mayor cuidado que en lo jurídico se exige, válidamente, tratándose de datos sensibles susceptibles de ocasionar discriminación, como sería información sobre la preferencia sexual de las personas o su orientación religiosa.

---

[68] Remolina Angarita, Nelson, "Los derechos de acceso, rectificación, cancelación y oposición en la Ley de Datos Personales y su Reglamento", en Piñar Mañas, José Luis, y Ornelas Núñez, Lina (coords.), *La protección de datos personales en México*, México, Tirant Lo Blanch, 2013, pp. 177-201.

En consecuencia, los derechos ARCO constituyen una especie de autorización otorgada por el Estado para que un particular pueda acudir de manera lícita con otro particular, o con el mismo Estado, a solicitarle lleve a cabo una acción de tratamiento de información en beneficio del titular del dato, quien es al final la persona que permanentemente debe tener el control sobre su propia información.

La protección de la intimidad y la privacidad –el primero entendido como el núcleo duro del segundo– supone el reconocimiento a la facultad de la persona para acceder a su información personal, a tener un control sobre la misma y a rechazar cualquier invasión que considere le genera una molestia en su mera comodidad. Ello viene del antecedente al derecho a estar solo, a la tranquilidad del sujeto[69]. Este derecho es una expresión de la libertad personal que cada uno tiene de decidir por sí mismo quien puede conocerlo y de qué forma puede conocerlo.

Por esta razón, en palabras de Aristeo García González, "el uso y control sobre los datos concernientes a cada persona, debe serle reconocido ya no solo como una mera prerrogativa, sino como un derecho fundamentalmente protegido y garantizado por mecanismos de protección idóneos"[70]. Así, vemos que la protección a los datos personales puede estar catalogada dentro de la tercera generación de derechos humanos. Aquellos que nacen del uso de las nuevas tecnologías y que inclusive se pueden hacer valer frente a otros particulares. Los derechos ARCO, como derechos fundamentales, al estar expresamente reconocidos en nuestra Constitución son objeto de protección por el Estado a través de la legislación secundaria.

III. LOS DERECHOS ARCO A NIVEL INTERNACIONAL

En consonancia con la casi nula existencia de fronteras en el tráfico de información, los derechos ARCO también han sido reconocidos a nivel mundial a través de distintos instrumentos internacionales emitidos por autoridades y redes globales como lo son la Organización para la Cooperación y Desarrollo Económicos

---

[69] Warren, S., y Brandeis, L., "The right to privacy", *Harvard Law Review*, trad. de Benigno Pendas y Pilar Baselga, Madrid, Civitas, 1995.

[70] García González, Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", *Boletín Mexicano de Derecho Comparado*, México nueva serie, año XL, número 120, septiembre-diciembre de 2007, pp. 743-778.

(OCDE), el Parlamento Europeo, el Consejo de Europa (CE), la Organización de las Naciones Unidas (ONU), el Foro de Cooperación Económica Asia Pacífico (APEC) y la Red Iberoamericana de Protección de Datos Personales (RIPD); los cuales han emitido diversas resoluciones, recomendaciones, directivas y directrices que involucran los principios generalmente aceptados y reconocidos en la materia.

Si bien estas autoridades y sus resoluciones pueden tener diferencias atendiendo a los ámbitos espaciales en donde tienen efectos, los derechos ARCO se hacen presentes como mecanismo de efectividad de protección a los datos personales, lo que se traduce de manera uniforme en la protección al derecho de la autodeterminación informativa.

Nelson Remolina Angarita[71] nos proporciona un cuadro comparativo práctico e ilustrativo sobre la forma en las que los distintos ordenamientos internacionales prevén los derechos ARCO. Los documentos comparados por dicho autor son:

a) Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales del 23 de septiembre de 1980 por la Organización para la Cooperación y Desarrollo Económicos (OCDE);
b) Convenio 108 del Consejo de Europa, de fecha 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal;
c) Principios rectores para la reglamentación de los ficheros computarizados de datos personales, adoptados por la Asamblea General de la ONU en su resolución 45/95, de 14 de diciembre de 1990;
d) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de fecha 24 de octubre de 1995, relativa a la protección de los datos personales de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos;
e) Marco de privacidad del Foro de Cooperación Económica Asia (APEC);
f) Carta de los derechos fundamentales de la Unión Europea (2000/C 364/01);

---

[71] Remolina Angarita, Nelson, *op. cit.*, p. 184.

g) Directrices para la armonización de la protección de datos en la comunidad iberoamericana aprobadas por la Red Iberoamericana de Protección de Datos; y

h) "Estándares internacionales sobre protección de datos y privacidad", aprobados el 5 de noviembre de 2009 en Madrid, en el marco de la 31° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (Res Madrid).

INCORPORACIÓN EXPLÍCITA DE LOS DERECHOS ARCO EN DOCUMENTOS INTERNACIONALES				
	ACCESO	**RECTIFICACIÓN**	**CANCELACIÓN**	**OPOSICIÓN**
OCDE, 1980	Sí	Sí	No	No
Conv. 108 del CE, 1981	Sí	Sí	No	No
Res ONU 45/95, 1990	Sí	Sí	No	No
Dir 95/46/CE, 1995	Sí	Sí	No	Sí
APEC, 1999	Sí	Sí	No	No
Carta Europea, 2000	Sí	Sí	No	No
RIPD, 2007	Sí	Sí	Sí	Sí
Res Madrid, 2009	Sí	Sí	Sí	Sí

Como puede observarse, a través de la información compilada por dicho autor, los derechos de acceso y rectificación son comúnmente aceptados por todas estas cartas internacionales, mientras que los derechos de cancelación y oposición no encuentran uniformidad en su regulación. Situación similar a la sucedida en el ámbito constitucional mexicano donde los primeros derechos reconocidos a nivel constitucional fueron los de acceso y rectificación para posteriormente incluirse los de cancelación y oposición.

Por parte de la Organización de los Estados Americanos, de la cual México es parte desde 1948, existe, mientras se escriben estas líneas, un proceso de prepa-

ración, discusión y aprobación de la Ley Modelo Interamericana sobre Protección de Datos Personales. Ésta tiene por objeto establecer parámetros generales y ser una hoja de ruta que puede ser incorporada completa o parcialmente en la legislación interna del Estado[72].

La Asamblea General de la OEA, durante el 83° periodo ordinario de sesiones del Comité Jurídico Interamericano, el Presidente le pidió al Dr. David P. Stewart que fungiera como relator del tema. En este sentido, del 10 al 14 de marzo de 2014, durante el 84° periodo ordinario de sesiones, el Dr. David P. Stewart presentó el documento denominado "Privacidad y Protección de Datos"[73], teniendo en cuenta los sucesos y normas internacionales pertinentes, de los cuales para los efectos que nos importan y tienen relación con el tema de derechos ARCO resaltamos:

a) La evolución constante de las tecnologías de la información amenaza constantemente la privacidad personal;
b) En las Américas no ha surgido un enfoque regional coherente;
c) Más que la redacción de códigos y leyes lo que necesita la región es una mayor interacción con los Estados miembros;
d) Para establecer la Ley Modelo se deben primero asentar los principios generales sobre privacidad y protección de datos para garantizarlos como los derechos sustantivos en juego y respetar la autodeterminación informativa de las personas;
e) Las personas debe contar con mecanismos de protección frente al uso de su información por parte de terceros;
f) Se debe buscar un equilibrio entre el derecho de las personas a controlar la forma en que se recopilan, almacenan y utilizan sus datos personales y los intereses de las organizaciones en el uso de datos personales con fines comerciales legítimos razonables.

---

[72] *http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp.*
[73] *http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI_doc_450-14.pdf.*

En este sentido, observamos como el medio para la protección de los principios y los mecanismos idóneos son precisamente los derechos ARCO con los que la persona podrá controlar su información de carácter personal en la mejor forma posible. Sin embargo, será necesario siempre, buscar un equilibrio sano entre el derecho de las personas a controlar su información y el libre flujo transfronterizo de información con fines comerciales legítimos razonables.

Confiamos que la Ley Modelo emitida eventualmente por la OEA pueda ayudar a mejorar los procesos para ejercer los derechos ARCO en las legislaciones internas de los Estados parte, incluyendo México. Sobre todo sea un promotor natural de la cooperación en el ejercicio de los derechos ARCO a niveles internacionales dentro de la región de las Américas. El flujo casi infinito de la información en la región crea la necesidad de establecer procesos internacionales para que las personas tengan un control sobre su información y crear una autoridad garante que pueda velar por su cumplimiento.

IV. LOS DERECHOS ARCO EN LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES Y EL REGLAMENTO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

El día 5 de julio de 2010 se publicó en el Diario Oficial de la Federación, el Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Ley), ordenamiento de orden público y de observancia general en toda el territorio nacional que tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Poco más de un año después, el 21 de diciembre de 2011, el Ejecutivo Federal publicó en el Diario Oficial de la Federación, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Reglamento) que tiene por objeto reglamentar en la esfera administrativa la Ley secundaria antes expedida.

Consideramos correcto que la Ley tenga como propósito garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Lo que busca es tutelar el derecho de las personas de reservarse ciertos aspectos de su vida frente a la acción y conocimiento de terceros que tengan la calidad de particulares.

A manera de antecedente, dos años antes a la emisión de la Ley, el Tercer Tribunal Colegiado en Materia Civil del Primer Circuito emitió una interesante tesis en donde reconoció el derecho de las personas a la autodeterminación informativa y su relación con el derecho a la intimidad, señalando que el derecho de la autodeterminación de la información supone la posibilidad de elegir qué información de la esfera privada de la persona puede ser conocida o cuál debe permanecer en secreto, así como designar quién y bajo qué condiciones puede utilizar esa información (Amparo en Revisión 73/2008)[74]. Consecuentemente, este derecho puede ser oponible frente a los poderes públicos y frente a los particulares.

Lo relevante de esta tesis es que acepta la existencia de un derecho que no estaba tutelado por una ley secundaria (derecho a la autodeterminación informativa) en ese momento y reconoce que este puede ser oponible, inclusive, frente a los particulares como sujetos obligados, privilegiando la doctrina de la eficacia horizontal de los derechos fundamentales[75], ello antes de la reforma constitucional en materia de derechos humanos publicada en el Diario Oficial de la Federación el 10 de junio de 2011.

Ahora bien, como se ha dicho, el núcleo fundamental del derecho a la protección de datos personales gira en torno a los principios de finalidad, responsabilidad, información, proporcionalidad, licitud, lealtad, consentimiento y calidad y los mecanismos para su protección, es decir, los derechos ARCO. El rango constitucional de estos últimos deja en claro su importancia y trascendencia en la legislación secundaria y disposiciones infra-legales.

---

[74] Tesis I.3o.C.695 C, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXVIII, septiembre de 2008, p. 1253.

[75] Para conocer más acerca de la eficacia horizontal de los derechos fundamentales puede consultarse, Mijangos y González, Javier, *Los derechos fundamentales en las relaciones entre particulares*, México, Porrúa-Instituto Mexicano de Derecho Procesal Constitucional, 2007, Biblioteca de Derecho Procesal Constitucional, número 18.

En primer lugar el ejercicio de los derechos ARCO debe ser, en la medida de lo posible, sencillo y parcialmente gratuito. No serviría de nada que las personas tengan la carga de llevar a cabo acciones desproporcionadas para la protección de su información personal. De lo contrario su ejercicio sería prácticamente inexistente. La idea es que los particulares puedan ejercerlos por sí mismos sin la necesidad de la ayuda de un experto (como lo sería un abogado especializado en la materia), a menos de encontrarse ante una negativa del responsable para acceder, rectificar, cancelar o excluir sus datos personales.

Por otra parte, recordemos que el ejercicio de estos derechos no es absoluto y encuentra restricciones constitucionales por razones de orden público, seguridad y salud pública, o para proteger derechos de terceros.

Estimamos, a diferencia de los casos donde los datos se encuentran en manos de la autoridad, existen muy pocas hipótesis viables donde un particular podría negarse a, por ejemplo, cancelar o rectificar la información personal de otro particular. Las razones de la negativa y la limitación tendrían que estar sumamente bien sustentadas para evitar una sanción por parte de la autoridad garante. Un ejemplo legítimo para negar la cancelación, podría materializarse si un usuario de servicios de seguridad privada solicitara a la empresa de seguridad que opera en la modalidad "sistemas de prevención y responsabilidades"[76] que elimine su nombre y domicilio de su base de datos.

A manera ejemplificativa, la restricción legítima al ejercicio de los derechos ARCO la encontraríamos en el Artículo 32, fracción XXXII, de la Ley Federal de Seguridad Privada[77] que obliga a esta clase de empresas a crear y mantener un

---

[76] Artículo 15. Es competencia de la Secretaría, por conducto de la Dirección General, autorizar los servicios de Seguridad Privada, cuando estos se presten en dos o más entidades federativas y de acuerdo a las modalidades siguientes: …
VI. *Sistemas de prevención y responsabilidades*. Se refieren a la prestación de servicios para obtener informes de antecedentes, solvencia, localización o actividades de personas, y…

[77] Artículo 32. Son obligaciones de los prestadores de servicios: …
XXXII. Tratándose de prestadores de servicios que operen en la modalidad prevista en la fracción VI del artículo 15 de la presente Ley, deberán crear y mantener un registro de compradores y usuarios, el cual deberá contener datos personales del usuario y la persona o empresa que suministró el equipo.

registro de compradores y usuarios, el cual deberá contener "*datos personales*" del usuario y la persona o empresa que suministró el equipo. Al ser esta una ley de orden público y de observancia general en toda la república sus disposiciones son irrenunciables, por lo que los particulares prestadores de servicios de la modalidad citada podrán negarse, legítimamente, al ejercicio de los derechos ARCO por parte del titular, siendo este el que contrató los servicios privados de seguridad.

Asimismo, el ejercicio de cualquiera de los derechos ARCO no es un prerrequisito para el ejercicio de los otros derechos[78]. Es decir, no será necesario que primero ejerza mi derecho de acceso para que después tenga que ejercer mi derecho de cancelación. El ejercicio de los derechos es independiente y pueden solicitarse de manera separada, en la misma solicitud que se haga o en una diversa. Esta permisibilidad la encontramos dentro del mismo derecho a la autodeterminación informativa antes explicado.

El responsable debe tratar los datos de tal forma que se facilite el ejercicio de los derechos ARCO del titular. Aquél puede designar a una persona o empresa que se encargue de tramitar las solicitudes de derechos ARCO que reciba. Recordemos que estas obligaciones aplican para todas las personas ubicadas dentro del territorio nacional con excepción de las sociedades de información crediticia y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial[79].

El responsable de garantizar los derechos ARCO será un banco, un colegio, un abogado, un dentista, un fotógrafo, un hotel o cualquier otra persona o empresa que trate datos que identifiquen o hagan identificable a una persona física. Por ejemplo, no podremos ejercer los derechos ARCO contra una persona que tenga un álbum de fotos en las cuales se observe nuestra imagen si la tiene guardada en un cajón, a menos que el responsable sea un fotógrafo, use nuestra imagen con prospección comercial o la difunda en redes sociales. De esta forma quedaría incluido dentro del supuesto de aplicación de la norma al tener un ánimo de divulgación de nuestra imagen personal o la esté usando con fines de lucro.

---

[78] Artículo 87 del Reglamento.
[79] Artículo 2o. de la Ley.

El responsable tiene la obligación de otorgar una respuesta sobre la procedencia o no del ejercicio de los derechos ARCO, para lo cual cuenta con un plazo de 20 días hábiles contados a partir del momento que en recibió la solicitud. Si la respuesta se da en sentido positivo, la entrega, rectificación o cancelación de los datos debe realizarse dentro de los 15 días hábiles siguientes a la fecha en que se comunicó la respuesta de procedencia de los mismos.

Existe la posibilidad de que el responsable niegue total o parcialmente los derechos ARCO del titular. Sin embargo, deberá tener cuidado en la forma en que expone su justificación para evitar una sanción y necesariamente le deberá informar al titular que puede iniciar un procedimiento de protección de derechos ante la autoridad garante.

Recordemos que el sujeto sancionable es siempre el responsable del tratamiento de los datos, por ende, la ley castiga con apercibimiento, el no cumplir, sin razón fundada, con la solicitud del titular para el ejercicio de los derechos ARCO y con multa de 100 a 160,000 días de salario mínimo vigente en la Ciudad de México el actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de los derechos ARCO[80].

El ejercicio de estos derechos implica una libertad para el titular que no puede desconocerse por parte del responsable. El control sobre el flujo de su información personal es lo que debe prevalecer frente a la obstrucción del ejercicio legítimo de cualquiera de estos derechos.

V. EXPERIENCIAS PRÁCTICAS "NOVEDOSAS" EN EL EJERCICIO DE LOS DERECHOS ARCO

El ejercicio profesional de la abogacía, plantea frecuentemente retos que superan los conceptos genéricos de los libros o desafían las hipótesis jurídicas generales por definición de los ordenamientos legales. A manera de cierre para este capítulo basta describir con ánimo provocador algunos casos de frontera en materia de rectificación de datos.

---

[80] Artículo 63, fracciones I y II, y 64, fracciones I y II, de la Ley.

Las personas (físicas o morales)[81] son titulares de derechos, algunos claramente limitados a las primeras (personas físicas) como el derecho de libertad religiosa consagrado en nuestra Constitución, esta libertad religiosa, históricamente polémica en México, conlleva la libertad de cambiar libremente de religión o dejar de profesar cualquier religión[82]. ¿Esta libertad permite entonces a los particulares pedir la rectificación o cancelación de sus datos personales en registros, partidas, libros o ficheros de instituciones religiosas o incluso académicas con cierta identidad religiosa, en las que se han venido asentando? Esta cuestión deriva de un planteamiento profesional real donde debe considerarse la naturaleza personal y sensible de la preferencia religiosa en un país donde la mayoría de la población se declara, todavía católica.

Un trabajador da por terminada su relación laboral en virtud de una renuncia voluntaria y, en ejercicio de la libertad de trabajo, consagrada en la Constitución Política de los Estados Unidos Mexicanos, busca un nuevo empleo refiriendo su experiencia laboral anterior como parte de su historia de vida laboral. El potencial empleador pide referencias a sus anteriores patrones y ellos revelan datos personales sensibles que obran en su poder, perjudicando o privando de la contratación. ¿Estos hechos generan el derecho para el extrabajador de pedir se cancelen y rectifiquen de los archivos y expedientes laborales en poder del antiguo empleador?

---

[81] Sobre el derecho y obligación de las personas morales en materia de protección de datos véase la Contradicción de Tesis 56/2011 entre las sustentadas por la Primera y Segunda Salas de la Suprema Corte de Justicia de la Nación mexicana, donde se analiza ampliamente la titularidad en los derechos vinculados a datos de las personas jurídicas.

[82] En Derecho Canónico, este sentido negativo en el ejercicio de la libertad religiosa es cercano a la denominada apostasía prevista en el Canon 751 del Código de Derecho Canónico vigente.

VI. FUENTES DE INFORMACIÓN

1. *Bibliografía*

CANALS, Dolores *et. al.*, *Datos, protección, transparencia y buena regulación,* Girona, Documenta Universitaria, 2016.

CARBONELL, Miguel, *El ABC de los derechos humanos y del control de convencionalidad*, 2ª. ed., México, Porrúa, 2015.

CARBONELL, Miguel, *Los derechos fundamentales en México,* 4ª. ed., México, Porrúa, 2011.

GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", *Boletín Mexicano de Derecho Comparado*, México, nueva serie, año XL, número 120, septiembre-diciembre de 2007.

GARCÍA MARTÍN, Pilar, *Protección de datos. Manual de obligaciones y derechos en materia de protección de datos de carácter personal,* Sevilla, Punto Rojo, 2014.

MIJANGOS Y GONZÁLEZ, Javier, *Los derechos fundamentales en las relaciones entre particulares*, México, Porrúa-Instituto Mexicano de Derecho Procesal Constitucional, 2007, Biblioteca de Derecho Procesal Constitucional, número 18.

REMOLINA ANGARITA, Nelson, "Los derechos de acceso, rectificación, cancelación y oposición en la Ley de Datos Personales y su Reglamento", en PIÑAR MAÑAS, José Luis, y ORNELAS NÚÑEZ, Lina (coords.), *La protección de datos personales en México*, México, Tirant Lo Blanch, 2013.

WARREN, S., y BRANDEIS, L., "The right to privacy", *Harvard Law Review*, trad. de Benigno Pendas y Pilar Baselga, Madrid, Civitas, 1995.

2. *Legislación*

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

Ley Federal de Telecomunicaciones y Radiodifusión.

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

3. *Sitios de Internet*

http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI_doc_450-14.pdf.

http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp.

https://sjf.scjn.gob.mx/SJFSem/Paginas/SemanarioIndex.aspx.

CAPÍTULO SEXTO
Responsabilidades y sanciones

Nuhad PONCE[83]

SUMARIO

I. INTRODUCCIÓN

El derecho a la intimidad, privacidad y su defensa a través de la protección de los datos personales, es relevante en su día a día, ya que el tema del uso de las tecnologías de la información y comunicación, es un derecho humano fundamen-

[83] Es Licenciada en Derecho así como Maestra en Derecho de la Empresa por la Universidad Panamericana con mención honorifica. Está certificada por "Normatividad y Certificación Electrónica" (NYCE), como profesional certificado en protección de datos personales, nivel senior. Es miembro del Consejo Directivo de la Asociación Nacional de Abogados de Empresa, Colegio de Abogados, A.C. (ANADE). Es catedrática de licenciatura y especialidades de la Universidad Panamericana campus Mixcoac y Santa Fe; de la Maestría en Propiedad Intelectual de la Universidad Anáhuac México Norte, de la Maestría en Derecho Corporativo en la Universidad Anáhuac de Querétaro y la Universidad Anáhuac Cancún. Ha participado como panelista en diversas conferencias y programas especializados. Cuenta con distintas publicaciones en revistas especializadas en Derecho Corporativo y protección de datos.

tal que tradicionalmente se ha estudiado y aplicado desde el interés individual de las personas, con la finalidad de autodeterminar la información que se comparte con otros, el derecho a conocer las finalidades que dicha información tendrá, y para permitir el ejercicio de otros derechos, evitando así daños a la intimidad y privacidad.

En los últimos años se ha ido desarrollando la legislación aplicable para delimitar las responsabilidades y las sanciones que como responsables de datos personales debemos tener. También se han implementado diversas herramientas con el objetivo de salvaguardar la integridad de las personas.

Las responsabilidades y sanciones las analizaremos tomando el papel de responsable de los datos personales.

II. RESPONSABLE

En materia de protección de datos personales, el responsable será la persona jurídica y/o física, privada o pública, que decide sobre el tratamiento de los datos, es decir, toma decisiones sobre qué hacer con los mismos, es el responsable desde que el dato entra a formar parte del sistema de información hasta la eliminación del mismo, es el responsable durante toda la "vida" del dato[84].

Es importante destacar que nuestra legislación al día de hoy está dividida en dos grandes rubros: el privado y el público.

Por lo que hace al ámbito privado, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), define al responsable en su Artículo 3o. como: "la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales". Por otra parte y hablando del ámbito público, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), define en su Artículo 3o. al responsable como: "Los sujetos obligados a que se refiere el artículo 1o. de la presente Ley que deciden sobre el tratamiento de datos personales". Estos sujetos referidos por el dispositivo mencionado en dicha Ley, son: sujetos del ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y

[84] Blázquez Rodríguez, Carmen, *Responsable y encargado de tratamiento de datos personales*, Madrid, Convelia, 2011.

Judicial, órganos autónomos, partidos políticos, fideicomisos, y fondos públicos. 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.

Como responsables, ya sea en el ámbito privado o público, se tienen ciertas obligaciones o responsabilidades frente a los titulares de datos y frente a la autoridad. Las principales consisten en:

1. Elaborar avisos de privacidad. El aviso de privacidad es el instrumento mediante el cual el responsable en el manejo de los datos pone a consideración del titular de los mismos los alcances del manejo de datos que realizará en virtud del consentimiento del titular[85].

Como ya se ha visto en capítulos previos de esta obra, es responsabilidad elaborar los avisos de privacidad de acuerdo a cada base de datos, por los responsables. Estos avisos deben cumplir con lo señalado por el Artículo 16 de la LFPDPPP y por los Artículos 27 y 28 de la LGPDPPSO.

Es muy importante destacar que para la elaboración de los avisos de privacidad, el responsable debe primero analizar que bases de datos maneja, que datos requiere, con que objeto, y que tratamiento les dará. Por ejemplo, no será el mismo aviso de privacidad para los empleados de un hospital, que para sus pacientes.

2. Observar los principios rectores. El responsable en el tratamiento de los datos personales deberá observar los siguientes principios[86]:

a) Licitud. Este principio obliga al responsable a que el tratamiento de los datos personales, sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional[87].
b) Consentimiento. En este principio se menciona que el responsable deberá obtener el consentimiento para el tratamiento de los datos personales, salvo las excepciones que prevé la propia legislación.

---

85 Tenorio Cueto, Guillermo A., *Transparencia y acceso a la información*, México, Novum, 2014.
86 *Idem*.
87 Artículo 10 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Cabe destacar, aunque el consentimiento puede ser expreso o tácito, existe la crítica de la posible derogación de facto del consentimiento tácito, toda vez que en caso de algún procedimiento, el responsable siempre tiene la carga de la prueba. En este sentido y debido a que no se puede probar un hecho negativo, el Reglamento de la Ley otorga al responsable la obligación de tener el consentimiento de manera fehaciente.

Los dos principios mencionados previamente actúan como piedra angular del tratamiento legítimo de los datos personales.

c) Información. El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad, de conformidad con lo previsto en la Ley y el presente Reglamento[88].

d) Calidad. Los datos personales deben ser exactos, completos y actualizados para el cumplimiento de las finalidades para las que sean tratados. Los datos personales deben ser suprimidos una vez que se cumplan o agoten las finalidades para las cuales fueron recabados[89]. Este principio le corresponderá al responsable de la base de datos, quien estará a cargo de establecer los medios y mecanismos necesarios para evita la violación de los sistemas que contengan los datos.

e) Finalidad. El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades determinadas, explícitas y legítimas del responsable del tratamiento[90].

---

[88] Artículo 23 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[89] Artículo 36 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[90] Artículo 40 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

f) Lealtad. Para la obtención de datos personales no debe valerse del engaño o fraude, de forma tal que la persona no pueda conocer con propiedad los términos y condiciones vinculados a ese tratamiento[91].

g) Proporcionalidad. El tratamiento de datos personales debe circunscribirse a aquellos que resulten adecuados, relevantes y no excesivos con relación a las finalidades que justificaron su obtención[92].

h) Responsabilidad. El responsable está obligado a implementar aquellos mecanismos necesarios para evidenciar dicho cumplimiento, ante los titulares como a la autoridad garante[93].

3. Tener un tratamiento adecuado de los datos personales, de acuerdo a las finalidades previstas en el aviso de privacidad. El responsable debe dar tratamiento a los datos personales, limitándose al cumplimiento de las finalidades, que señaló en el aviso de privacidad. Es su responsabilidad que el tratamiento sea el que resulte necesario y adecuado con relación a los propósitos para los que fueron recabados los datos personales.

Para dar un tratamiento pertinente a los datos personales, es muy importante contar con el consentimiento del titular (véase el apartado de consentimiento).

4. Contar con las medidas de seguridad físicas, técnicas y administrativas correspondientes. Es responsabilidad de los que darán tratamiento a los datos personales, contar con las medidas de seguridad físicas, técnicas y administrativas, de las que se habló anteriormente. Estas medidas son para proteger los datos personales contra cualquier daño, pérdida, alteración, destrucción o uso no autorizado de los mismos.

---

[91] Artículo 44 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[92] Artículo 45 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

[93] Artículo 47 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Aunque la legislación vigente no hace mención, como en otros países, del tipo de medidas de seguridad que debe tenerse, si menciona que existe la expectativa de que el responsable utilice medidas no menores a las que mantiene para la protección de su misma información o secretos de negocio.

El no contar con estas medidas de seguridad puede tener serias consecuencias para el responsable.

5. Dar atención a los derechos ARCO que sean ejercidos o solicitados por los titulares. Todo responsable tiene la obligación de designar a una persona o departamento de datos personales, quien será quien dará trámite a las solicitudes de los titulares[94]. Esta designación es fundamental para fomentar la protección de los datos personales y para dar cumplimiento a las obligaciones que se tienen como responsable de datos personales. Al día de hoy la mayoría de los procedimientos de sanción del INAI son por falta de atención a solicitudes de derechos ARCO.

6. Guardar confidencialidad respecto de los datos personales. El responsable junto con los terceros (encargado) que intervengan en cualquier parte del tratamiento de los datos personales, tienen la obligación de guardar confidencialidad respecto de estos datos. Esta obligación no tiene vigencia alguna, por lo que subsiste aún terminada la relación que exista entre el responsable y el titular.

Mucho se ha hablado de si se pudo incluir una temporalidad para esta obligación de secrecía, sin embargo para cierto tipo de datos y para determinado tipo de responsables, la confidencialidad debe subsistir con el paso del tiempo. Por ejemplo: un laboratorio de análisis clínicos, guarda los datos de los estudios que se ha practicado un paciente, independientemente de si es un paciente recurrente o no. Es así como este responsable (laboratorio de análisis clínicos), guarda la información del titular y guarda secrecía respecto de dicha información. Sería ilógico pensar, que si el paciente no regresa en un determinado tiempo a practicarse algún otro estudio, pudiera entonces el laboratorio divulgar su información.

---

[94] Tenorio Cueto, Guillermo A., *Transparencia y acceso a la información*, *op. cit.*

III. AUTORIDAD GARANTE

En materia de protección de datos personales se entenderá como Instituto al INAI, quien tendrá el objetivo de difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, así como promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de las obligaciones por parte de los sujetos mencionados previamente[95].

El Instituto tiene las siguientes atribuciones[96]:

a) Vigilar y verificar el cumplimiento de las disposiciones contenidas en la LFPDPPP;
b) Interpretar en el ámbito administrativo la LFPDPPP;
c) Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas;
d) Emitir los criterios y recomendaciones, de conformidad con la LFPDPPP, para efectos de su funcionamiento y operación;
e) Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;
f) Conocer y resolver los procedimientos de protección de derechos y de verificación;
g) Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales;
h) Rendir al Congreso de la Unión un informe anual de sus actividades;
i) Acudir a foros internacionales;

---

[95] Artículo 38 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
[96] Artículo 39 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

j) Elaborar estudios de impacto sobre la privacidad previos a la puesta en prácticas de una nueva modalidad de tratamiento de datos personales;

k) Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales.

IV. OBLIGACIONES DE TRANSPARENCIA CON RESPECTO A LAS INSTITUCIONES PÚBLICAS

De acuerdo con el Artículo 7o. de la Ley Federal de Transparencia y Acceso a la Información Pública, todas las instituciones públicas deberán poner a disposición de la sociedad la siguiente información:

a) Su estructura orgánica;

b) Las facultades de cada unidad administrativa;

c) El directorio de sus servidores públicos, desde el nivel de Jefe de Departamento o sus equivalentes;

d) La remuneración mensual por puesto, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes;

e) El domicilio de la unidad de enlace, además de la dirección electrónica donde podrán recibirse las solicitudes para obtener información;

f) Las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos;

g) Los servicios que ofrecen;

h) Los trámites, requisitos y formatos. En caso de que se encuentren inscritos en el Registro Federal de Trámites y Servicios o en el Registro que para la materia fiscal establezca la Secretaría de Hacienda y Crédito Público, deberán publicarse tal y como se registraron;

i) La información sobre el presupuesto asignado, así como los informes sobre su ejecución, en los términos que establezca el Presupuesto de Egresos de la Federación;

j) Los resultados de las auditorías al ejercicio presupuestal de cada sujeto obligado que realicen, según corresponda, la Secretaría de la Función Pú-

blica, las contralorías internas o la Auditoría Superior de la Federación y, en su caso, las aclaraciones que correspondan;

k) El diseño, ejecución, montos asignados y criterios de acceso a los programas de subsidio;

l) Las concesiones, permisos o autorizaciones otorgados, especificando los titulares de aquellos;

m) Las contrataciones que se hayan celebrado en términos de la legislación aplicable.

La legislación vigente en materia de protección de datos personales, establece procedimientos para la vigilancia del cumplimiento de estas disposiciones.

V. PROCEDIMIENTO DE PROTECCIÓN DE DERECHOS

El procedimiento de protección de derechos se iniciará cuando exista una inconformidad por parte del titular derivada de acciones u omisiones del responsable con motivo de los derechos ARCO.

Se iniciará a petición del titular de los datos o de su representante legal, donde deberá expresar con claridad el contenido de su reclamación, y los preceptos que considere vulnerados[97].

Esta solicitud podrá presentarla el titular o su representante[98] ante el Instituto, de manera presencial, servicio de mensajería y medios electrónicos[99].

La solicitud de protección de derechos deberá contener la siguiente información[100]:

a) El nombre del titular o, en su caso, el del representante legal, así como del tercero interesado en caso de que exista alguno;

---

97 Artículo 45 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

98 Artículo 13 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

99 Artículo 12 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

100 Artículo 46 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

b) El nombre del responsable ante el cual se presentó la solicitud de ejercicio de los derechos ARCO;
c) El domicilio para oír y recibir notificaciones;
d) La fecha en que se le dio a conocer la respuesta del responsable, salvo que se inicie por falta de respuesta;
e) Los actos que motivan su solicitud;
f) Los demás elementos que se consideren procedentes.

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

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

Del estudio y análisis del contenido de la solicitud, el Instituto podrá ejercer las siguientes acciones:

a) Prevenir al titular dentro de los veinte días hábiles siguientes a la presentación de la solicitud;
b) Admitir la solicitud en un plazo no mayor a diez días hábiles;
c) Desechar por improcedente la solicitud;
d) Reconducir la solicitud si no se actualiza alguna de las causales de procedencia[101].

En caso de admisión, el Instituto notificará la misma al promovente, de igual manera al responsable, en un plazo no mayor a diez días hábiles, anexando copia de todos los documentos que el titular hubiere aportado, a efecto de que manifieste lo que a su derecho convenga en un plazo de quince días, con el objetivo de que el responsable manifieste lo que en su derecho convenga, para posteriormente el titu-

[101] Artículo 19 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

lar revisar la respuesta del responsable, y en caso de conformidad con la respuesta, el procedimiento será sobreseído[102].

Asimismo, durante el proceso se puede buscar una conciliación entre el titular de los datos o su representante y el responsable[103]. De llegarse a un acuerdo de conciliación entre ambos, este se hará constar por escrito y tendrá efectos vinculantes, que serán que la solicitud de protección de datos quedará sin materia y el Instituto verificará el cumplimiento del acuerdo respectivo.

En caso de no existir una conciliación, se continuará con el procedimiento de protección de derechos emitiéndose el acuerdo correspondiente[104].

El plazo máximo para dictar la resolución en el procedimiento de protección de derechos será de cincuenta días hábiles, contados a partir de la fecha de presentación de la solicitud de protección de datos, a excepción de una causa justificada por parte del Instituto donde se podrá ampliar por una vez el mismo plazo[105].

De igual manera en caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos de la misma, se prevendrá al titular de los datos dentro de los veinte días hábiles siguientes a la presentación de la solicitud de protección de datos, por una sola ocasión, para que subsane las omisiones dentro de un plazo de cinco días. Transcurrido este plazo, sino se ha desahogado la prevención se tendrá por no presentada la solicitud.

En este sentido el Instituto, tiene la facultad para suplir las deficiencias en los casos que así se requiera, siempre y cuando no altere el contenido original de la solicitud de acceso, rectificación, cancelación u oposición de datos personales, ni se modifiquen los hechos o peticiones expuestos en la misma o en la solicitud de protección de derechos.

---

[102] Artículo 22 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

[103] Artículo 25 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

[104] Artículo 34 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

[105] Artículo 46 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

VI. PROCEDIMIENTO DE VERIFICACIÓN

El INAI verificará el cumplimiento de la LFPDPPP y de la normatividad que de esta derive. Posteriormente al procedimiento de protección de derechos, seguirá el diverso de verificación, que podrá iniciarse de oficio o a petición de parte.

La verificación procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos a que se refiere la LFPDPPP o se presuma fundada y motivadamente la existencia de violaciones a dicha Ley[106].

A través de este procedimiento, el Instituto tendrá acceso a la información y documentación que considere necesarias, dependiendo la resolución que lo motive. La presentación de las denuncias, se deberán hacer por escrito o por medios electrónicos[107].

El procedimiento de verificación se podrá llevar a cabo de dos maneras distintas[108]:

a) Mediante requerimientos de información; y
b) A través de visitas de verificación.

En los cuales, el personal del Instituto que lleve a cabo las visitas de verificación, deberá presentarse en el domicilio del responsable, con el oficio de comisión y la orden de verificación debidamente fundada y motivada[109].

Posteriormente a la verificación, se levantará un acta de verificación, con todos los datos relativos a la actuación, así como de los involucrados.

---

[106] Artículo 59 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
[107] Artículo 49 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.
[108] Artículo 60 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.
[109] Artículo 63 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

VII. SANCIONES E INFRACCIONES

Las causales de incumplimiento que dan origen a una sanción en materia de datos personales son las siguientes:

a) En caso de que el responsable de los datos personales, no cumpla con la solicitud del titular para el acceso, rectificación, cancelación u oposición (ARCO) con respecto del tratamiento de sus datos personales, sin causa justificada bajo las excepciones que se mencionan en la Ley;

b) En caso de que el responsable actué con negligencia o dolo en la tramitación y respuesta de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

c) En caso de que el responsable declare dolosamente la inexistencia de los datos personales, cuando existan total o parcialmente en su base de datos;

d) En caso de que el responsable de un tratamiento a los datos personales en contravención a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad;

e) Omitir en el aviso de privacidad, alguno o todos los elementos;

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

g) No cumplir con el apercibimiento en caso de incumplimiento con la solicitud del titular;

h) Incumplir el deber de confidencialidad;

i) Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin el consentimiento del titular;

j) Transferir datos a terceros sin comunicar a estos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

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

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

m) En caso de que el responsable recabe o transfiera datos personales, sin el consentimiento expreso del titular;

n) En caso de que se impida al Instituto realizar el proceso de verificación;

o) En caso de que se recaben datos en forma engañosa y fraudulenta;

p) En caso de que el responsable continúe usando de manera ilegítima los datos personales del titular, una vez que este haya solicitado el cese del mismo por el Instituto o los titulares;

q) Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición;

r) Crear bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas;

s) Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto por esta Ley.

VIII. PROCEDIMIENTO DE IMPOSICIÓN DE SANCIONES

El procedimiento de imposición de sanciones se podrá iniciar como consecuencia de la resolución que se emita en los diversos de protección de derechos, o el de verificación, cuando tuviera el Instituto conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de la Ley[110].

El encargado de llevar a cabo el procedimiento de sanciones será el INAI, quien lo iniciará si posteriormente al desahogo del procedimiento de protección de derechos o del procedimiento de verificación, se tuviera conocimiento de un incumplimiento de los principios o disposiciones de esta Ley.

Se empieza con la notificación que efectué el Instituto al presunto infractor en el domicilio que se tenga registrado de este, sobre los hechos que motivaron el inicio del procedimiento.

---

[110] Artículo 68 de los Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

El Instituto le otorgará un plazo de quince días al presunto infractor, para que presente pruebas y ejerza su derecho de defensa, es decir manifieste lo que a su derecho le convenga.

En caso de que el presunto infractor no presente pruebas, el Instituto resolverá conforme a los elementos de convicción que disponga.

Posteriormente a que el presunto infractor presente las pruebas, el Instituto se encontrará facultado para analizar las que estime pertinentes para después proceder a su desahogo.

Una vez concluida la práctica de las pruebas, el Instituto notificará al presunto infractor el derecho que le asiste para que, de considerarlo necesario, esté presente sus alegatos dentro de los cinco días siguientes a su notificación.

Por último, el Instituto analizará todos los elementos de convicción que estime atingentes y resolverá en definitiva dentro de los cincuenta días siguientes a la fecha en que inicio el procedimiento sancionador. Sin embargo, este plazo se podrá ampliar por una vez y hasta por un periodo igual a este bajo causa justificada. La resolución que emita el Instituto deberá ser notificada a las parte[111].

IX. SANCIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

Las infracciones contempladas en la LFPDPPP tienen diversas sanciones que son las siguientes:

a) El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, es decir, en caso de que el responsable no cumpla con la solicitud de los derechos ARCO ejercida por el titular;
b) Una multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal;
c) Una multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal; y
d) Por último, en caso de que de una manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional

[111] Artículo 62 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal, así mismo en caso de que se trate de datos sensibles, las sanciones podrán incrementarse hasta por dos veces[112].

Para determinar la sanción que corresponde, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales deberá fundar y motivar sus resoluciones, tomando en cuenta:

a) La naturaleza del dato;
b) La notoria improcedencia de la negativa del responsable;
c) El carácter intencional o no, de la acción u omisión constitutiva de la infracción;
d) La capacidad económica del responsable; y
e) La reincidencia[113].

De igual manera, el Instituto impondrá sanciones sin perjuicio de la responsabilidad civil o penal que resulte.

X. DELITOS EN MATERIA DE TRATAMIENTO INDEBIDO DE DATOS PERSONALES

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

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

En el caso de que se trate de datos personales sensibles, las penas mencionadas previamente se duplicarán.

---

[112] Artículo 64 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
[113] Artículo 65 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Como podemos ver esta Ley tiene también sanciones privativas de libertad, y en algunos casos las penas son consideradas para delitos graves, por lo que no se alcanzará la libertad bajo fianza. Es importante destacar, que el tema de responsabilidad penal tratándose de una persona moral, recae en su representante legal.

XI. RECURSOS EN CONTRA DE LAS RESOLUCIONES DEL INAI

La LFPDPPP señala, que ante la resolución en sentido desfavorable, o bien, que no satisfaga a plenitud la pretensión del titular de los datos emitidos, el particular podrá promover el juicio de nulidad ante el hoy Tribunal Federal de Justicia Administrativa[114]: "Artículo 56. Contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa".

XII. PUBLICIDAD DE LAS RESOLUCIONES DEL INAI

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

XIII. SANCIONES IMPUESTAS POR EL INAI

Durante los últimos años el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ha impuesto diversas sanciones en materia de Datos Personales, entre los casos más relevantes resaltan los siguientes:

1. *Responsable: Banco Mercantil del Norte, S.A., Institución de Banca Múltiple, Grupo Financiero Banorte*

El veintidós de enero de dos mil catorce, el entonces Instituto Federal de Acceso a la Información y Protección de Datos, actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Organismo Autónomo, recibió una denuncia de una titular en contra de Banco Mercantil del Norte, S.A., Institución de Banca Múltiple, Grupo Financiero Banorte, por presuntas violaciones

---

[114] Tenorio Cueto, Guillermo A., *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares*, México, Porrúa, 2012.

a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, señalando que un contrato que celebro de crédito automotriz denominado "Autoestrene de Banorte" nunca se incluyó algún aviso de privacidad y de que de igual manera nunca otorgo su consentimiento para el tratamiento de sus datos personales, sin embargo, sus datos personales fueron transmitidos a un tercero llamado "INTEGRA CAPITAL", quien debido a esto, vulneró su integridad.

Posteriormente al analizar la situación, el INAI inició un procedimiento de verificación, que resultaría a favor de la titular de los datos personales, para posteriormente iniciar el procedimiento de sanciones en contra de los grupos mencionados previamente, quienes fueron sancionados con una multa aproximada de $18'544,200.00 (dieciocho millones quinientos cuarenta y cuatro mil doscientos pesos 00/100 M.N.) debido a que recabaron datos personales sensibles sin su consentimiento. De igual manera fueron sancionados con otra multa aproximadamente de $8'673,900.00 (ocho millones seiscientos setenta y tres mil novecientos pesos 00/100 M.N.). Debido a que se encontraron datos de la persona, sin su consentimiento recabados en su base de datos y por último se le impuso una multa de e $4'788,591.00 (cuatro millones setecientos ochenta y ocho mil quinientos noventa y un pesos 00/100 M.N.), debido a que los grupos mencionados anteriormente, no pusieron a disposición del titular un aviso de privacidad[115].

2. *Responsable: Radiom*óvil Dipsa*, S.A. de C.V. (Telcel)*

Con fecha 16 de abril de 2013, el Instituto Federal de Acceso a la Información y Protección de Datos recibió una denuncia de un titular, en la cual explicaba que celebró un contrato con Telcel, el cual venció por falta de pago, lo que conllevó a que el departamento de cobranza empezara a comunicarse con los conocidos del Titular para exigir el pago del cumplimiento del contrato, posteriormente esta información fue comprobada por el gerente del departamento de cobranza, al confirmar que se empezaron a comunicar con los conocidos del titular, debido a la falta de respuesta del mismo. Debido a estas infracciones, Radiomóvil Dipsa, S.A. de C.V. (Telcel) fue

[115] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Resoluciones, procedimiento de imposición de sanciones, Expediente: PS.0016/14.

sancionado con una multa de $1’813,280.00 (un millón ochocientos trece mil doscientos ochenta pesos 00/100 M.N.). De igual manera fue sancionado con una multa de $3’399,900.00 (tres millones trescientos noventa y nueve mil novecientos pesos 00/100 M.N.) por incumplir el deber de confidencial establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Así mismo con otra multa de $3’108,480.00 (tres millones ciento ocho mil cuatrocientos ochenta pesos 00/100 M.N.), por vulnerar la seguridad de bases de datos, locales, programas o equipos y finalmente con una multa de $1’942,800.00 (un millón novecientos cuarenta y dos mil ochocientos pesos 00/100 M.N.), por recabar o transferir datos personales sin el consentimiento expreso del titular[116].

3. *Responsable: Sport City, S.A. de C.V.*

El 6 de junio de 2012, El Instituto Federal de Acceso a la Información y Protección de Datos, recibió una denuncia por presuntas violaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que mencionaban que en su aviso de privacidad en la página de internet se estaba omitiendo que los titulares de los datos personales podían oponerse al tratamiento de los datos personales, lo que implicó que posteriormente se iniciara un proceso de verificación en su contra, y al ser correcta la información, se procediera a un procedimiento de imposición de sanciones. El Instituto Federal de Acceso a la Información y Protección de Datos Personales, impuso una multa de $1’246,600.00 (un, doscientos cuarenta y seis mil seiscientos pesos 00/100 M.N.) por omitir en el aviso de privacidad, alguno o todos los elementos que este debe contener[117].

4. *Responsable: Grupo Camtol, S.A. de C.V.*

El veinticuatro de octubre de dos mil catorce, el entonces Instituto Federal de Acceso a la Información y Protección de Datos, actualmente Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales,

---

[116] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Resoluciones, Procedimiento de Imposición de Sanciones, Expediente: PS.0026/13.

[117] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Resoluciones, Procedimiento de Imposición de Sanciones, Expediente: PS.0004/12.

Organismo Autónomo, recibió de una titular, una denuncia en contra de Grupo Camtol, S.A. de C.V, por presuntas violaciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, señalando medularmente que debido a la mala obtención de sus datos personales, no logro el acuerdo que había sido pactado previamente, en base a esto, el Instituto sancionó a Grupo Camtol, S.A. de C.V. con una multa de $269,160.00 (Doscientos sesenta y nueve mil ciento sesenta pesos 00/100 M.N.) basándose en que el tratamiento de los datos personales, fueron en contravención a los principios.

5. *Responsable: Operadora Oceánica Internacional, S.A. de C.V.*

El pleno del Instituto, impuso una multa de $2'493,200.00 (dos millones cuatrocientos noventa y tres mil doscientos pesos 00/100 M.N.) a Operadora Oceánica Internacional, S.A. de C.V., por violar la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

La sanción fue acordada por unanimidad en el Órgano Colegiado, después de que se acreditó que la empresa no pudo desvirtuar el haber obstruido actos de verificación ordenados por el INAI.

El procedimiento fue ordenado a partir de que el Instituto tuvo conocimiento de que en una nota periodística del 18 de mayo de 2011 se hicieron públicos los datos de una persona "que presuntamente" había sido paciente del "Centro de Rehabilitación Oceánica".

En dos ocasiones (23/05/11 y 12/07/11), el INAI solicitó a la empresa un informe relacionado con dicha publicación, pero no atendió ninguno de ellos.

Ante la negativa, el Instituto ordenó una visita de verificación a Operadora Oceánica Internacional, S.A. de C.V., en sus instalaciones en Mazatlán Sinaloa; sin embargo, cuando el personal comisionado se presentó al domicilio, no se le dieron las facilidades correspondientes y se le negó el acceso al inmueble, obstruyendo con ello los actos de verificación de la autoridad.

En razón de lo anterior, el Pleno del Instituto determinó el 21 de marzo de 2012 el inicio de un procedimiento de imposición de sanciones.

Inconforme con esta resolución, la empresa presentó un juicio de nulidad ante el entonces Tribunal Federal de Justicia Fiscal y Administrativa, autoridad que el 8 de abril de 2013 dictó sentencia definitiva en contra de Oceánica.

Con este fallo, se dio continuidad al procedimiento en contra de Operadora Oceánica Internacional, S.A. de C.V., el cual quedó resuelto con la imposición de la citada multa, por la obstrucción del procedimiento de verificación previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Donde en dicha se Ley establece que constituyen infracciones a la misma, "obstruir los actos de verificación de la autoridad".

XIV. FUENTES DE INFORMACIÓN

1. *Bibliografía*

BLÁZQUEZ RODRÍGUEZ, Carmen, *Responsable y encargado de tratamiento de datos personales*, Madrid, Convelia, 2011.

TENORIO CUETO, Guillermo A., *Los datos personales en México. Perspectivas y retos de su manejo en posesión de particulares,* México, Porrúa, 2012.

TENORIO CUETO, Guillermo A., *Transparencia y acceso a la información*, México, Novum, 2014.

Transparencia, acceso a la información y datos personales, México, IFAI, 2007.

VITAL ROMÁN SÁNCHEZ, Carlos, *Derecho a la privacidad, a la protección de datos y a la información en México*, México, Thomson Reuters, 2015.

2. *Legislación*

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

Ley Federal de Transparencia y Acceso a la Información Pública.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos de los Procedimientos de Protección de Derechos, de Investigación y Verificación, y de Imposición de Sanciones.

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

3. *Sitios de Internet*

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Resoluciones, procedimientos de sanciones, *http://inicio.inai.org.mx/SitePages/ResolucionesPDP.aspx.*

SEGUNDA PARTE

Los desafíos contemporáneos de la protección de datos

CAPÍTULO SÉPTIMO
Protección de datos personales en el sector público

Josefina ROMÁN VERGARA[118]
Luis Ricardo SÁNCHEZ HERNÁNDEZ[119]

SUMARIO

I. BREVE ANÁLISIS SOBRE LA DIMENSIÓN Y CONTEXTO DE LA PROTECCIÓN DE LOS DATOS PERSONALES

La protección de datos personales ha adquirido relevancia en la actualidad como un derecho fundamental. Los efectos de la modernidad en la edad contempo-

[118] Doctora en Derecho, Comisionada y Excomisionada Presidenta del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (INFOEM). Primera Coordinadora de Organismos Garantes de las Entidades Federativas del Sistema de Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

[119] Director de Protección de Datos Personales del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos de Personales del Estado de México y Municipios (INFOEM).

ránea, dieron relieve a los derechos de la personalidad de los individuos como se puede apreciar en el artículo "*The right to privacy*", que en su inicio señala:

> El que los individuos deban contar con total protección de sus derechos a su persona y propiedades, es un principio del derecho común, pero con el paso del tiempo ha sido necesario definir continuamente la naturaleza y extensión del ámbito de su protección. Los cambios políticos, económicos y sociales implican el reconocimiento de nuevos derechos y el derecho común se vuelve eternamente joven, puesto que debe ampliarse para cumplir las demandas de la sociedad. Así, en varios momentos tempranos, las leyes únicamente daban remedios para las injerencias físicas con la vida o la propiedad, para transgresiones *vi et armis* (fuerza y armas). Entonces, el "derecho a la vida" servía únicamente para proteger ese supuesto a través de diversos mecanismos, el significado de la libertad se concebía a través de las garantías contra su restricción, y el derecho a la propiedad aseguraba al individuo sus tierras y ganado. Posteriormente, vino el reconocimiento de la naturaleza espiritual del ser humano, de sus sentimientos e intelecto. Gradualmente, el alcance de dichos derechos se fue ampliando; y ahora, el derecho a la vida ha adquirido el significado de disfrutar la vida –el derecho a ser dejado solo, el derecho para garantizar la libertad de ejercer una extensa gama de privilegios civiles, y el concepto de propiedad se ha ampliado para comprender cada forma de posesión– tanto de manera intangible, así como en sus aspectos tangibles[120].

El uso extendido de nuevas tecnologías ha puesto de relieve el desdoblamiento en el alcance del ámbito de actuación de las personas, dando lugar a la reflexión sobre conceptos inherentes tales como vida privada, privacidad e intimidad[121], que no son unívocos, sino que adquieren una dimensión particular en las culturas las cuales se encuentran insertas y las características que rigen su contexto en un momento determinado.

---

[120] Warren, Samuel D., y Brandeis, Louis D., "The right to privacy", *Harvard Law Review*, vol. 4, número 5, 15 de diciembre de 1890, pp. 193-220, *http://www.jstor.org/stable/1321160?seq=1#page_scan_tab_contents, el 25/08/2017.*

[121] *Cfr*. Garzón Valdés, Ernesto, *Lo íntimo, lo privado y lo público*, México, IFAI, 2005, *http://201.144.56.20/transparencia/cuadernillo_06.pdf, ISBN 968-5954-16-X.*

Dicho ámbito de actuación tiene una existencia cierta en la realidad, a pesar de su tangibilidad e intangibilidad, por lo que a su vez encuentra espacio dentro de la esfera de los derechos de las personas, atendiendo a los efectos y alcances de los intereses que pudieran resultar afectados con motivo de su desenvolvimiento con terceros.

En ese orden de ideas, los datos personales constituyen la medida por la cual es posible identificar ese ámbito de actuación de las personas, ya que a través del tratamiento[122] del cual es objeto dicha información, es posible atribuir los efectos y alcances de existencia, e inclusive, conciencia de los individuos titulares de los datos.

Así, la protección de datos personales se coloca como el instrumento protector de los derechos inherentes a la personalidad de los individuos, así como a los efectos que estos pueden tener respecto a su existencia cierta en la realidad, con injerencia directa sobre los bienes jurídicos que tutela el derecho. Apunte que se estima necesario realizar, puesto que sin negar el carácter fundamental de este derecho, resulta importante destacar su carácter instrumental para la protección de derechos diversos, como punto medio de control para evitar afectaciones específicas a los mismos, es decir, en la mayoría de las ocasiones constituye un derecho llave para la protección de otros derechos.

Sin embargo, también cuenta con una dimensión sustantiva propia, la cual se asocia con el concepto de autodeterminación informativa, entendida como el poder de decisión y control de los titulares sobre la información de carácter personal[123], reflexión surgida con motivo de la sentencia de Sala del Tribunal Constitucional

---

[122] Resulta ilustrativo para el concepto de tratamiento, lo dispuesto por el Artículo 3o. fracción XXXIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, que establece lo siguiente: "Tratamiento: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales…".

[123] Que a su vez implica dos presupuestos importantes para su vigencia, como son los derechos de los titulares de la información para hacer efectivo el derecho, y por otra, la obligación del Estado de brindar mecanismos para la seguridad de la información (lo cual a su vez presupone vinculación con la ciberseguridad, es decir, los mecanismos previstos para la seguridad en entornos informáticos y el ciberespacio).

de la República Federal de Alemania, de fecha 15 de diciembre de 1983, en las audiencias públicas de 18 y 19 de octubre de dicho año, sobre la Ley del Censo de Población, Profesión y Lugares de Trabajo; sentencia que constituye el primer antecedente reconocido en la conceptualización de la autodeterminación informativa "porque destaca la importancia y el alcance de derecho a la autodeterminación de la información o autodeterminación informativa… y plantea los supuestos fácticos, jurídicos y administrativos que deben rodear el proceso de recolección y tratamiento de datos personales a través de los censos"[124].

Es así, que el derecho a la protección de datos personales se ha ido insertado en la consciencia, cultura colectiva y reconocimiento en las diversas legislaciones del mundo, cuyo detonante puede trazarse a través de teoría sociológica de la posmodernidad en la época contemporánea, la cual surge de manera aparejada, con la llamada *era digital*.

En principio, se identifica como primer antecedente el Artículo 12 de la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, que establece en su redacción de origen (por constituir el inglés idioma de trabajo en la fecha de su adopción, en el entendido que el español fue considerado como tal un día después[125]), es decir, la Declaración Universal de los Derechos Humanos fue definida sobre concepciones francesas, inglesas y estadounidenses, por lo que la versión en español, a pesar de constituir versión en idioma oficial, es susceptible de considerarse únicamente como traducción) lo siguiente: "No one shall be subjected to arbitrary interference with *his privacy*[126], family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks" (el énfasis es añadido).

Posteriormente, el desarrollo legislativo formal de la materia se dio en el ámbito del derecho europeo que constituye la principal referencia en la actualidad, a través de la Constitución portuguesa de 1976, al contar con la primer referencia a

---

[124] Remolina Angarita, Nelson, *Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012*, Bogotá, Legis, 2013, p. 28.

[125] Organización de Naciones Unidas, *http://ask.un.org/es/faq/13553.*

[126] Concepto construido con una fuerte influencia anglosajona, como se puede identificar en el contexto de este apartado.

la protección de datos personales en su Artículo 26.2 al establecer que "la ley establecerá garantías efectivas contra la utilización abusiva, o contraria a la dignidad humana de informaciones referentes a las personas y a las familias"[127], señalando en el diverso Artículo 35, disposiciones específicas para el acceso a datos, limitaciones sobre su uso y difusión, así como las prohibiciones para la asignación de un número nacional.

Las diversas aproximaciones constitucionales posteriores a este derecho por parte de los demás países europeos, fueron rápidamente consolidadas a través del Consejo de Europa y el Derecho de la Unión Europea, en su vertiente como derecho fundamental, a través del Convenio 108, de 28 de enero de 1981, y posteriormente, a través de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de la Unión Europea, de 24 de octubre de 1995, último instrumento que constituye el antecedente inmediato de lo que hoy es el Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos, también reconocido como Reglamento General de Protección de Datos (citado de manera extendida por sus siglas en inglés como GDPR).

A partir de estos sucesos, el derecho a la protección de datos personales fue extendiéndose a través de diversas legislaciones y Constituciones nacionales a lo largo del mundo, como una disciplina con objeto propio. Sobre el particular, resulta importante señalar que si bien es posible identificar en diversos países de familias jurídicas distintas[128], legislaciones sectoriales que se encuentran vinculadas con algún ámbito de protección de la información de carácter personal, la protección de datos personales se asocia principalmente al ámbito europeo, tomando como referencia su reconocimiento como derecho fundamental[129].

---

[127] Troncoso Reigada, Antonio, *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant Lo Blanch, 2010, p. 49.

[128] Lo cual algunos doctrinarios han asociado con la existencia de tres modelos de protección, a saber: el europeo, el estadounidense (sectorial) y el latinoamericano (habeas data).

[129] Por ello, si bien no se pierde de vista que las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales fueron adoptadas de manera previa como una recomendación del Consejo de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), el

Ahora, tomando el derecho europeo como referencia, se identifica que de manera formal el derecho a la protección de datos personales tiene dos dimensiones acotadas, como derecho fundamental (Convenio 108) y como Derecho común de la UE (debido tratamiento de los datos para las relaciones sociales y económicas entre sus miembros y terceros, en términos de lo previsto por el Reglamento General de Protección de Datos).

A su vez, ambas dimensiones cuentan con disposiciones específicas respecto a tratamientos realizados por el sector público y privado, lo cual es importante tener presente para determinar el alcance del derecho, dependiendo del supuesto en el cual resulte exigible su cumplimiento.

Ante tales circunstancias, el objeto de estudio de la protección de datos personales cuenta con diversas vertientes para su análisis, en los cuales destaca la novedad del derecho y también los enfoques para su protección, lo que inclusive al día de hoy, no permite realizar su clasificación específica dentro de alguna rama jurídica particular, tal como el Derecho Administrativo, el Derecho Sancionador o Disciplinario, Derecho de Acceso a la Información o inherente a la libertad de expresión, o, en el Derecho de las Nuevas Tecnologías, entre diversas ramas en las cuales pudiera estar inserto.

Aunado a ello, en la época actual la evolución de esta disciplina es tan dinámico que lo establecido en estas líneas es muy distinto de lo que se hubiera apuntado hace apenas seis meses. Circunstancia que se destaca ante la coyuntura actual a nivel nacional e internacional que limita de manera importante el desarrollo de este documento, destinado al análisis de la protección de datos personales en el sector público, puesto que en el caso internacional, Europa se encuentra en transición hacia la adopción del Reglamento General de Protección de Datos[130], proceso

---

23 de septiembre de 1980, también lo es que dicho documento no tiene el mismo alcance que el Convenio 108, en el que se insiste, se otorga carácter de derecho fundamental a la protección de datos personales.

[130] Que ha obligado a los países la adopción de la normativa, en el caso de España, a pesar de que se cuenta con un anteproyecto, todavía no se tiene registro de la aprobación de una nueva Ley Orgánica de Protección de Datos.

que acaba el mes de mayo del siguiente año, y en el caso de México, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se encuentra en implementación en el sector público, en términos de lo que establecen sus Artículos Transitorios.

II. APUNTES SOBRE LA PROTECCIÓN DE DATOS PERSONALES EN OTROS PAÍSES

Existe una gran variedad de información en Derecho Comparado en materia de protección de datos personales, en los cuales –como en el caso de México– se identifican políticas interesantes respecto a la materia, así como una serie de buenas prácticas en países que no necesariamente pertenecen a Europa.

Como se ha referido de manera implícita en este documento, la protección de datos personales no es, y nunca ha sido, un tema local o regional, sino que conlleva la cooperación y desarrollo de estándares y prácticas comunes por parte de las múltiples partes interesadas, atendiendo la diversidad de medios por los cuales la información de carácter personal puede ser sujeta a tratamiento; por ello, de manera adicional al interés que genera el estudio del Derecho Comparado en protección de datos personales, constituye una exigencia necesaria para que las políticas en la materia puedan adquirir eficacia, en concordancia al modelo globalizado e interconectado a través de Internet, que no deja aspectos afuera de su aplicación.

No obstante, de manera general se analizan tres ejemplos del ámbito europeo de protección de datos personales, a saber: Reino Unido, España y el Reglamento General de Protección de Datos.

El modelo de protección de datos personales de Reino Unido destaca como el más completo en lo que hace a la tutela del derecho, puesto que conlleva la protección administrativa de la información conforme a las leyes europeas de protección de datos personales, y a la vez, cuenta con mecanismos de protección de la privacidad a través de las decisiones judiciales en el Co*mmon Law*.

En el ámbito de protección de datos y acceso a la información, destacan el *Data Protection Act* del 16 de julio de 1998 y el *Freedom of Information Act* del 30 de noviembre del año 2000, que establecen disposiciones para la protección de la in-

formación conforme al ámbito europeo; leyes aplicables a través de una autoridad de control denominada Comisionado de Información (*Information Commissioner´s Office, ICO*), con atribuciones específicas para el control sobre la protección de datos personales. Sin embargo, la Ley de Protección de Datos Personales, también establece disposiciones relativas al Tribunal de Protección de Datos (*Data Protection Tribunal/ Information Tribunal/ First-tier Tribunal*).

Adicionalmente, la Corte de Reino Unido también cuenta con facultades sobre agravios en contra de la privacidad, en términos del derecho previsto por el Artículo 8o. de la *Human Rights Act* del 9 de noviembre de 1998.

Como se puede ver, contrario a lo que pudiera corresponder a Reino Unido conforme al sistema jurídico al que pertenece (*Common Law*), cuenta con un esquema de protección robusto, en congruencia con el modelo de protección de datos personales europeo.

En lo que atañe a España, este país ha destacado en protección de datos personales en el ámbito europeo, desarrollo que a su vez se ha traducido en una de las mayores decisiones judiciales en materia de protección de datos personales en el contexto europeo, como lo es la sentencia del 13 de mayo de 2014 del Tribunal de Justicia de la UE, que dio origen al debate respecto al *"derecho al olvido"*.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, constituye el principal instrumento legal que rige esta materia, desarrollándose a través del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999.

En el caso español, cuenta con una autoridad de control especializada en protección de datos personales denominada Agencia Española de Protección de Datos, competente tanto en asuntos del sector público como el privado.

La legislación y el reglamento español, destacan a nivel internacional por contar con los mecanismos administrativos de control completos conforme a la normativa europea, en desarrollo a la vez de las obligaciones previstas por la Directiva 95/46/CE, que en la misma inteligencia, actualmente se encuentran en revisión para su adecuación con el Reglamento General.

Es así, que en esta legislación se pueden identificar supuestos de tratamiento diferenciados para el sector público y el privado, como en el caso del consentimiento, datos de seguridad pública, transmisiones, conservación, régimen de responsabilidad e indemnización, ficheros de titularidad pública, excepciones para el acceso, rectificación o cancelación, obtención de datos, que establecen disposiciones diferenciadas para las Administraciones Públicas.

Asimismo, resulta importante apuntar que actualmente la Agencia Española de Protección de Datos, es de las principales autoridades impulsoras de este derecho no solo en el ámbito local, sino en el internacional, a través de diversos mecanismos de difusión y cooperación con otros países, destacando iniciativas como los Premios Internacionales en Protección de Datos y las actividades en la Red Iberoamericana de Protección de Datos, organización en la que detenta la Secretaría Permanente. Así mismo, al igual que la autoridad de Reino Unido, la Agencia Española de Protección de Datos es miembro de la Conferencia Internacional de Comisionados de Protección de Datos y Privacidad, que surge desde el año 1979.

Finalmente, como se mencionó previamente, el Reglamento General de Protección de Datos, aprobado el 27 de abril de 2016, sustituye a la Directiva 95/46/CE, a través de un proceso de transición de dos años que culmina el 24 de mayo de 2018, modernizando el esquema de protección de datos personales de la UE.

Las disposiciones del Reglamento Europeo de Protección de Datos constituyen al día de hoy, el desarrollo normativo de referencia más importante en la materia, actualizando los supuestos de aplicación a la realidad tecnológica e incorporando nuevos derechos, como lo son la portabilidad y el derecho al olvido.

III. EL ÁMBITO DE ACTUACIÓN DEL SECTOR PÚBLICO EN NUESTRO PAÍS Y LA PROTECCIÓN DE DATOS PERSONALES

Los mecanismos de operación por parte de las entidades del sector público poseen características propias que les facilita un esquema de control y límite de sus atribuciones y funciones.

En principio, por su propia naturaleza, el sector público se encuentra sujeto a la aplicación estricta de legalidad como espacio limítrofe de su actuación, es decir, que las autoridades deben acotar su esfera de influencia a lo que estrictamente le corresponde en términos de la legislación que les da origen y finalidad, que por ende, circunscriben su injerencia en la vida de las personas a los presupuestos rigurosamente establecidos en el marco jurídico aplicable.

El cumplimiento del principio de legalidad constituye un cálculo necesario para la consecución de la seguridad jurídica, la justicia y el bien común, con los fines del Estado, al dotar a su estructura orgánica de funciones específicas acotadas al poder delegado por la población.

De manera adicional, el régimen de derechos fundamentales vigente, como en el caso de nuestro país, la reforma constitucional en derechos humanos del 10 de junio de 2011, ha modificado el paradigma en torno al actuar por parte de los entes públicos de los Estados contemporáneos.

A manera de guisa, el Artículo 1o., tercer párrafo, de la Constitución Política de los Estados Unidos Mexicanos establece que todas las autoridades, en el ámbito de su competencia, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad.

En consecuencia, la actuación de las autoridades en nuestro país no solamente se encuentra sujeta al cumplimiento del principio de legalidad, sino que adquiere un enfoque multidimensional en materia de derechos humanos, como una exigencia implícita en cada acto y procedimiento, que inclusive puede resultar reclamable a través del control difuso "*ex officio*" o inclusive convencional, que a su vez debe integrar la aplicación de diversos principios interpretativos, entre los cuales se señala el "*pro persona*".

En este primer acercamiento, es posible identificar que la protección de datos personales en el sector público, cuenta con un esquema predefinido de actuación que provoca como consecuencia una protección de datos personales por defecto, a pesar que eventualmente la protección de datos personales, no se encuentre re-

conocido expresamente en los textos constitucionales, las autoridades estarán implementando mecanismos indirectos de protección, atendiendo a la exigencias que rigen un Estado de Derecho[131].

A fin de ejemplificar lo anterior, tomando como referencia el ámbito federal del gobierno mexicano[132], se observa la existencia de diversos sistemas y mecanismos de control, que a través de su implementación deben ser articulados dentro del esquema de rendición de cuentas del Estado mexicano, tal como se observa de lo dispuesto por el último párrafo del apartado A del Artículo 6o. de la Constitución Federal, que establece: "A… El organismo garante coordinará sus acciones con la Auditoría Superior de la Federación, con la entidad especializada en materia de archivos y con el organismo encargado de regular la captación, procesamiento y publicación de la información estadística y geográfica, así como con los organismos garantes de las entidades federativas, con el objeto de fortalecer la rendición de cuentas del Estado Mexicano".

A su vez, los Artículos 108 y 134, párrafos primero y séptimo, de nuestra Carta de Derechos Fundamentales establecen:

> Artículo 108. Para los efectos de las responsabilidades a que alude este Título se reputarán como servidores públicos a los representantes de elección popular, a los miembros del Poder Judicial de la Federación, los funcionarios y empleados y, en general, a toda persona que desempeñe un empleo, cargo o comisión de cualquier naturaleza en el Congreso de la Unión o en la Administración Pública Federal, así como a los servidores públicos de los organismos a los que esta Constitución otorgue autonomía, quienes serán responsables por los actos u omisiones en que incurran en el desempeño de sus respectivas funciones.
>
> El Presidente de la República, durante el tiempo de su encargo, solo podrá ser acusado por traición a la patria y delitos graves del orden común.
>
> Los ejecutivos de las entidades federativas, los diputados a las Legislaturas

[131] Que deónticamente de manera posterior.

[132] Sin perjuicio de diversas disposiciones que tienen el carácter general, y por ende, pudieran analizarse en un contexto nacional.

Locales, los Magistrados de los Tribunales Superiores de Justicia Locales, en su caso, los miembros de los Consejos de las Judicaturas Locales, los integrantes de los Ayuntamientos y Alcaldías, los miembros de los organismos a los que las Constituciones Locales les otorgue autonomía, así como los demás servidores públicos locales, serán responsables por violaciones a esta Constitución y a las leyes federales, así como por el manejo y aplicación indebidos de fondos y recursos federales.

Las Constituciones de las entidades federativas precisarán, en los mismos términos del primer párrafo de este artículo y para los efectos de sus responsabilidades, el carácter de servidores públicos de quienes desempeñen empleo, cargo o comisión en las entidades federativas, los Municipios y las demarcaciones territoriales de la Ciudad de México. Dichos servidores públicos serán responsables por el manejo indebido de recursos públicos y la deuda pública.

Los servidores públicos a que se refiere el presente artículo estarán obligados a presentar, bajo protesta de decir verdad, su declaración patrimonial y de intereses ante las autoridades competentes y en los términos que determine la ley.

Artículo 134. Los recursos económicos de que dispongan la Federación, las entidades federativas, los Municipios y las demarcaciones territoriales de la Ciudad de México, se administrarán con eficiencia, eficacia, economía, transparencia y honradez para satisfacer los objetivos a los que estén destinados.

…

Los servidores públicos de la Federación, las entidades federativas, los Municipios y las demarcaciones territoriales de la Ciudad de México, tienen en todo tiempo la obligación de aplicar con imparcialidad los recursos públicos que están bajo su responsabilidad, sin influir en la equidad de la competencia entre los partidos políticos.

Derivado de lo anterior, se observa que el régimen de rendición de cuentas y de responsabilidades de los servidores públicos, cuenta con diversos presupuestos para su aplicación, para lo cual se realizará un señalamiento de la legislación federal más relevante, que establece mecanismos de control que favorecen la protección de datos personales, a pesar de no estar dentro de su ámbito material especial de aplicación.

Es así, que la Ley General de Contabilidad Gubernamental y la Ley Federal de Presupuesto y Responsabilidad Hacendaria, establecen requisitos adicionales a los previstos en los presupuestos de egresos anuales, con la finalidad de que el registro de las operaciones contables, así como el ejercicio y comprobación de los recursos económicos del Estado, se administren con eficiencia, eficacia, economía, transparencia y honradez para satisfacer los objetivos a los que estén destinados.

Sobre el particular, el esquema de rendición de cuentas del Estado mexicano no se traduce únicamente a obligaciones cuantitativas con relación a la erogación de los recursos, sino que se ha transitado hacia un modelo cualitativo: el presupuesto basado en resultados, en el cual no importa solamente la cantidad de presupuesto ejercido, sino los resultados obtenidos con motivo de cada peso invertido y si dicha inversión tiene valor social, es decir, que los resultados obtenidos son eficaces para abatir la problemática social identificada.

La dinámica presupuestal exige actividades de programación, planeación, aprobación, ejercicio, control, evaluación de los ingresos y egresos públicos federales, que a su vez se deriva del análisis de información que conlleva tratamiento de datos personales, puesto que inclusive pueden tener injerencia con la evaluación de la gestión y el desempeño. Dicha legislación establece obligaciones de generar documentos y registros, así como de llevar a cabo el resguardo de la información por determinado tiempo, implicando con ello una gestión de la información con mecanismos de control específicos, que significa al uso de diversas medidas de seguridad tales como las físicas, lógicas de desarrollo, aplicaciones y que inclusive pudiera abarcar las de comunicaciones y redes, si se toma en consideración si vinculación con los procedimientos de contratación pública.

En el ámbito de legalidad, encontramos la Ley Federal de Procedimiento Administrativo y la Ley Federal de Procedimiento Contencioso Administrativo, que establecen de manera genérica los requisitos esenciales que deben cumplirse en los procedimientos y procesos federales, que al implicar tratamiento de datos personales, establece la obligación de los servidores públicos de seguir ciertas formalidades en los procedimientos en que intervengan, a fin de que su actuación sea

válida. Este tipo de actividades válidamente pueden asociarse con medidas de seguridad de tipo lógico en materia de protección de datos personales.

La Ley Federal de Telecomunicaciones y Radiodifusión, la Ley Federal del Derecho de Autor y la Ley de Propiedad Industrial, se destacan a pesar de no tener un aplicación directa de control en el servicio público, sin embargo, contienen elementos vinculados a la implementación de medidas de seguridad en comunicaciones y redes, así como relativas a cifrado.

La Ley de Firma Electrónica Avanzada, establece el esquema general aplicable para la identificación y autenticación en el uso de medios electrónicos, así como los presupuestos para el no repudio.

A través de la Ley Federal para prevenir y eliminar la Discriminación, Ley General de los Derechos de Niñas, Niños y Adolescentes, se establecen disposiciones sectoriales inherentes a datos que deben ser especialmente protegidos, atendiendo a supuestos de hecho diferenciados.

En otra vertiente, podemos localizar a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y la Ley Federal de Archivos, legislación que no solamente establece la gestión y preservación y publicidad de los datos personales, sino las medidas de seguridad relativas a la gestión documental, y a través de ellas, las relativas a los soportes de la información, incluyendo a los datos personales.

Por último, finalizan la muestra de referencia la Ley General del Sistema Nacional Anticorrupción, Ley General de Responsabilidades Administrativas, Ley Federal de Responsabilidad Patrimonial del Estado, Ley de Fiscalización y Rendición de Cuentas de la Federación, como instrumentos para el control, revisión y sanción del actuar gubernamental.

Como se ha podido observar, aunque sea de manera mínima, el régimen de actuación de los servidores públicos involucra no solamente el cumplimiento del principio de legalidad y un enfoque en materia de derechos humanos, sino que se encuentra acotado a disposiciones jurídicas sectoriales que le exigen responsabilidades específicas en el manejo de la información, que a su vez implícitamente presuponen un nivel mínimo de protección de datos personales.

Ahora, por lo que hace a la segunda aproximación, esta constituye el esquema formal de protección de datos en nuestro país.

En México, la protección de datos personales constituye un derecho humano en términos de lo que establecen los Artículos 6o., apartado A, fracción II y 16 segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, que también reconoce de manera implícita el derecho a la privacidad (privacía de las comunicaciones, Artículo 16, párrafo doceavo), vida privada (Artículo 6o. primer párrafo y apartado A, fracción II) e intimidad (libertad de convicciones éticas, de conciencia y religiosas, Artículo 24, primer párrafo).

No obstante, conforme a nuestro régimen jurídico podemos encontrar dos ámbitos de aplicación: el tratamiento a cargo de particulares, y el relativo a entes públicos (sobre el cual se hará un mayor análisis).

La protección de datos personales por parte del sector privado constituye una materia federal, cuya base constitucional se encuentra en los Artículos 16 segundo párrafo, 73 fracción XXIX-O y 124 de la Constitución Política de los Estados Unidos Mexicanos; tratamiento para el cual resulta aplicable la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada el Diario Oficial de la Federación el 5 de julio de 2010, con excepción de lo relativo a los denominados "burós de crédito", que cuentan con una legislación sectorial, la Ley para Regular las Sociedades de Información Crediticia, publicada en el Diario Oficial de la Federación el 15 de enero del año 2002.

En el caso de entes públicos, la protección de datos personales tiene sustento en los Artículos 6o., apartado A, fracción II y 16 segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos, con dos niveles de aplicación a pesar de su carácter nacional[133], a saber: el ámbito federal (que en supuestos específicos adquiere el carácter de nacional) y el ámbito local, que integra al nivel de gobierno estatal y a los municipales de su territorio.

---

[133] Que implica el establecimiento de mecanismos de control a través de una autoridad centralizada para los tres niveles de gobierno.

En el ámbito federal, el primer referente legislativo es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental publicada en el Diario Oficial de la Federación el 11 de junio de 2002, en la cual se incluye la protección de datos personales como una limitante del derecho de acceso.

En esa tesitura, la primera reforma constitucional en la que se incorpora la protección de datos personales[134], se publicó en el Diario Oficial de la Federación el día 20 de julio del año 2007, adicionando un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Federal[135], mismo que en su fracción II incluye la protección de los datos personales como una limitante del derecho de acceso[136], por lo que es común identificar que ante dicha reforma el derecho a la protección de datos personales fue asociado de manera accesoria al derecho de acceso a la información.

Posteriormente, el 1 de junio del año 2009, se publica en el Diario Oficial de la Federación la reforma al Artículo 16 de la Constitución, adicionando un segundo párrafo en el cual se reconoce el derecho a la protección de datos personales, tal como se identifica enseguida:

> … 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.

---

[134] Si bien la protección de la privacidad y vida privada puede trazarse a una fecha anterior, no será materia del análisis de referencia por no corresponder al enfoque del marco conceptual del proyecto de investigación.

[135] Párrafo que de manera posterior se convirtió en un apartado A con la reforma en materia de Telecomunicaciones del 11 de junio de 2013.

[136] Redacción de la reforma original: Artículo 6o… 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…
II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
III. al VII...

Fundamento que constituye al día de hoy, el sustento por el que la protección de datos personales representa una materia propia, independiente y específica dentro del sistema jurídico mexicano.

Es así que con la publicación el 26 de enero de 2017, en el Diario Oficial de la Federación, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[137], se generó una nueva época en la protección de datos personales en el sector público, ya que hasta antes de esta fecha, no existió disposición legislativa específica en torno a dicho derecho en el ámbito federal, sino que su desarrollo se dio principalmente en las entidades federativas.

No obstante lo anterior, el entonces Instituto Federal de Acceso a la Información y Protección de Datos, hoy Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, generó normatividad a fin de desarrollar las disposiciones en la materia, existentes en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, entre las cuales se identifican las siguientes:

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección (publicación Diario Oficial de la Federación el 12 de junio de 2003, reforma Diario Oficial de la Federación el 2 diciembre 2008).

[137] Ley General que surge con motivo de la última reforma constitucional y estructural en materia de transparencia, publicada en el Diario Oficial de la Federación el 7 de febrero de 2014. Se sostiene lo anterior, puesto que el Artículo Tercero Transitorio de la Ley General de Transparencia y Acceso a la Información Pública (Ley General emitida por mandato constitucional), estableció lo siguiente: "En tanto no se expida la Ley General de Datos Personales en Posesión de Sujetos Obligados, permanecerá vigente la normatividad federal y local en la materia, en sus respectivos ámbitos de aplicación".

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales (publicación Diario Oficial de la Federación el 20 de agosto de 2003, sin efectos por el Artículo Sexto Transitorio de los Lineamientos de Protección de Datos Personales).
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos (publicación en el Diario Oficial de la Federación 25 agosto de 2003, reforma Diario Oficial de la Federación el 2 de diciembre 2008).
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares (publicación Diario Oficial de la Federación el 6 de abril de 2004, reforma Diario Oficial de la Federación el 2 de diciembre de 2008).
- Lineamientos de Protección de Datos Personales (publicación Diario Oficial de la Federación el 30 de septiembre de 2005, reforma Diario Oficial de la Federación el 17 de julio de 2006).
- Lineamientos para la entrega de la información y los datos que los sujetos obligados contemplados en el inciso a), fracción XIV del Artículo 3o. de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental generarán para la elaboración del informe anual que el Instituto Federal de Acceso a la Información Pública presenta ante el H. Congreso de la Unión (publicación Diario Oficial de la Federación el 27 de enero 2006).
- Acuerdo por el que se modifica el Cuadragésimo de los Lineamientos de Protección de Datos Personales (publicación Diario Oficial de la Federación el 17 de julio de 2006).

- Modificaciones a los Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección; Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos, y Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares (publicación Diario Oficial de la Federación el 2 de diciembre de 2008).
- Lineamientos del Aviso de Privacidad (Diario Oficial de la Federación el 17 de enero de 2013).

Asimismo, en la fecha de publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[138], solamente 11 entidades federativas contaban con una Ley específica en materia de protección de datos personales, a saber: Campeche, Chihuahua, Colima, Distrito Federal (hoy Ciudad de México), Durango, Estado de México, Guanajuato, Oaxaca, Puebla, Tlaxcala y Veracruz.

Sin embargo, contrario a lo que pudiera suponer este hecho, las demás entidades federativas en mayor o menor medida contaban con disposiciones en sus leyes locales de transparencia que regulaban la protección de datos personales, en el mismo esquema que en el ámbito federal, complementando a través de reglamentos o lineamientos, y solamente en un caso, no se identificó legislación, ni normatividad en materia de protección de datos personales.

---

[138] Diario Oficial de la Federación el 26 de enero de 2017.

No obstante, así como la legislación de los Estados de México, Tlaxcala y Ciudad de México destacan por haber desarrollado normatividad complementaria en protección de datos personales, también se identifica que no existe homogeneidad en los mecanismos implementados en las entidades federativas para su protección hasta la entrada en vigor de la Ley General, puesto que en algunos casos inclusive se hace referencia al habeas data como instrumento para la protección de los datos personales.

IV. EL ESQUEMA DE PROTECCIÓN DE DATOS PERSONALES VIGENTE EN EL SECTOR PÚBLICO EN MÉXICO: IMPLEMENTACIÓN DE LA LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

El 26 de enero de 2017 se publicó en el Diario Oficial de la Federación, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, como resultado de un proceso similar al de la Ley General de Transparencia y Acceso a la Información Pública, en el que se realizaron foros de consulta a académicos, organismos garantes y sociedad civil, a fin de integrar un dictamen con los diversos puntos de vista de los actores involucrados[139].

De conformidad con lo establecido por el Artículo 1o. de esta Ley, 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 sujetos obligados.

El concepto sujetos obligados tiene una connotación particular, puesto que si bien esta Ley se encuentra destinada principalmente al sector público, no todos los

[139] Lo cual puede identificarse en el Dictamen de la Ley, en su proceso tanto en el Senado de la República como en la Cámara de Diputados del Congreso de la Unión, proceso en el cual la autora Josefina Román Vergara tuvo la oportunidad de intervenir junto con integrantes del Pleno del INFOEM, el Comisionado Coordinador de la Comisión de Protección de Datos Personales y Comisionados de entidades federativas del Sistema Nacional de Transparencia, en su carácter de Comisionada Presidenta y Coordinadora de Organismos Garantes de las Entidades Federativas del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

sujetos a los que les resulta aplicable su contenido son entes públicos, es así, que el propio Artículo, establece las reglas aplicables para determinar quiénes serán sujetos obligados de dicha Ley, tal como se puede observar a continuación:

> Artículo 1o…
>
> …
>
> Son sujetos obligados por esta Ley, 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.
>
> 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.
>
> En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Disposición con la cual se delimita el ámbito personal de aplicación de esta Ley, que difiere con los sujetos obligados previstos por la Ley General de Transparencia y Acceso a la Información Pública, que si bien resulta orientadora, genera algunos inconvenientes prácticos para su aplicación por parte de quienes no constituyen sujetos obligados y, por ende, se rigen por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, como en el caso de los sindicatos y el tratamiento de afiliación sindical como dato personal sensible[140], que a su vez, constituye una obligación de transparencia en términos del Artículo 79, párrafo primero, fracción III, de la Ley General de Transparencia antes citada.

---

[140] Ver Artículo 3o., fracción VI, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares que establece: Para los efectos de esta Ley, se entenderá por: … VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, *afiliación sindical*, opiniones políticas, preferencia sexual.

De igual forma, de conformidad con los Artículos Transitorios, se cuentan con distintos plazos para su implementación, como se refiere a continuación:

- Su entrada en vigor a partir del día siguiente de su publicación en el Diario Oficial de la Federación, es decir, a partir del 27 de enero de 2017.
- Seis meses para la armonización de disposiciones federales (término: 26 de julio de 2017), con la prevención que en caso de omisión la Ley General tendrá aplicación directa en términos del Artículo Segundo Transitorio.

  En este supuesto particular, resulta importante señalar que al 25 de agosto de 2017, 28 entidades federativas han armonizado su legislación local, 22 en tiempo, y 6 con posterioridad al 27 de julio de 2017, fecha en la cual cobró aplicación directa la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. El día en que se entrega esta colaboración, únicamente Ciudad de México, Nuevo León, Michoacán y Nayarit, faltan por aprobar su legislación en la materia. En el caso federal, la Ley General tiene aplicación directa.
- La exigencia de previsión presupuestal para su aplicación por parte de la Cámara de Diputados del Congreso de la Unión y de las Legislaturas de las Entidades Federativas, a partir del ejercicio 2018, conforme al Artículo Tercero Transitorio.
- La emisión de los Lineamientos Generales a que hace referencia la Ley General y su publicación en el Diario Oficial de la Federación y Gacetas o Periódicos Oficiales Locales, a más tardar el 26 de enero de 2018, señalada en términos del Artículo Quinto Transitorio.
- Emisión del Programa Nacional de Protección de Datos Personales a más tardar el 26 de enero de 2018.
- Tramitación, expedición o modificación de la normatividad interna de los sujetos obligados a más tardar dentro de los dieciocho meses siguientes a la entrada en vigor de esta Ley en términos del Artículo Séptimo Transitorio, es decir, a más tardar el 26 de julio de 2018, normatividad en la que se puede incluir la elaboración de documentos de seguridad y de los

documentos vinculados al mismo, tales como plan de trabajo, análisis de riesgo y brecha, bitácoras de incidentes e inventarios de bases de datos.

- Inclusión del principio de progresividad en el Artículo Octavo Transitorio, con el objeto de que las entidades federativas no disminuyeran o ampliaran plazos y procedimientos en perjuicio de los titulares de los datos.

El día de hoy, se identifica un panorama en la protección de datos personales en el sector público distinto al que se encontraba en el día de la publicación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, puesto que la legislación de las entidades federativas, de manera uniforme, se ajustan a las disposiciones de la Ley General.

De manera particular, se identifica que en las leyes de protección de datos personales en posesión de sujetos obligados publicadas al día de elaboración de este trabajo y a las cuales se tuvo acceso, cuatro entidades federativas prevén en sus leyes tipos y niveles de seguridad (Estado de México, Morelos, Veracruz y Zacatecas); tres prevén un enfoque basado en procesos a través del concepto de sistemas de datos personales (Estado de México, Morelos y Veracruz) y únicamente el Estado de México, incluye el concepto de administrador, como el servidor público al que en principio le resultan exigibles las obligaciones establecidas por la Ley a cargo del responsable (sujeto obligado), con lo cual se individualizan responsabilidades, así como algunos ajustes específicos que lo distinguen de lo que establece la Ley General.

Sin embargo, de manera previa al análisis de los supuestos establecidos en el párrafo que precede, se considera pertinente llevar a cabo un breve estudio del esquema de protección de datos personales en el sector público, a partir de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En principio, resulta importante enfatizar que esta Ley General, sin duda, constituye un instrumento jurídico de avanzada en la materia acorde con los últimos estándares internacionales, cuenta con un enfoque preventivo para la protección y destaca la flexibilidad en su implementación, incorpora características propias, y a su vez, incluye los temas que se encuentran presentes en la agenda

global para las autoridades de control, entre ellas, la línea marcada en el ámbito de protección con la inminente transición hacia la adopción plena del Reglamento General (Europeo) de Protección de Datos.

En este momento, resulta necesario realizar una pauta para la primera reflexión, ¿existen metodologías para la protección de datos personales? y ¿en caso de que la respuesta sea afirmativa, en qué se diferencian de las técnicas o normas técnicas en materia de seguridad de la información?

A través del presente documento no se pretende dar respuesta a estas interrogantes, puesto que desde este momento se anticipa que en la primera pregunta seguramente existirán sendas contestaciones con sentidos contrarios, y a la vez, con validez fáctica de ambas en su aseveración. Esto es así, puesto que como se atisbó previamente, la protección de datos personales conlleva el cumplimiento de una serie de pasos, requisitos, procedimientos y métodos para su implementación, lo cual se encuentra recogido en las diversas leyes nacionales e internacionales, atendiendo que esta materia también encuentra significado en su contenido y alcance, es decir, en una tutela efectiva de la autodeterminación informativa de las personas.

Conforme a la *Ley de Hume*, este presupuesto en inicio resulta falaz, ante la imposibilidad lógica de inferir el ser a partir del deber ser, es decir, que a partir de la emisión de una legislación se puedan obtener los resultados esperados conforme al fenómeno que se analiza, que es la efectiva protección de datos personales.

Si bien, las diversas leyes de protección de datos personales en el mundo establecen diversos presupuestos para dar contenido y alcance a la protección de datos personales, estas son carentes de método, puesto que se limitan a establecer una serie de medidas que constituyen evidencia de un estado de protección.

Por otra parte, existe una diversidad de normas vinculadas con la seguridad de la información, que a su vez, constituyen las técnicas sobre las cuales subyacen las medidas de seguridad en materia de protección de datos personales, estos últimos, como una especie de dentro del género información.

Bajo este contexto, no se identifican metodologías específicas para la protección de datos personales, y si bien, se observa que existen diversas normas técnicas que pueden facilitar la gestión de la seguridad, estas no pueden ser implementadas

de manera generalizada, puesto que el contexto y la finalidad del tratamiento, requieren no solamente su adaptación, sino inclusive la elección de una herramienta específica al contexto del tratamiento, que no siempre puede tener la misma aplicación en un caso concreto.

A pesar de los inconvenientes que traen en su aplicación las interrogantes iniciales, se considera que el enfoque que establece la Ley General, en su Artículo 34, es integradora y logra establecer una aproximación cercana, al establecer lo siguiente:

> Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un *sistema de gestión*.
>
> Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.

Elemento que constituye un presupuesto medular para la protección de datos personales conforme a una exigencia técnica, y a su vez, es susceptible de constituir una metodología de protección y producir efectos jurídicos, ante el establecimiento de obligaciones, responsabilidades y autoridades específicas en torno a la protección de datos personales.

Esto es, que la protección de datos personales no puede ser garantizada en ningún caso, dados los factores endógenos y exógenos en torno a la misma, sino que únicamente pueden gestionarse los elementos inherentes al tratamiento para controlar los riesgos.

En ese entendido, el contenido técnico relativo a la protección de los datos personales se asocia con la seguridad de la información, objeto sobre el cual se implementa un sistema de gestión. A manera de referencia se observa que el numeral 2.33 de la Norma ISO/IEC 27000:2014, en su versión en inglés, conceptualiza a la seguridad de la información como la "preservación de confidencialidad, integridad y disponibilidad de la información" *(2.33, information security, preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information. Note 1 to entry:*

In addition, other properties, such as authenticity (2.8), accountability, non-repudiation (2.54), and reliability (2.62) can also be involved), concepto que en una nota seguida señala que de manera adicional, otras propiedades o atributos, tales como la autenticidad, responsabilidad proactiva, no repudio y confiabilidad pueden estar involucrados.

Es así, que haciendo un símil conforme a lo que establece la Ley General, a través de la preservación de la confidencialidad, integridad y disponibilidad, de los datos personales, se estarán implementando las medidas de seguridad inherentes a los riesgos relacionados con los mismos tales como el uso y transmisión no autorizados (confidencialidad), deterioro o alteración (integridad) y pérdida o destrucción (disponibilidad), con lo cual se estará brindando un parámetro razonable para la seguridad de los datos personales.

Un sistema de gestión se asocia con cuatro etapas denominadas como Círculo de Deming, consistentes en planear, hacer, verificar y actuar, conforme a las cuales se gestiona un objeto específico (en este caso, la seguridad de la información), con el objeto de alcanzar los resultados esperados, y a su vez, promover la mejora continua en la organización.

Sin embargo, aquí entramos se presenta un segundo análisis, ¿un sistema de gestión de protección de datos personales o un sistema de gestión de seguridad de la información?, interrogante para la cual tampoco hay una respuesta específica, puesto que el Artículo 34 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, tampoco exige un sistema de gestión de seguridad de la información como tal[141], sino que permite inclusive la implementación de sistemas de gestión compatibles con el tratamiento que se lleve a cabo, tales como gestión de riesgos o continuidad de negocios, sistemas de gestión que pudieran resultar compatibles en aquellos tratamientos de datos personales que utilicen mayormente información pública, en donde los riesgos inherentes a la vulnera-

[141] A pesar que pudiera encontrar implícito en términos de lo dispuesto por el Artículo 12, primer párrafo, fracción IV de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

ción de la confidencialidad cuenten con una probabilidad e impacto mínimos de ocurrencia.

Aunado a ello, deberá definirse el sistema de gestión a utilizar, puesto que contrario a lo que pudiera parecer, la implementación de un sistema de gestión cuenta con diversas opciones de normas técnicas, sin embargo, no todas cuentan con un alcance total para las operaciones del ente, o no resultan accesibles o se ajustan a la cultura y/o requerimientos institucionales.

Se considera que estas interrogantes, si bien no quedarán resueltas con el paso del tiempo, sí contarán con mayores elementos de guía para los sujetos obligados ante la emisión de los lineamientos generales que establece la Ley y con la emisión del Programa Nacional de Protección de Datos, que en uno de sus ejes, debe desarrollar los elementos relativos a un sistema de gestión de seguridad, conforme lo establece el Artículo 12, primer párrafo, fracción IV de la Ley General.

En ese entendido, considerando los plazos de implementación de la Ley General, se identifican dos momentos, el plazo de un año para la emisión de lineamientos generales, del impulso y mantenimiento relativo a un sistema de gestión de seguridad, y un plazo restante de seis meses para la adecuación de la normatividad interna, resultando importante precisar que los sujetos obligados no cuentan con ningún impedimento para comenzar actividades relativas a la implementación del sistema de gestión, puesto que la Ley General, establece los requisitos inherentes al documento de seguridad, que constituye el principal documento y registro por el cual se lleva a cabo la planificación, operación, evaluación y mejora del sistema de gestión.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, sin duda, presenta elementos importantes a destacar, que por extensión del presente trabajo y dada la coyuntura en la implementación de la Ley, solamente serán referidos, con la confianza de que serán temas sujetos a un análisis y desarrollo posterior por la doctrina y los sujetos obligados, ante las exigencias derivadas de su vigencia. En consecuencia, se considera importante puntualizar como aspectos destacados de la Ley General, los siguientes:

- Establece una serie de definiciones, que facilitan la comprensión de la Ley;
- Se definen las fuentes de acceso público y se establecen los supuestos que actualizan dicha hipótesis;
- Se reconoce el derecho a la protección de la privacidad;
- Prohibición para tratamiento de datos personales sensibles e inclusión del interés superior de la niña, niño y adolescente para menores de edad;
- Inclusión de la interpretación conforme y principio *pro persona*;
- Determina la legislación de aplicación supletoria;
- Establece vinculación con el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales;
- Crea el Programa Nacional de Protección de Datos Personales, como un instrumento rector para la integración y coordinación del Sistema Nacional, el cual debe determinar y jerarquizar los objetivos y metas que este debe cumplir, así como definir las líneas de acción generales que resulten necesarias;
- Establece los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales;
- De manera especial, en lo que hace al principio de información, establece la obligación de contar con aviso de privacidad y hacerlo del conocimiento del titular de los datos de manera previa, así como los requisitos que deben cumplirse para tal efecto;
- Se incorpora la protección de datos personales por defecto, como parte del cumplimiento del principio de responsabilidad;
- Se integra el deber de seguridad en el Artículo 31, puesto que establece el objeto de la protección a través de lo siguiente: "Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, *el responsable deberá establecer y mantener las medidas de seguridad* de carácter administrativo, físico y técnico para

la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, *así como garantizar su confidencialidad, integridad y disponibilidad"* (énfasis añadido);

- Se establece que exigencia de que el nivel de protección sea adecuado a las condiciones del tratamiento;
- Establece la obligatoriedad de un documento de seguridad, análisis de riesgos, análisis de brecha, plan de trabajo y programas de capacitación;
- Dispone mecanismos de respuesta ante vulneraciones de seguridad, obligando a los responsables a notificar al titular cuando se afecten de forma significativa los derechos patrimoniales o morales;
- Establece los derechos de Acceso, Rectificación, Cancelación y Oposición de Datos Personales, la Portabilidad, así como los procedimientos y mecanismos para su ejercicio;
- Establece la relación entre responsable y encargado, así como requerimientos especiales cuando el encargado brinde servicios de cómputo en nube, ya sea en infraestructura, aplicaciones o servicios;
- Se establecen reglas para transferencias y remisiones;
- Se incorporan acciones preventivas, entre las cuales encontramos el registro de mejores prácticas y las evaluaciones de impacto en la protección de datos;
- Se establece un capitulado específico para bases de datos de instancias de seguridad, procuración y administración de justicia;
- Se definen responsabilidades del Comité de Transparencia, así como del Instituto Nacional y organismos garantes;
- Se incorpora la figura del Oficial de Protección de Datos Personales;
- Entre los procedimientos de impugnación, se establecen reglas comunes y también supuestos específicos para el los recursos de revisión, inconformidad, y de revisión en materia de seguridad nacional, así como lo relativo a la facultad de atracción;

- Se incorpora el articulado relativo a los Criterios de Interpretación;
- Se establecen facultades de investigación y verificación, así como auditorías voluntarias. Resulta importante señalar en este punto que se dota de atribuciones a los organismos garantes para la imposición de medidas cautelares en el procedimiento de verificación, atribución que al día de hoy es objeto de polémica entre las autoridades de protección de datos;
- Finalmente, se incorporan las medidas de apremio y sanciones acordes con el régimen general de responsabilidades vigente.

A través de lo anterior, sobra decir que cada una de las figuras mencionadas da lugar a un análisis particular, pero que a través de su inclusión, otorga una dimensión robusta a la protección de datos personales en el sector público, que deberá ajustarse a los procedimientos y mecanismos que rigen conforme a las leyes aplicables en cada acto.

Sin embargo, con el objeto de finalizar esta contribución, resulta importante señalar que la labor realizada por parte de las entidades federativas, también da lugar a supuestos de reflexión en torno a la actualidad y proyección de la protección de datos personales en posesión de entes públicos.

Para tal efecto, se analizarán los elementos identificados destacados en las leyes de protección de datos personales de los Estados de México, Morelos, Veracruz y Zacatecas relacionados con los tipos y niveles de seguridad, así como el concepto relativo al enfoque basado en procesos a través de sistemas de datos personales, y finalmente, la inclusión de la figura de administrador.

Sobre el particular, si bien se ha destacado el acierto que constituye la exigencia de un sistema de gestión, también lo es que por sus propias características, este sistema de gestión debe quedar definido claramente, a fin de que los sujetos obligados cuenten con un marco de actuación establecido de manera concreta.

Es así que, el sistema de gestión debe contar con objetivos de control definidos, que a su vez, le permitan generar evidencia del cumplimiento de presupuestos para la gestión de la seguridad, sin embargo, estos difícilmente podrán establecerse si no se cuenta con un parámetro de referencia, como lo son los tipos y niveles de seguridad.

Tipos que si bien se encuentran establecidos dentro del glosario de conceptos de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, estos se encuentran desvinculados de los objetivos de control, lo cual eventualmente puede volver inoperante el sistema de gestión, si este no ha sido implementado de manera estratégica.

Así, al contar con un marco de referencia con relación al valor de los activos, vez genera a su vez un parámetro para determinar el nivel de seguridad, muestra de ello es el Artículo 82 de la Ley General que establece:

> Los responsables de las bases de datos a que se refiere este Capítulo, deberán establecer medidas de seguridad de *nivel alto*, para garantizar la integridad, disponibilidad y confidencialidad de la información, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Sin embargo, del análisis de dicha legislación no se establece qué parámetros deberán cumplirse para contar con ese nivel de protección.

Es por eso que, para evitar esfuerzos desproporcionados por parte de los sujetos obligados, se deben contar con parámetros mínimos de referencia sobre el adecuado tratamiento de datos personales, para lo cual resulta útil el establecimiento de tipos y niveles de seguridad.

Ahora bien, en lo que hace al enfoque basado en procesos, también constituye un elemento importante para la protección de los datos, puesto que para poder establecer las medidas de seguridad adecuadas, resulta importante identificar la trazabilidad del tratamiento de los datos personales y gestionar adecuadamente los soportes a través de los cuáles son utilizados, a través de la identificación y registro de sistemas de datos personales.

La Ley General contempla la obligación de llevar a cabo un inventario de datos personales y de los sistemas relativos a su tratamiento, sin embargo, se considera que dicha disposición resulta insuficiente, puesto que los riesgos inherentes al tratamiento se pueden presentar en cada etapa en la cual este se realice, por lo cual adquiere importante el enfoque basado en procesos, es decir, identificar en

qué momento inicia el tratamiento de datos personales y en qué momento termina, con la finalidad de identificar las diversas bases de datos y soportes, y establecer las medidas de seguridad adecuadas para cada etapa.

Finalmente, un tema importante para gestionar la protección de datos personales es la responsabilidad de los servidores públicos, tema en el cual la Ley General no establece ninguna regla para su individualización, puesto que el concepto responsable es genérico y por ende pudiera aplicar para cualquier servidor público del sujeto obligado, lo cual pudiera convertirse en factor crítico para una protección de datos personales efectiva, en la cual el factor humano es primordial a través de la asignación de funciones, responsabilidades y autoridades.

Sobre el particular, como se mencionó previamente, el Artículo 95 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, establece lo siguiente:

> Corresponde en principio al administrador el cumplimiento de las disposiciones previstas en esta Ley para el responsable, sin perjuicio que los titulares de las áreas o unidades administrativas que decidan sobre el tratamiento, contenido o finalidad de los Sistemas de Datos Personales, encargados, terceros, usuarias o usuarios y demás autoridades previstas en este capítulo incurran en responsabilidad solidaria.
>
> Los responsables deberán colaborar con el Instituto para capacitar y actualizar de forma permanente a todos sus servidores públicos en materia de protección de datos personales, a través de la impartición de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.

Artículo en el cual se observa la individualización de responsabilidades para proveer la implementación de la Ley, con el objeto de ilustrar que todavía queda un importante camino en la implementación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por parte de los diversos actores involucrados.

V. REFLEXIONES FINALES

La protección de datos personales en el sector público cuenta con características que le distinguen de la que se realiza en el sector privado, en congruencia con el marco jurídico de actuación que rige a los entes públicos, la cual, constituye un punto de partida para el desarrollo de principios y procedimientos especiales para este tipo de tratamiento.

La coyuntura actual a nivel nacional e internacional, presenta cambios importantes en la dimensión y aplicación de la protección de datos personales, por lo que resulta necesario dar seguimiento a las acciones que implementen las autoridades de control en torno a dichos ajustes.

En México, tanto en el sector público como en el privado, contamos con legislación en protección de datos personales acorde a estándares internacionales, y, a pesar de que esta disciplina es de reciente incorporación a nuestra cultura y legislación, es factible su adopción rápida por parte de nuestro país dada la estructura de sus instituciones y su régimen jurídico, a través de mecanismos rígidos de protección, pero a la vez flexibles para permitir su uso y flujo de manera segura por parte de los entes responsables del tratamiento.

No obstante lo anterior, el diseño institucional solamente constituye el cimiento para la generación de la curva de aprendizaje que deberán experimentar tanto titulares como responsables, que a través de disposiciones generales facilitan su uniformidad, sin limitar la posibilidad de que las entidades federativas sean progresivas de este derecho, actividades que en el transcurso de los años, determinarán en definitiva el alcance y dimensión de la protección de datos personales en México, promoviendo la certidumbre de un uso confiable de los datos personales de los mexicanos como ciudadanos del mundo.

VI. FUENTES DE INFORMACIÓN

1. *Bibliografía*

GARZÓN VALDÉS, Ernesto, *Lo íntimo, lo privado y lo público*, México, IFAI, 2005, *http://201.144.56.20/transparencia/cuadernillo_06.pdf, ISBN 968-5954-16-X.*

REMOLINA ANGARITA, Nelson, *Tratamiento de datos personales. Aproximación internacional y comentarios a la Ley 1581 de 2012*, Bogotá, Legis, 2013.

TRONCOSO REIGADA, Antonio, *La protección de datos personales. En busca del equilibrio*, Valencia, Tirant Lo Blanch, 2010.

WARREN, Samuel D., y Brandeis, Louis D., "The right to privacy", *Harvard Law Review*, vol. 4, número 5, 15 de diciembre de 1890, *http://www.jstor.org/stable/1321160?seq=1#page_scan_tab_contents, el 25/08/2017.*

2. *Legislación*

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

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

3. *Sitios de Internet*

Organización de las Naciones Unidas, *http://ask.un.org/es/faq/13553.*

CAPÍTULO OCTAVO
Los derechos ARCO en los sujetos obligados

Sergio HERNÁNDEZ[142]

SUMARIO

I. INTRODUCCIÓN

El derecho a la protección de datos personales (en adelante DPDP) es definido por Pulido como "la protección jurídica con la que cuentan las personas respecto a la recopilación, almacenamiento, utilización, transmisión y cualquier otra operación realizada sobre cierta información personal con características particulares a la que se le han llamado datos personales"[143].

[142] Licenciado en Derecho por la Universidad Nacional Autónoma de México. Maestro en Tecnologías de la Información por el Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC). Actualmente se desempeña como Subdirector de Indicadores y Desempeño del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

[143] Citado por Gurza Jaidar, Laura "La protección de la privacidad en la era de la vigilancia masiva", ponencia dentro del panel 2, *Foro: La privacidad en la era digital*, 20 de octubre de 2015, *http://slideshowes.com/doc/1289603/panel-2.--la-protecci%C3%B3n-de-la-privacidad-en-la-era-de-la.*

En ese sentido, partiremos de que el DPDP es aquella facultad con la que cuenta cualquier persona física, que tutela el tratamiento de información que pudiese identificar o hacer identificable a una persona, por lo que tal protección debe abarcar toda aquella información personal que lo es por su propia naturaleza, tal y como se establece en la normativa nacional e internacional en la materia[144].

Tal derecho fundamental ha ido evolucionando normativamente de tal manera que actualmente ha cobrado una mayor injerencia en el actuar de cualquier ente privado o gubernamental.

En México, el DPDP actualmente se ejerce ante dos grandes ámbitos, el sector privado y el sector público, los cuales cuentan con normatividad específica para garantizar su respeto, a través de procedimientos.

Por lo que, para efectos de este artículo, se analizará lo establecido en la normativa federal aplicable en materia de la protección de datos personales en el sector público, incluyendo algunos acuerdos emitidos por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante INAI), con motivo de la interpretación y aplicación de la ley misma.

Antes de ello, e necesario hacer referencia a algunos antecedentes normativos en México, que marcaron el inicio de la regulación para el ejercicio del DPDP en nuestro país, hasta la emisión de la actual Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (en adelante LGDPPSO).

---

[144] Las normas jurídicas a las que me refiero son a nivel internacional: la Carta de Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, el Convenio número 108 del Consejo de Europa, de 28 de enero de 1981, la Directiva 95/46/CE relativa a la protección de datos (misma que quedará derogada en mayo de 2018) en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.
A nivel nacional, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y en diversas leyes estatales en materia de protección de datos en posesión de sujetos obligados. En ellos se retoma, de manera general, que por dato personal se debe entender a toda información concerniente o relativa a una persona física identificada o identificable.

II. ANTECEDENTES DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN MÉXICO

En primer lugar, se debe hacer mención de dos reformas constitucionales, que fueron parteaguas en materia de datos personales. Así, en el año 2007, el Artículo 6o. constitucional fue objeto de una reforma que, entre otras cosas, sería la primera inclusión en la Carta Magna (hasta ese entonces como garantía individual), respecto de la protección de datos en los siguientes términos[145]:

> A…
>
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su actualización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
>
> …

Tanto en la fracción segunda como en la tercera del Artículo citado, por primera vez se estableció la mención expresa de la protección a la vida privada y los datos personales, e incluso se garantizó a cualquier persona el acceso y rectificación de los mismos[146]. Cabe señalar que esta primera mención incluyó dentro del Artículo que fijaba las bases para el ejercicio del derecho de acceso a la información.

Posteriormente, durante el año 2009 se presentaron dos reformas constitucionales que impactaron de manera amplia en el desarrollo del DPDP en nuestro país.

---

[145] Decreto por el que se reforma la fracción X del Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, en el Diario Oficial de la Federación el 20 de julio de 2017, Artículo Único, *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_174_20jul07_ima.pdf*.

[146] En palabras de la Dra. Puente de la Mora, Ximena, Comisionada del INAI, con dicha reforma constitucional, además de reconocer formalmente el reconocimiento de derecho a la protección de datos personales en México, también se trató de "unificar algunas disposiciones existentes en algunas constituciones de entidades federativas en la República Mexicana, como las de los estados de Colima, Guanajuato, Tlaxcala, Morelos, Oaxaca, México y Coahuila, puesto que cada uno de ellos hasta la fecha, conceptualizan este derecho en términos, con condiciones y alcances diferentes".
Comunicado de Prensa del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales: *Sin precedente, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, INAI, INAI/015/17, 26 de enero de 2017, *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-015-17.pdf*.

La primera ocurrió el 30 de abril, en la que se modificó el Artículo 73 constitucional, con la cual se le otorgó al Congreso de la Unión, la facultad exclusiva de "legislar en materia de protección de datos personales en posesión de particulares"[147].

La segunda reforma constitucional en materia de protección de datos personales en 2009, se publicó en el Diario Oficial de la Federación el 1 de junio y fue respecto al Artículo 16, estableciéndose en su segundo párrafo lo siguiente:

> *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 pública o para proteger los derechos de terceros.
>
> …

Con el conjunto de reformas mencionadas, se obtuvo un grado de protección altísimo al derecho fundamental a la protección de datos personales en el marco jurídico mexicano, pues con ello se garantiza la Constitución, el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición) previa acreditación de la personalidad de su titular o la de su representante legal[148].

Pero a pesar de que tal protección se formalizó constitucionalmente hasta el año 2009, ello no impidió que el ejercicio de los derechos de acceso, corrección (rectificación), ya se hubiera contemplado en legislación secundaria a nivel federal

---

[147] Decreto por el que se adiciona la fracción XXIX-O al Artículo 73 constitucional, publicado en el Diario Oficial de la Federación el 30 de abril de 2009, Artículo Único, *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf*.

[148] No se óbice hacer referencia a la reforma constitucional del 10 de junio de 2011, por la que se modificó, entre otras cosas, su Título Primero, sustituyendo el término "garantías individuales" por el de "derechos humanos", con lo que se dio entrada a la cláusula de interpretación conforme y control de convencionalidad, introduciéndose el principio *pro persona*. Lo anterior tuvo como consecuencia, que hasta la fecha cualquier autoridad deba aplicar los derechos humanos contenidos en tratados internacionales ratificados por nuestro país, ya que cuentan con un nivel de protección constitucional, favoreciendo en todo tiempo a las personas, la protección más amplia. Decreto por el que se modifica la denominación del Capítulo I del Título Primero y reforma diversos artículos de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación, el 10 de junio de 2011, Artículo Único, *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_194_10jun11.pdf*.

desde el año 2002, como fue el caso de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) publicada en el Diario Oficial de la Federación el 11 de junio de ese mismo año.

En concordancia con ello, en la LFTAIPG se establecieron los procedimientos y se sensibilizó sobre las características y la importancia del DPDP, de tal manera que, ante la convergencia de ese derecho, con el derecho de acceso a la información, se pretendió garantizar la protección de los datos personales en el sector público. No obstante, se dejó fuera de su ámbito de aplicación a la protección, los datos personales en poder de particulares. Para reglamentar tal derecho en el Diario Oficial de la Federación el 5 de julio de 2010, se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares que se encuentra vigente actualmente.

En notable resaltar la relación que existe entre ambos derechos, pues la protección de datos personales se constituyó como un límite al derecho de acceso a la información, a través de su clasificación como información confidencial con el objeto de proteger la privacidad de cualquier persona.

Además, derivado de la reforma constitucional de 2011 en materia de derechos humanos, ambos derechos, dejaron de ser garantías individuales, para elevar la protección a nivel de derechos fundamentales, lo cual nos lleva a la siguiente relación, en la que se encuentra la realización de un análisis de ponderación para su ejercicio, como lo manifestó el Ministro Gutiérrez Ortiz Mena: "No puede ejercerse un derecho fundamental en perjuicio de otro derecho si no media una causa proporcionada idónea que así lo justifique"[149].

Esto es, debe existir un equilibrio o ponderación entre ambos, que justifique conocer la información que se clasificó como confidencial y, por lo tanto, sea accesible para quien la haya solicitado, por así convenir al interés público que prevalece frente al deber de cuidado de la información confidencial. Esta responsabilidad recae con mayor peso en las entidades gubernamentales que realizan el tratamiento de datos personales debido a que es su obligación transparentar y rendir cuentas

[149] *Reflexiones sobre el Derecho de Acceso a la Información y la Iniciativa de Ley General de Transparencia,* México, Centro de Análisis e Investigación FUNDAR, 2015, p. 10, *http://www.senado.gob.mx/comisiones/estudios_legislativos2/docs/transparencia/Reflexiones_FUNDAR.pdf*.

de lo que sin menoscabar los derechos fundamentales de quienes debe proteger conforme a la Ley.

A través de la LFTAIPG se garantizó la protección de los datos personales en el sector público federal, en posesión de los sujetos obligados[150]. Cualquier persona comenzó a ejercer principalmente los derechos de acceso y corrección (rectificación), de manera formal por así estar contemplados en la Ley indicada, a sus datos personales en posesión de cualquier dependencia o entidad federal, otorgando al entonces Instituto Federal de Acceso a la Información (IFAI) la competencia para garantizar ese derecho.

En su capítulo IV, denominado "Protección de Datos Personales", que comprende de los Artículos 20 a 26, se establecieron las diversas obligaciones para los denominados sujetos obligados[151] como lo fue, primeramente, el establecimiento de un marco regulatorio para su tratamiento.

Poco a poco se adoptaron los procedimientos adecuados para la tramitación de solicitudes de acceso y corrección de datos personales, capacitar a los servidores públicos, tratar los datos personales, capacitar a los pertinentes y no excesivos en relación con los propósitos para los cuales se hubiese obtenido (por cualquier motivo), e informando a sus titulares los propósitos para su tratamiento. Se procuró que fueran exactos y actualizados, se adoptaron las medidas necesarias que garantizaran la seguridad de los datos personales y evitaran su alteración, pérdida, transmisión y acceso no autorizado.

Es claro que los particulares tienen múltiples causas por las que comparten sus datos personales con las entidades y dependencias del gobierno federal, tales como trámites, pago de impuestos, solicitudes de apoyo, entre otros. De ahí que

---

[150] Artículo 4o., fracción III de la LFTAIPG: III. Garantizar la protección de los datos personales en posesión de los sujetos obligados.

[151] Conforme al Artículo 3o., fracción XIV de la LFTAIPG, se estableció como sujeto obligado: a) El Poder Ejecutivo, la Administración Pública Federal y la Procuraduría General de la República; b) El Poder Legislativo, integrado por la Cámara de Diputados y la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal; d) Los órganos constitucionales autónomos; e) Los tribunales administrativos federales, y f) Cualquier otro órgano federal.

los interesados, con fundamento en la LFTAIPG, y en el ejercicio de sus derechos ARCO, accedían y corregían sus datos personales cuando resulten inexactos o incompletos[152] (Artículo 24), dentro del sector público y verificaban que los sujetos obligados, durante su tratamiento, cumplieran con la finalidad con la que los habían obtenido, así como ha ocurrido en otros países, como es el caso de España[153].

Por su parte, además de lo establecido en su Capítulo IV, el Artículo 61 de la LFTAIPG dispuso que el Poder Legislativo Federal, a través de la Cámara de Senadores y la Cámara de Diputados, la Comisión Permanente y la Auditoría Superior de la Federación; el Poder Judicial de la Federación mediante la Suprema Corte de Justicia de la Nación, el Consejo de la Judicatura Federal y la Comisión de Administración del Tribunal Federal Electoral; los órganos constitucionales autónomos y los tribunales administrativos, en el ámbito de sus respectivas competencias, debían emitir reglamentos o acuerdos de carácter general, así como los órganos, criterios y procedimientos institucionales para proporcionar a los particulares el acceso a la información, de conformidad con los principios y plazos establecidos en dicha Ley y en el ejercicio de los "procedimientos de acceso y rectificación de datos personales a los que se refiere el Artículo 24 y 25" de la LFTAIPG[154].

---

[152] *Derecho de Rectificación*, Madrid, Agencia Española de Protección de Datos Personales, 2014, *http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/rectificacion-ides-idphp.php.*

[153] *Derecho de Acceso,* Madrid, Agencia Española de Protección de Datos Personales, 2014, *http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/acceso-ides-idphp.php.*

[154] Además de lo establecido en la LFTAIPG, la Administración Pública Federal debía aplicar lo contenido en el Capítulo XIII, De los procedimientos de acceso y corrección de los datos personales, de su Reglamento, así como los Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procedimiento, trámite, resolución y notificación de las solicitudes de corrección de dichos datos, los últimos tres emitidos por el entonces Instituto Federal de Acceso a la Información Pública, motivo por el cual los sujetos obligados debían aplicar varios cuerpos normativos para cumplir con el derecho a la protección de datos personales en nuestro país.
http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFTAIPG.pdf.
http://inicio.ifai.org.mx/MarcoNormativoDocumentos/250803.pdf.
http://inicio.ifai.org.mx/MarcoNormativoDocumentos/dof060404.pdf.
http://inicio.ifai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf.

El procedimiento iniciaba a partir de una solicitud hecha por el particular ante el sujeto obligado de su interés, acreditando previamente su personalidad o la de su representante legal. La unidad de enlace correspondiente, comunicaba a la unidad administrativa competente dentro del sujeto obligado, del contenido de la solicitud de datos personales, para que en el plazo de 10 a 30 días hábiles improrrogables, entregara el documento que contuviera los datos personales solicitados o bien llevara a cabo su modificación cuando así procediera, para que ésta la hiciera del conocimiento del solicitante.

Asimismo, en los casos en los que no resultara procedente el acceso a la corrección de los datos personales debido a su inexistencia dentro de los archivos del sujeto obligado, su Comité de Información debía analizar el informe remitido por la unidad administrativa en el que se fundaran y motivaran las razones por las que la información no se había localizado, de tal manera que dicho Comité debía emitir una resolución, igualmente, fundada y motivada a través de la cual confirmara su inexistencia. En casi de que la información si estuviese pero que no procediera su corrección, el Comité también debía pronunciarse respecto a la improcedencia total o parcial de las correcciones solicitadas, misma que se le notificaban al particular.

Por lo que el particular desde el momento en que tenía conocimiento de la respuesta del sujeto obligado y estuviera inconforme con la misma, o bien hubiera transcurrido el plazo para su emisión (10 o 30 días hábiles) sin haberla recibido, contaba con un plazo de 15 días hábiles para la interposición del recurso de revisión, por sí mismo o a través de su representante legal previa acreditación de su personalidad.

En ese caso, el entonces IFAI en su carácter de organismo garante del DPDP a nivel federal, debía emitir una resolución dentro de los siguientes 50 días hábiles, prorrogables hasta por otro tanto igual, en la que se podría desechar o sobreseer el recurso de revisión, o en su caso confirmar, revocar o modificar la respuesta del sujeto obligado[155].

---

[155] Como se indicó líneas arriba, en los casos relativos a los sujetos obligados distintos a la Administración Pública Federal, indicados en el Artículo 61 de la LFTAIPG, también denominados "Otros Sujetos Obligados" (OSO's), el IFAI no era competente para sustanciar medios de impug-

Ahora bien, después de la referencia hecha a algunos antecedentes normativos y de procedimientos en nuestro país, donde establecieron el inicio a la regulación para la protección del DPDP, se continuará con el análisis del procedimiento del ejercicio de los derechos ARCO ante los sujetos obligados del orden federal, conforme a la recién vigente Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y demás normativa relacionada con la misma.

III. LEGISLACIÓN VIGENTE EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

La LGPDPPSO fue publicada en el Diario Oficial de la Federación el 26 de enero de 2017, y dentro del ámbito jurídico mexicano, fue considerada como una norma sin precedentes para "que dotará al sector público de certeza jurídica y equilibrio regulatorio para la protección de ese derecho fundamental"[156].

En ese sentido, uno de los principales cambios en la interpretación y, por lo tanto, en el ejercicio del derecho fundamental a la protección de datos personales, consistió en el ámbito de su aplicación. Así, la LGPDPPSO es de observancia general en toda la República Mexicana y para el caso de los sujetos obligados del orden federal, su aplicación y observancia es directa. Su objeto consiste en "establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados"[157].

Es así que, dicha Ley General amplía notablemente la cantidad de entes del sector público a las que les son exigibles las disposiciones que establece. De tal manera que por sujeto obligado en el mencionado ordenamiento jurídico, se entiende

---

nación interpuestos en contra de las respuestas emitidas por dichos entes gubernamentales. No obstante, conforme a la fracción VII del Artículo mencionado, los OSO's debían de contar con una instancia interna responsable de aplicar la LFTAIPG, resolver los recursos de revisión y las demás facultades que correspondieran en su carácter de organismo garante del derecho a la PDP.

156 Así lo manifestó la entonces Comisionada Presidente Ximena Puente de la Mora, el 26 de enero de 2017, en el marco de la conmemoración del Día Internacional de Protección de Datos Personales, *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-015-17.pdf.*

157 Artículo 1o. de la LGPDPPSO.

a todo ente en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismos de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

No obstante, la nueva Ley en materia de datos personales no alcanza a cubrir a los nuevos sujetos obligados en materia de transparencia como son 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. Para ellos, se contempla dentro de su marco normativo en materia de protección de datos personales, únicamente a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Ahora bien, respecto al ejercicio de los derechos ARCO por parte de sus titulares ante los sujetos obligados de la LGPDPPSO, en esta sí se regula de manera expresa la posibilidad de su acceso, rectificación, corrección y oposición por parte de los titulares de los datos personales.

Como bien se dijo líneas arriba, cualquier persona en nuestro país debe interactuar con los entes que pertenecen al sector público para poder ejercer sus derechos o cumplir sus obligaciones, y en esa interacción, existe una transmisión de datos personales desde su titular hacia la autoridad o ente del sector público, teniendo por consecuencia que se genere el tratamiento de los datos personales obtenidos.

En principio, la LGPDPPSO establece en su Artículo 3o., fracción XXXIII, que por tratamiento se debe entender: "Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales"[158].

Por lo que es tan amplia la serie de actos en los que se puede presentar el tratamiento de datos personales, que los sujetos obligados deben cumplir con los objetivos establecidos en la LGDPPSO, garantizando la observancia de los princi-

[158] Artículo 3o. de la LGPDPPSO.

pios de su protección y permitiendo que toda persona pueda ejercer su DPDP. Por tanto, el ejercicio del DPDP inicia desde aquel momento en que dentro de los archivos (expedientes, bases de datos, etc.) de cualquier ente que pertenece al sector público, existen datos personales, cuyo tratamiento ilegal o sin el consentimiento otorgado, podría generar un menoscabo en la esfera jurídica de sus titulares.

Con la LGPDPPSO, se amplía la gama de vertientes que puede seguir un particular para el ejercicio de los derechos ARCO ante los sujetos obligados, y a su vez, estos adquieren nuevas obligaciones y deberes para su cumplimiento, las cuales de manera general se indican a continuación[159]:

- Deben establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona física a la protección de sus datos personales en posesión de todo ente público de los tres órdenes de gobierno (todos sujetos obligados);
- Deben establecer y respetar los diversos conceptos, figuras jurídicas que participaron en la protección de datos personales, tales como los relativos al ejercicio de los derechos ARCO, aviso de privacidad, bloqueo, documento de seguridad, responsable, encargado, medios de impugnación, procedimiento de verificación, medidas de apremio y sanciones, entre otras, de acuerdo con los estándares nacionales e internacionales en la materia;
- Se distribuyen competencias entre el organismo garante nacional (INAI) y los organismos garantes estatales, para una coordinación de los tres órdenes de gobierno para el cumplimiento normativo;
- Define un régimen de transferencias nacionales e internacionales de datos personales, que facilite el intercambio de información personal entre las autoridades de los tres órdenes de gobierno; y

[159] Así lo ha informado el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en diversos comunicados de prensa. Por ejemplo: *Sin precedente, la Ley General de Protección de Datos Personales en Posesión de sujetos Obligados: INAI*, INAI/015/17; *Hoy entra en vigor la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, INAI/020/17; *Ley General sentará bases para construcción de un sólido sistema de protección de datos personales en sector público,* INAI/029/17; entre otros. *http://inicio.ifai.org.mx/SitePages/Comunicados-2017.aspx*.

- Establece reglas para el tratamiento de datos personales por parte de instancias de seguridad y precaución de justicia.

Ahora bien, el procedimiento relativo al ejercicio de los derechos ARCO ante los sujetos obligados, se encuentra regulado en el Titulo Tercero, Derecho de los Titulares y su Ejercicio, de la LGPDPPSO; en él se determinan las siguientes bases:

¿Quién puede ejercer los derechos ARCO? Los derechos ARCO pueden ser ejercidos en todo momento por el titular o su representante, acreditando la identidad del primero y en su caso la identidad y personalidad del segundo. Excepcionalmente por persona distinta al titular o su representante, en casos previstos por alguna disposición legal o por mandato judicial.

Para el caso de menores de edad o de personas en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación. Tratándose de datos personales concernientes a personas fallecidas, su derecho podrá ser ejercido por la persona que acredite tener un interés jurídico, siempre que el titular hubiere expresado fehacientemente su voluntad o que exista un mandato judicial para dicho efecto.

Características del ejercicio de derechos ARCO:

- Es gratuito. Solo se pueden realizar cobros ara recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable;
- El titular puede proporcionar el medio de reproducción de los datos personales, evitando así el costo respectivo;
- Los sujetos obligados, a través de la Unidad de Transparencia, pueden exceptuar el pago de costos de reproducción y envío, en atención a las circunstancias socioeconómicas del titular, o cuando la entrega de la información sea de no más de veinte hojas simples;
- El responsable (sujeto obligado) no puede establecer algún costo al titular para la presentación de solicitudes de ejercicio de derechos ARCO;
- Es deber de los sujetos obligados establecer procedimientos sencillos que permitan el ejercicio de derechos ARCO;

- El plazo de respuesta no deberá exceder de veinte días hábiles contados a partir del día siguiente a la recepción de la solicitud, mismo que podrá ser ampliado por una sola vez hasta por diez días hábiles, siempre y cuando se le notifique al titular dentro del plazo de respuesta;
- Si el ejercicio de cualquier derecho ARCO resulto procedente, el sujeto obligado debe hacerlo efectivo en un plazo máximo de quince días hábiles contados a partir del día siguiente a la notificación de la respuesta; y
- Ante la solicitud para el ejercicio de derechos ARCO no pueden exigirse mayores requisitos a los establecidos en el Artículo 52 de la LGPDPPSO.

IV. FASES DEL EJERCICIO DE DERECHOS ARCO (A NIVEL FEDERAL)[160]

Este documento, marca el inicio del ejercicio de los derechos ARCO del titular de los datos personales, la cual se puede presentar ante la Unidad de Transparencia del responsable a través de escrito libre, formatos, medios electrónicos o cualquier otro que a efecto establezca el INAI o el sujeto obligado, en el ámbito de sus respectivas competencias.

Es necesario precisar que, para el caso de los formatos, el Pleno del INAI, mediante el Acuerdo número ACT-PUB/01/02/2007.06[161], aprobó el Formato para la atención de solicitudes de ejercicio de los derechos ARCO[162], no obstante, el particular puede presentar un escrito libre con los requisitos establecidos en el Artículo 52 de la LGPDPPSO.

Para ambos casos (formatos y escrito libre), al momento en el que se presenta ante la oficina de la Unidad de Transparencia del sujeto obligado, el responsable del mismo también debe registrar la petición en los sistemas electrónicos, generando el correspondiente acuse del sistema que contendrá un folio con el que el interesado podrá dar seguimiento a su solicitud de derechos ARCO.

---

[160] Cabe señalar que si bien, la LGPDPPSO establece las bases, principios y procedimientos para el ejercicio de derechos ARCO en los tres niveles de gobierno, lo cierto es que para efectos del presente artículo nos enfocamos al trámite que se presenta a nivel federal por la aplicación directa de la Ley General de la materia, sin olvidar que para que el caso de las legislaciones estatales, la LGPDPPSO resulta supletoria para los casos no previstos.

[161] Disponible en: *http://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-01-02-2017.06.pdf.*

[162] Disponible en: *http://inicio.ifai.org.mx/FormatosINAI/FormatoDerechosARCO.docx.*

Por lo que hace a "medios electrónicos o cualquier otro medio", los titulares pueden presentar su solicitud de derechos ARCO en las páginas electrónicas correspondientes al sistema INFOMEX[163], y por supuesto, en la Plataforma Nacional de Transparencia (PNT)[164]. En ambos sistemas, es necesario que el titular se registre como usuario (en caso de no tenerlo) y para darle seguimiento a su solicitud.

Todas las notificaciones se hacen a través del mismo medio por el que se presentó la solicitud, salvo que el particular indique algún otro para recibirlas como lo es, un domicilio físico, un correo electrónico o por medio de los estrados.

Además, el INAI ha establecido un servicio telefónico denominado Tel-INAI (01-800-835-4324) cuya función es, entre otras, realizar el registro de solicitudes el cual administra el Centro de Atención a la sociedad del mencionado organismo garante.

1. *Trámite de la solicitud*

Como se señaló líneas arriba, al momento de la presentación de la solicitud de derechos ARCO, el sujeto obligado a través de la Unidad de Transparencia debe dar el trámite que conforme a derecho corresponda.

Por lo que la Unidad de Transparencia del responsable comienza a analizar si la solicitud cumple con todos los requisitos establecidos en la LGPDPPSO para poder darle trámite. En su defecto, y si no cuenta con los elementos para subsanar la falta de alguno de los requisitos, prevendrá al solicitante dentro de los cinco días siguientes a la presentación de la solicitud, por una sola ocasión, con el fin de subsanar las omisiones correspondientes en un plazo de diez días hábiles, a partir del día siguiente al de la notificación en el medio indicado.

Si el plazo de prevención transcurre sin su desahogo, la solicitud de ejercicio de derechos ARCO se tendrá por no presentada. La prevención interrumpe el plazo que tiene el sujeto obligado para la atención de la solicitud de ejercicio de los derechos ARCO, es decir, los veinte días hábiles.

Ahora bien, para que el sujeto obligado pueda analizar y atender la solicitud de derecho de cancelación, el titular debe señalar las causas que lo motiven a soli-

---

[163] Disponible en: *https://www.infomex.org.mx/gobiernofederal/home.action.*
[164] Disponible en: *http://www.plataformadetransparencia.org.mx/web/guest/inicio.*

citar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable. En el caso de oponerse al tratamiento de los datos personales, el titular debe manifestar las causas legítimas o la situación específica que lo llevaron a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia de tal actividad, o en su caso, las finalidades especificas respecto de las cuales requiere ejercer el derecho de oposición.

Posteriormente, el sujeto obligado debe determinar su competencia sobre el asunto, ya que, en caso de no hacerlo, tiene la obligación de notificarlo al titular, dentro de los tres días siguientes a la presentación de la solicitud y en su caso orientarlo hacia el responsable competente.

Además, si el responsable advierte que la solicitud del particular corresponde a un derecho diferente de los previstos en la presente Ley (es decir, acceso a la información) deberá reconducir la vía haciéndolo del conocimiento del titular.

2. *Tipos de respuesta*

A. *Prevalencia de un trámite o procedimiento*

En los casos que exista alguna disposición aplicable a determinados tratamientos de datos personales que indiquen el tratamiento o procedimiento específico para solicitar el ejercicio de derechos ARCO ante el responsable, el mismo tiene que hacerlo del conocimiento del particular en un plazo no mayor a cinco días siguientes a la presentación de la solicitud.

Por lo que el titular de los datos personales tiene la facultad de decidir si ejerce sus derechos a través del trámite específico, o bien, utiliza del procedimiento institucionalizado para la atención de solicitudes que debe estar apegado a las bases que establece la LGPDPPSO.

B. *Improcedencia de la solicitud de derechos ARCO*

El responsable del sujeto obligado, al momento de analizar el contenido de la solicitud de derechos ARCO, tanto en sus elementos de fondo y forma, puede determinar en un plazo de veinte días, que la misma no es procedente, fundando y motivando su determinación.

Entre los supuestos que permiten determinar la improcedencia del ejercicio de este derecho fundamental (contenidos en el Artículo 55 de la Ley General de la materia), están la falta de acreditación para su ejercicio, debido a que los datos personales no se encuentran en posesión del responsable, que este no sea competente, o que exista un impedimento legal, y que con ello se lesionen los derechos de un tercero. Asimismo, que una resolución de autoridad competente restrinja el acceso a los datos personales o no permita su rectificación, cancelación u oposición; o que la cancelación u oposición hayan sido previamente realizadas.

Igualmente hay falta de acreditación cuando los datos personales son necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular, y son parte de la información de las entidades sujetas a la regulación y este en cumplimiento a los requerimientos de información sobre sus operaciones, organización, actividades, entre otros.

C. *Procedencia del derecho ARCO correspondiente*

Como se mencionó líneas arriba, el responsable debe llevar a cabo el análisis de la procedencia de la solicitud para el ejercicio de los derechos ARCO del titular, por lo que después de realizar la búsqueda exhaustiva de los datos personales y verificar la procedencia de la pretensión requerida, el responsable del sujeto obligado tendrá como resultado lo siguiente por cada derecho:

- Acceso. Implica la obligación del responsable en informar al titular cuáles son los datos personales que tiene en su posesión, así como cualquier otra información que trata dentro de sus archivos y conforme a sus funciones, consentidas por el dueño de los datos. Además, con el ejercicio de este derecho, el particular podrá conocer las condiciones y generalidades de su tratamiento contenidas en el aviso de privacidad.

  El sujeto obligado debe poner a disposición del titular los datos personales en la modalidad solicitada (mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías de la información), en el plazo de veinte días hábiles a partir de la presentación de la solicitud, y cuyo acceso debe generarse en

formatos legibles o comprensibles en forma gratuita. El titular debe cubrir únicamente los gastos de envío, reproducción y, en su caso, certificación de documentos, salvo que él presente algún medio para la reproducción de la información.

- Rectificación. El titular puede ejercer este derecho en caso de que estén desactualizados, sean inexactos o incompletos. Para tales efectos, debe entregar la documentación que acredite la rectificación solicitada de acuerdo a los datos personales correctos.

  La pretensión de este derecho, se enfoca a controlar la calidad de la información de manera que se corrijan las imperfecciones, errores o defectos de los datos personales que trata.

  El sujeto obligado debe verificar los archivos que contienen los datos personales, y realizar los cambios correspondientes, permitiendo que esa información que trata sea exacta, pertinente, correcta y actualizada para el cumplimiento de las finalidades y principios en materia de protección de datos personales.

- Cancelación. Consiste en la eliminación de los registros, archivos o bases de datos, la información personal que indique el solicitante, cuando considere que la misma no está siendo utilizada adecuadamente, en otras palabras, solicita que termine el tratamiento de sus datos, debido a un tratamiento indebido o ilegal.

  Por lo anterior, es dable decir que este derecho se ve íntimamente relacionado con el principio de finalidad del tratamiento de los datos personales, ya que puede requerir que el responsable se abstenga de seguir utilizando los datos referidos cuando se haya cumplido con la finalidad por la que fueron recabados.

  Cabe señalar, que previo a la cancelación del dato personal, el responsable debe identificar aquellos datos que hayan cumplido con su finalidad y conservarlos únicamente con el propósito de determinar posibles responsables en relación con el tratamiento, hasta el plazo de prescripción

legal o contractual de estas. Transcurrido ese tiempo, se procederá a su cancelación en la base de datos que corresponda, si es que el particular no ha ejercido este derecho.

A este hecho se le denomina *bloqueo*, y se vuelve una obligación del responsable durante el tratamiento de datos personales, ya que debe notificarlo a su titular en cuanto inicie el periodo de bloqueo.

- Oposición. Consiste en la manifestación de la voluntad del titular negándose al tratamiento de sus datos personales para, manifestando las causas legítimas o la situación específica que lo llevan a solicitarlo, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades concretas respecto de las cuales requiere el derecho de oposición.

  Ante este tipo de solicitudes, el sujeto obligado debe notificar al titular sobre la procedencia de su petición, en el plazo máximo de quince días hábiles contando a partir del día siguiente a la notificación de la respuesta, es decir, dentro de veinte días hábiles contando a partir de la presentación de la solicitud.

D. *Inexistencia e incompetencia*

En este punto, conviene aclarar que si bien es cierto, la inexistencia de los datos personales y la incompetencia del sujeto obligado para atender la solicitud de ejercicio de derechos ARCO, son supuestos contenidos en los Artículos 53 y 55 de la LGPDPPSO, también lo es, que dicho cuerpo normativo no establece los procedimientos de búsqueda de los datos personales que den certeza jurídica a los particulares sobre el procedimiento usado para su localización.

No obstante, los Artículos 83 y 85 de la LGPDPPSO establecen que tanto la integración como el funcionamiento de la unidad y el Comité de Transparencia deberán llevarse a cabo conforme a la Ley General de Transparencia y Acceso a la Información Pública:

> Artículo 83. Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de

> Transparencia y Acceso a la Información Pública y demás normatividad aplicable.
>
> El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales…
>
> Artículo 85. Cada responsable contará con una Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, esta Ley y demás normatividad aplicable…

Asimismo, tanto el procedimiento de búsqueda de los datos personales y la declaración de incompetencia podrían ejecutarse conforme a lo establecido en la Ley General de Transparencia y Acceso a la Información Pública.

Es decir, para el caso de la búsqueda de la información, la Unidad de Transparencia debe turnar la solicitud de información a todas las áreas dentro del sujeto obligado, que pueden contar con los datos personales, por tanto valorar la procedencia de su solicitud, y con ello, las aquellas se pronuncien sobre la localización de la información y la procedencia del requerimiento del particular.

Lo anterior es relevante, ya que el sujeto obligado debe llevar a cabo el procedimiento de búsqueda exhaustivo y razonable, utilizando un criterio de interpretación amplio, en el que su objeto sea localizar los datos personales respecto de los cuales el particular dese ejercer sus derechos ARCO.

Si el sujeto obligado cumple con lo indicado en los párrafos anteriores, su Comité de Transparencia debe emitir la resolución que confirme la inexistencia de los datos personales, en la que se analizará el caso y tomará las medidas pertinentes para localizar los datos personales requeridos y en su caso de no encontrarse, se expedirá una resolución en dichos términos.

Cabe señalar que el Pleno del entonces IFAI emitió el Criterio 12-10[165], "Propósito de la declaración formal de inexistencia", a través del cual se advierte que la intención de la emisión de una declaración formal de inexistencia por el Comité de Transparencia, es garantizar al solicitante que efectivamente se realizaron las ges-

[165] Disponible en: *http://inicio.ifai.org.mx/Criterios/Criterio%20%20012-10%20Prop%C3%B3sito%20declaraci%C3%B3n%20inexistencia.pdf.*

tiones necesarias para la ubicación de la información de su interés y que estas fueron las adecuadas para atender a la particularidad del caso concreto; es decir, que se dé certeza al solicitante del carácter de la búsqueda de la información requerida.

Ahora bien, respecto a la competencia para atender la solicitud de derechos ARCO, la LGPDPPSO no establece la inexistencia de la figura jurídica denominada *notoria incompetencia*, por lo que es dable interpretar que, para la declaración de incompetencia del sujeto obligado, y conforme a lo establecido en la Ley General de Transparencia y Acceso a la Información Pública, se deberá emitir por el Comité de Transparencia, una resolución que así lo confirme.

En dicha declaración de incompetencia se debe analizar las atribuciones del sujeto obligado para conocer de los datos personales de interés del particular, ya que la incompetencia, es un concepto que se atribuye al sujeto obligado, es decir, implica la ausencia de atribuciones del ente público para poseer información solicitada[166], ya que se trata de una cuestión de derecho, en tanto que no existen facultades para contar con lo requerido; por lo que la incompetencia es una cualidad atribuida al sujeto obligado que la declara.

3. *Otros tipos de respuesta*

Ahora bien, dada la amplia gana de normativa que aplica a la materia de protección de datos personales y acceso a la información, se puede presentar algunas situaciones en las que se niegue el ejercicio de derechos ARCO por algún interés jurídico superior que se deba proteger frente al interés del particular que pretende ejercer el mencionado derecho fundamental.

Una de ellas, es la clasificación de los datos personales como confidenciales, que debería realizarse conforme al procedimiento establecido en la Ley General de Transparencia y Acceso a la Información pública y los lineamientos que de ella emanen[167].

---

[166] Así lo estableció el Pleno del INAI en el Criterio 13/17 "Incompetencia", disponible en: *http://criteriosdeinterpretacion.inai.org.mx/Criterios/13-17.pdf*.

[167] Para el caso de la clasificación de información, resultan aplicables los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración

Otro supuesto puede ser la atención en una modalidad distinta que ocurre cuando, los sujetos obligados se encuentran en la necesidad de cambiar modalidad que eligió el particular para el ejercicio de sus derechos ARCO. Y, si bien, es cierto que en principio tal situación podría alterar el resultado esperando por el titular respecto de sus datos personales, también lo es que la norma pueda dificultar en ocasiones que el responsable atienda la modalidad requerida, lo cual sin duda alguna debe fundar y motivar de acuerdo al caso concreto.

Sin embargo, en un afán de garantizar plenamente el DPDP, se recomienda a los sujetos obligados analizar de manera amplia la posibilidad de atender la modalidad elegida por el particular y en su defecto, ofrecer todas las modalidades restantes con el fin de garantizar el ejercicio de los derechos ARCO del particular, aunque sea en otro medio de reproducción[168].

V. RECURSO DE REVISIÓN ANTE ORGANISMO GARANTE FEDERAL (INAI)

Es claro que, para un efectivo ejercicio del DPDP, los titulares deben contar con un mecanismo que les permita verificar, revisar e incluso exigir que se garantice su derecho fundamental a la protección de datos personales.

Para la materia de protección de datos personales en el sector público a nivel federal, los particulares cuentan con el medio de defensa denominado "recurso de revisión", y que pueden interponer ante el INAI, el cual es el organismo constitucio-

---

de versiones públicas, publicadas en el Diario Oficial de la Federación el 15 de abril de 2016, así como también su modificación de Artículos Sexagésimo Segundo, Sexagésimo Tercero y Quinto Transitorio, publicada el 29 de julio de 2016, disponibles para su consulta, respectivamente en: *http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Lineamientos%20generales%20en%20materia%20de%20clasificacion.pdf;* y *http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Acuerdos%20por%20los%20que%20se%20modifican%20los%20articulos.pdf*.

[168] Es cierto que en materia de protección de datos personales, no se han emitido criterios de interpretación por parte del INAI en cuanto a los cambios de modalidad elegida, sin embargo se podría interpretar de manera análoga lo emitido por dicho organismo garante en su Criterio 08/17 "Modalidad de entrega. Procedencia de proporcionar la información solicitada en una diversa a la elegida por el solicitante", disponible en: *http://criteriosdeinterpretacion.inai.org.mx/Criterios/08-17.pdf*.

nal autónomo garante de la federación en materia de protección de datos personales en posesión de los sujetos obligados.

En ese sentido, ante la respuesta a la falta de ella por parte del sujeto obligado[169], el particular cuenta con un mecanismo jurídico que le permita contar con mayor certeza jurídica respecto de la respuesta otorgada por el responsable y en su caso, obtener el correcto ejercicio de su derecho a la PDP por parte del sujeto obligado.

Dicho mecanismo es el recurso de revisión. Al respecto, con base al Artículo 89, fracciones III y XIX de la LGPDPPSO, el INAI emitió los Lineamientos para la recepción, sustanciación y resolución de los recursos de revisión en materia de datos personales, interpuestos ante el mencionado organismo garante para la sustanciación de los medios de impugnación que le sean interpuestos en la materia, con la finalidad de generar certeza y seguridad jurídica de las partes involucradas de todas y cada una de las actuaciones realizadas por el Instituto[170].

En otras palabras, dichos Lineamientos contienen el desarrollo de las etapas del procedimiento relativo a la tramitación, sustanciación y resolución de los recursos de revisión que conoce el INAI en materia de protección de datos personales, incluyendo las fases concernientes a la procedencia del recurso, la conciliación, acreditación de la personalidad y etapa probatoria.

VI. PENDIENTES NORMATIVOS DE LA LGPDPPSO

Si bien con la publicación de la LGPDPPSO el 26 de enero de 2017 en el Diario Oficial de la Federación, se marca el inicio de su entrada en vigor al día siguiente, lo cierto es que en sus Artículos Primero, Segundo y Cuarto Transitorios se otorgó un periodo (seis meses a partir de su entrada en vigor) de armonización legislativa

---

[169] Los supuestos de procedencia se encuentran en el Artículo 104 de la LGPDPPSO y que básicamente consisten en la negativa de la procedencia del ejercicio de derechos ARCO, que se ejerzan de manera parcial, la falta de respuesta o que el titular no esté conforme con la modalidad, costos de reproducción, entre otros.

[170] Considerando 10 del Acuerdo número ACT-PUB/29/03/2014.05, por el que se aprueban los Lineamientos para la recepción, sustanciación y resolución de los recursos de revisión en materia de datos personales, interpuestos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, disponible en: *http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Acuerdo%20-%20Lineamientos%20Recursos%20de.pdf*.

tanto para el Congreso de la Unión, como para las Legislaturas de las Entidades Federativas, que concluyó el 27 de julio de 2017 y que hasta esta fecha, solo 22 Estados contaban con una Ley aprobada, y el resto aplicaría de manera directa la LGPDPPSO.

No obstante, para el caso de la Federación, el Congreso de la Unión resultó omiso en realizar los ajustes correspondientes en la Ley Federal de Transparencia y Acceso a la Información Pública y las demás leyes federales aplicables en la materia, generando una responsabilidad mayor al INAI, ya que por un lado debe aplicar directamente la LGPDPPSO, y por otro debe emitir toda la normativa que derive de dicha Ley, a fin de garantizar al máximo el ejercicio del derecho fundamental a la protección de datos personales.

Ejemplos de lo anterior, se reflejan en la emisión de los mencionados Lineamientos para la recepción, sustanciación y resolución de los recursos de revisión en materia de datos personales, interpuestos ante el INAI, así como en los lineamientos que debe emitir conforme al Artículo 89 fracciones XXVII y XXVIII, relativos al debido tratamiento de los datos personales, así como para homologar el ejercicio de los derechos ARCO.

De tal manera que, si bien contamos una norma general que establece los mínimos irreductibles en el ejercicio del derecho a la protección de datos personales a nivel federal, lo cierto es que aún queda pendiente la emisión de diversos instrumentos que podrían aumentar las obligaciones de los responsables de datos personales, teniendo por consecuencia que el ejercicio del mencionado derecho fundamental pueda ser más claro o en su defecto, ser más complejo de lo que actualmente es, contradiciendo uno de los objetivos de la LGPDPPSO, respecto a que los procedimientos del ejercicio de los derechos ARCO deben ser sencillos y expeditos.

Finalmente, considero que, como titulares de este derecho, debemos exigir el cumplimiento a las bases mínimas que nos permitan ejercer nuestro derecho fundamental a la protección de datos personales por medio de los derechos ARCO ante los sujetos obligados.

VII. FUENTES DE INFORMACIÓN

1. *Bibliografía*

PELAYO MOYER, Carlos María, *Las reformas constitucionales en materia de derechos humanos*, 2ª. ed., México, Comisión de Derechos Humanos del Distrito Federal, 2013, *http://cdhdf.org.mx/serv_prof/pdf/lasreformasconstitucionalesenmateriade.pdf.*

Reflexiones sobre el Derecho de Acceso a la Información y la iniciativa de Ley General de Transparencia, México, Centro de Análisis e Investigación FUNDAR, 2015, *http://www.senado.gob.mx/comisiones/estudios_legislativos2/docs/transparencia/Reflexiones_FUNDAR.pdf.*

2. *Normatividad*

Acuerdo número ACT-PUB/01/02/2017.06, mediante el cual se aprueba el *Formato para la atención de solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales, de conformidad con lo dispuesto por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*.

Acuerdo número ACT-PUB/29/03/2017.05, por el que se aprueban los *Lineamientos para la recepción, sustanciación y resolución de los recursos de revisión en materia de datos personales, interpuestos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*.

Constitución Política de los Estados Unidos Mexicanos.

Criterio 08/17 "Modalidad de entrega. Procedencia de proporcionar la información solicitada en una diversa a la elegida por el solicitante", emitido por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Criterio 13/17 "Incompetencia", emitido por el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 30 de abril de 2009, Articulo Único.

Decreto por el que se modifica la denominación del Capítulo I del Título Primero y reforma diversos artículos de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 10 de junio de 2011, Artículo Único.

Decreto por el que se reforma la fracción X del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 20 de julio de 2007, Artículo Único.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Lineamientos de Protección de Datos Personales.

Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas.

Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.

Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal, en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.

Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

3. *Otros*

Comunicado de Prensa Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales: *Sin precedente, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: INAI*, INAI/015/17.

Comunicado de Prensa Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales: *Hoy entra en vigor la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, INAI/020/17.

Comunicado de Prensa Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales: *Ley General sentará bases para construcción de un sólido sistema de protección de datos personales en sector público,* INAI/029/17.

Derecho de Acceso, Madrid, Agencia Española de Protección de Datos Personales, 2014, *http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/acceso-ides-idphp.php.*

Derecho de Rectificación, Madrid, Agencia Española de Protección de Datos Personales, 2014, *http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derechos/principales_derchos/rectificacion-ides-idphp.php.*

GURZA JAIDAR, Laura, "La protección de la privacidad en la era de la vigilancia masiva", ponencia dentro del panel 2, *Foro: La privacidad en la era digital,* 20 de octubre de 2015, *http://slideshowes.com/doc/1289603/panel-2-la-protecci%C3%B3n-de-la-privacidad-en-la-era-de-la.*

CAPÍTULO NOVENO
Creación de un nuevo órgano: Instituto Nacional para la Protección de Datos Personales

Ana Dorotea VÁZQUEZ[171]

SUMARIO

I. INTRODUCIÓN

La última década ha sido testigo de un cambio sustantivo de la Constitución mexicana, en particular, en materia de derechos fundamentales y en el diseño de sus mecanismos de garantía y protección. Las modificaciones más significativas se generaron en 2011 con dos reformas que, aunque independientes, vistas en conjunto transforman el rostro del sistema constitucional mexicano, al punto que constituyen un nuevo paradigma constitucional[172]. La primera de estas reformas, pu-

[171] Cuenta con más de cinco años de experiencia en el ámbito de la consultoría legal especializada en materia de protección de datos personales. Ha asesorado y litigado a favor de grandes clientes en esta materia, tales como bancos, aerolíneas, maquiladoras, aseguradoras, afianzadoras e instituciones educativas de alto prestigio. Ha sido coautora de dos publicaciones, entre las que se encuentra "Protección de datos personales: Guía para la adecuación normativa", publicada junto con el Banco Mundial, Secretaría de Economía y AMIPCI, lo cual le ha permitido participar activamente en múltiples iniciativas en materia de protección de datos, así como en la impartición de diversos cursos, capacitaciones y conferencias de la mano de NYCE, autoridad mexicana certificadora en dicha materia.

[172] Carbonell, Miguel, y Salazar, Pedro, *La reforma constitucional de derechos humanos: un nuevo paradigma*, México, IIJ-UNAM, 2011, p. 5.

blicada en el Diario Oficial de la Federación (DOF), el 10 de junio de 2011, modifica diversos Artículos constitucionales en materia de derechos humanos, en específico el numeral 1o. Desde esa fecha, ese precepto establece que: "Todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. En consecuencia, el Estado debe prevenir, investigar, sancionar y reparar las violaciones a los derechos humanos, en los términos que establezca la ley". La segunda reforma, publicada en el DOF en junio de 2011, modifica los Artículos 94, 103, 104 y 107 constitucionales y, con ello, transforma el juicio de amparo, que es el principal mecanismo de protección de los derechos fundamentales en el ordenamiento jurídico mexicano. La misma reforma modifica la estructura del Poder Judicial de la Federación, fortaleciendo el papel de la Suprema Corte de Justicia de la Nación como Tribunal Constitucional.

Estas dos reformas, completan un largo proceso de cambios constitucionales que han incorporado a nuestra Constitución nuevos derechos e instituciones para garantizarlos[173]. Cabe señalar, que la modificación al Artículo 6o. constitucional (publicada en el DOF el 20 de julio de 2007), que adicionó un segundo párrafo con siete fracciones a ese Artículo y que estableció el principio general de publicidad de la información gubernamental, el derecho de acceso a la información pública y la protección de los datos personales en posesión de los autoridades. Esta reforma sentó las bases para una nueva política de transparencia gubernamental del Estado mexicano, orientada a facilitar la rendición de cuentas de todas las autoridades en los diferentes órdenes de gobierno (federal, estatal y municipal)[174]. Una segunda reforma, publicada en el DOF el 1 de julio de 2009, modificó el Artículo 16 para elevar a garantía constitucional el derecho a la protección de datos personales, así como el acceso, rectificación, cancelación y oposición de los mismos. En relación con esta reforma, el 30 de abril de 2009 también se adicionó la fracción XXIX, inciso O, del

---

[173] Fix-Fierro, Héctor, y López Ayllón, Sergio, "La modernización del sistema jurídico (1970- 2010)", Servín, Elisa, *Del nacionalismo al neoliberalismo*, México, CIDE-FCE, 2010, p. 47-93.

[174] López Ayllón, Sergio *et. al*., *Hacia una política de rendición de cuentas en México*, México, Auditoría Superior de la Federación-CIDE-Red por la Rendición de Cuentas, 2011, p. 54.

Artículo 73 de la Carta Magna, para facultar al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares.

Todos estos cambios, sumados a la evolución y desarrollo del ejercicio de estos dos derechos en todo el país, obligan a una reflexión cuidadosa sobre el diseño institucional del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Este organismo, cuya contribución a la promoción y al ejercicio efectivo de estos derechos es nacional e internacionalmente reconocida[175], tiene un lugar y una función peculiar en el entramado institucional mexicano, que requiere ser revisada a la luz de los nuevos retos que deberá enfrentar en los próximos años.

En efecto, desde su origen, diversas voces consideraron que el INAI debió ser constituido como un órgano encargado únicamente de la materia de transparencia[176]. Con los años, se ha reiterado que el INAI debe dejar de ser un órgano encargado de proteger el derecho a la protección de datos personales, para garantizar dicho derecho es necesario la creación de un nuevo órgano, que tenga la capacidad de salvaguardar la garantía de la protección de datos personales en todo el país.

Lo anterior fundamentado en que actualmente, una sociedad en la que la información se traduce en poder, donde la capacidad de almacenamiento y de difusión de datos es cada vez mayor y que se ha dado reconocimiento constitucional alrededor del mundo al derecho a la autodeterminación informativa, nos enfrentamos a un grave problemas en cuanto a la protección de datos se refiere: la cual se traduce en una indebida utilización de los datos personales.

---

[175] Sobel, David L. *et. al*., *El Instituto Federal de Acceso a la Información Pública en México y la cultura de la transparencia*, Pennsylvania, Annanberg School for Communications-University of Pennsylvania, 2006, p. 316.

[176] Por ejemplo en la iniciativa de Ley de Acceso a la Información del llamado Grupo Oaxaca se consideraba la creación de un Instituto Nacional de Acceso a la Información. En el mismo sentido se pronunciaron varias organizaciones en la consulta que realizó el Ejecutivo Federal para la expedición de la Ley de Acceso a la Información. Véase López Ayllón, Sergio, *Globalización, Estado de derecho y seguridad jurídica. Una exploración sobre los efectos de la globalización en los Poderes Judiciales de Iberoamérica*, México, Suprema Corte de Justicia de la Nación, 2004, p.18 y ss.; Luna Pla, Issa, *Movimiento social del derecho de acceso a la información en México*, México, IIJ-UNAM, 2009, p. 133 y ss.

Es factible decir, que la sociedad no es ajena al tema del mal tratamiento de los datos personales. Si bien, todo aquel que trata datos personales está obligado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares –en el caso del sector privado– y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental –en el caso del sector público–, la realidad es que mucha gente no conoce el contenido de sus obligaciones. En este panorama, las medidas exigidas por la Ley para la protección de los datos personales, tanto humanas, como técnicas y administrativas, se vuelven, en el plano fáctico, fantasmas. Las transferencias no reguladas, las ventas ilegales de bases de datos, el uso indebido o excesivo de información que no cumple con los principios legales, entre otros, se han vuelto panoramas habituales para gente que, con fines comerciales o criminales, trata datos personales de terceros que están en su poder.

Se plantea, ante este escenario, la necesidad de una autoridad estatal especializada en materia de protección de datos personales que sea dotada, tanto de fuerza política, como jurídica, para hacer frente a este escenario.

En este contexto, el objetivo del presente trabajo es proponer una solución que resuelva los problemas antes mencionados y que permita un mayor control y legalidad en el tratamiento de los datos personales de los ciudadanos. Creando así el Instituto Nacional para la Protección de Datos Personales, especializado en el tema de protección de datos personales y dedicado exclusivamente a salvaguardar este derecho constitucional. Es decir, una autoridad que pueda hacer valer este derecho de manera más específica que el actual INAI.

A lo largo de este capítulo, se analizarán dos escenarios de transgresión a la normativa en materia de protección de datos personales, dando así el panorama necesario para la comprensión de la necesidad de creación de un nuevo órgano que proteja dicho derecho, el Instituto Nacional para la Protección de Datos Personales.

II. PROTECCIÓN DE DATOS PERSONALES: SOBRE LA PROBLEMÁTICA EN NUESTRO PAÍS

La indebida utilización de los datos personales es un problema al que estamos expuestos, o incluso hemos experimentado, muchos de cuantos proporcionamos nuestros datos personales, ya sea a entidades públicas o privadas. La situación es conocida, repetitiva y fatigante: al realizar actividades como hacer un trámite ante un ente público; al pedir un crédito en un banco; al inscribirse en algún club deportivo; al ingresar al hospital para una consulta; o al ingresar por primera vez como alumno a una institución educativa[177]; se solicita al titular una exhaustiva lista de datos personales que deben ser proveídos para poder seguir adelante con el proceso en cuestión. Muchas veces, incluso, encontramos que se piden datos personales a los que no se puede encontrar vínculo o utilidad con el propósito del servicio solicitado[178].

Siendo así sería factible que surgieran, en las personas que proporcionan su información a entes públicos y privados, preguntas tales como: ¿Para qué necesitan tal cantidad de datos míos? ¿Con qué motivo me están solicitando estos datos en específico? Posteriormente, ya que ha sido suministrada la información demandada, podrán surgir cuestionamientos como: ¿Qué pasará con la información que entregué? ¿Dónde se guardará? ¿Con quién se compartirá? ¿Con qué fines la usarán? ¿Está segura mi información?

La LFPDPPP ha sido desarrollada justamente teniendo en mente que el titular de los datos personales conozca las respuestas a este tipo de preguntas, mediante diversos mecanismos, como es la puesta a disposición del aviso de privacidad correspondiente. No obstante, si bien es cierto que la legislación ha buscado prevenir que sucedan ciertos escenarios de mala utilización de los datos personales, en la práctica, mucha de la información personal que es proporcionada a diversos responsables se encuentra, archivada o circulando, en condiciones poco controladas, sin contar con las medidas de seguridad necesarias y/o siendo objeto de usos diversos de aquellos para los que fue entregada originalmente.

[177] Entre otros muchos trámites, los mencionados solo buscan ser ejemplos ilustrativos.
[178] Por ejemplo, la inclusión del rubro "religión" en el formato de tratamiento de una clínica facial.

Esto es, existe en nuestro país un marco normativo encaminado a la protección de datos personales que no está siendo eficazmente aplicado por la autoridad. Se ejemplificarán, para objeto del presente trabajo, algunos escenarios comunes de transgresión a dicha normativa, bien con fines comerciales e incluso con fines criminales.

1. *Escenarios de transgresión a la normativa: con fines comerciales*

En las últimas décadas, con la creciente expansión de la tecnología y, por lo tanto, del acceso a la información por medios digitales, nació una nueva forma de hacer negocio para las empresas. Se trata de un estilo novedoso de mercadotecnia, que tiene como objetivo directo a consumidores específicos. Esto es posible mediante el uso de bases de datos personales que le permiten a las empresas en cuestión conocer con precisión los datos básicos de segmentación de clientes potenciales como son: edad, género, ubicación geográfica, nivel socioeconómico, gustos de consumo, marcas preferidas, entre otros, y tener comprensión de sus preferencias. Este tipo de información resulta muy valiosa para las empresas ya que es una herramienta fundamental en el desarrollo de productos y estrategias de ventas.

Comercialmente, esto parece sumamente atractivo para las empresas ya que, si se conoce al individuo en cuestión, es mucho más fácil saber cuándo, cómo y qué productos ofrecerle[179]. Así, por medio de técnicas estadísticas, se desarrollan modelos de comportamiento de los consumidores, las cuales son utilizadas posteriormente para crear una selección de clientes determinados a quienes hacerles comunicaciones específicas. El problema de dichas bases de datos, las cuales contienen información de miles de personas, que son archivadas en grandes almacenes de datos y cuya compraventa es no solamente usual, sino altamente lucrativa, es que en muchas ocasiones son obtenidas de manera ilegal, en violación de la Ley.

Cito a continuación la publicidad contenida en la página de Internet de una empresa dedicada a este negocio:

---

[179] Moreno Ramírez, Ileana, *Los órganos constitucionales autónomos en el ordenamiento jurídico mexicano*, México, Porrúa, 2005, p. 67.

> Disponemos actualmente con más de 50 millones de registros a nivel nacional e internacional, datos depurados y actualizados constantemente; de personas físicas, segmentados por nivel socioeconómico, edad, sexo, profesión, etc., así como bases empresariales segmentadas por giro, tamaño de empresa, rango de ventas anual, rango de trabajadores, tomadores de decisión, etc.
> Elige de entre nuestros paquetes especiales armados con registros de las principales segmentaciones y diferentes campos incluidos o solicita tu cotización de nuestras bases personalizadas, donde puedes elegir el perfil e información que incluya la base de datos según tu necesidad[180].

Cada persona y, por lo tanto, la información que le pertenece se traducen en bases de datos que, en conjunto con las de otros individuos, son bienes valiosos en el mercado datos como: nombre, ubicación, información de contacto, nivel de gasto, región geográfica del gasto, preferencias, opiniones políticas o religiosas, orientación sexual, orientación de consumo, entre muchos otros campos por enumerar, son datos personales que, si bien son propiedad única y exclusiva de la persona a quien corresponden, se han convertido en bienes intercambiables de gran atractivo, muchas veces incluso con el desconocimiento de los propietarios mismos de los datos.

Aunque se ha argumentado por diversos países y organizaciones que los individuos son libres de proporcionar o suprimir sus nombres y demás información personal contenidos en dichas bases de datos usadas para el marketing, lo cierto es que la práctica misma se encuentra viciada de origen siempre que la persona en cuestión no ha dado su consentimiento para el tratamiento de sus datos personales para estas finalidades en específico; o peor aún, si el tratamiento lo realiza un responsable con quien el titular jamás ha tenido contacto con anterioridad, o ante el cual jamás ha consentido el uso de dichos datos. Esta práctica, común hoy en día[181], es un ejemplo de la indebida utilización de los datos personales para fines comerciales.

Otra práctica habitual donde existe una indebida utilización de los datos personales con fines comerciales es el caso de la cobranza extrajudicial, cuya definición se tomará de lo referido directamente por la actual autoridad en materia

---

[180] Grupo Net K, TM., disponible en: *http://www.sihay.com.mx/empresa.php*.

[181] ¿Cuántas veces el lector ha recibido correos electrónicos, mensajes o llamadas de personas u organizaciones desconocidas a nosotros, que ofrecen servicios que jamás ha solicitado?

de protección de datos personales como "*actividad que realiza una entidad financiera, directamente o a través de un despacho de cobranza*[182]*, a fin de requerir el pago de las obligaciones contraídas por el deudor, o para negociar o reestructurar los créditos, préstamos o financiamientos*"[183].

Esta actividad se ha difundido en nuestro país y, como consecuencia, ha aumentado el número de las quejas presentadas ante la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef). Las personas han presentado reclamaciones específicas contra las actuaciones de los mencionados despachos de cobranza y, entre los años de 2011 y 2013, la Comisión recibió 100,391 quejas referentes a este tema en concreto[184]. Los reclamantes alegaban que recibían comunicaciones por parte de despachos de cobranza reclamando el pago de una deuda cuando, en la mayoría de los casos, la persona contactada no era ni siquiera el titular de la deuda, ni tenía relación alguna con la empresa acreedora de la deuda ajena; asimismo, los titulares demandaban la rectificación de dichas situaciones, dado que en muchas ocasiones incluso recibían maltratos verbales u ofensas por parte de los agentes de dichos despachos de cobranza, o bien les contactaban en relación a un crédito que había sido previamente liquidado. El estudio realizado por el INAI al respecto, externa que:

> … se observa que un alto porcentaje de las quejas recibidas involucra el tema de la protección de datos personales, ya que se infringen los principios garantes del derecho a la protección de datos personales, tal es el caso del principio de calidad, pues el hecho de que las personas contactadas no sean los deudores o que se reclame un crédito que ya ha sido pagado, conduce a que los datos personales en posesión de los Despachos de Cobranza o Entidades no son exactos, correctos, ni actualizados; así como el principio de información, ya que las personas contactadas no conocen la identificación de quienes realizan

---

[182] A su vez, definido por el INAI como: "Despacho externo, incluyendo a terceros o representantes, que realiza la cobranza, negociación o reestructuración de los créditos, préstamos o financiamientos, y que actúa como intermediario entre las entidades financieras y comerciales y el deudor, a fin de recuperar los adeudos de la entidad en cuestión".

[183] *Guía para orientar el debido tratamiento de datos personales en la actividad de cobranza extrajudicial*, Instituto Federal de Acceso a la Información Pública y Protección de Datos, p. 7, disponible en: *http://inicio.ifai.org.mx/nuevo/Gu%C3%ADa%20Cobranza%20Extrajudicial%20IFAI.pdf.*

[184] *Ibidem*, p. 9.

[185] *Idem.*

la gestión de cobranza…[185]

> Esta mala práctica es realizada con frecuencia, ya que las entidades financieras y comerciales buscan, como tienen derecho, que las deudas que los titulares tienen con ellos sean efectivamente pagadas. El problema es que, en el afán legítimo de gestionar el cobro de los adeudos de los que son acreedores, invaden la privacidad de las personas, violentan la esfera del titular, investigan y acosan a los titulares en sus hogares y trabajos, y violan, con todo esto, las disposiciones en materia de protección de datos personales vigentes en nuestro país.

El negocio de los despachos de cobranza consiste en cobrar un porcentaje de comisión por cada crédito que logra que pague el deudor. Asimismo, otro esquema usualmente utilizado es la compra de cartera vencida de las instituciones financieras a costos muy bajos; una vez adquirida, hacen todo en su poder para recuperar la deuda. Es evidente que para la realización de esta lucrativa actividad es necesario contar con bases de datos de los deudores y explotarlas a su mayor límite, con tal de lograr el objetivo de que el titular pague. No obstante, los alcances de los despachos se extienden en muchas ocasiones por encima de los límites de la ley: no solo investigan a la persona deudora, sino que van más allá y realizan actividades que vulneran su privacidad y la de quienes los rodean. Un ejemplo de esto sería el caso de los despachos de cobranza que averiguan los datos de contacto de gente cercana al deudor, con el objetivo de exponer la deuda ante sus conocidos, intimidarlo y avergonzarlo y, por medio de dichas vulneraciones a su esfera personal, lograr que pague la suma correspondiente[186].

En este panorama, como en el de marketing, los datos personales de los individuos se vuelven bienes valiosos a partir de los cuales se puede obtener un lucro significativo. Es cada vez más evidente la importancia que tiene la debida obten-

---

[186] Un escenario similar sucedió en el caso de denuncia que tuvo Radiomóvil Dipsa, S.A. de C.V. (Telcel) ante el IFAI (Expediente P.S.0026/13), donde el denunciante alegaba que la compañía había hablado al teléfono de su jefe en repetidas e insistentes ocasiones para exponer la deuda del empleado, acosándolo sin que el empleado hubiera proporcionado ese número telefónico, como número de referencia, en el contrato suscrito con Telcel; disponible en: *http://inicio.ifai.org.mx/pdf/resoluciones/2013/PS%2026.pdf*.

ción y tratamiento de los datos personales, al ser estos activos contables para las empresas, en sus actividades.

Ante esta problemática, la Condusef celebró un convenio con la Asociación de Profesionales en Cobranza y Servicios Jurídicos A.C. (APCOB)[187], en conjunto con el entonces IFAI, con el objetivo de fomentar que las prácticas de cobranza extrajudicial se realicen en todo momento con apego a los principios legales y se salvaguarde la integridad, la privacidad y la dignidad de los deudores.

Si bien hoy en día las malas prácticas de los despachos de cobranza están mucho más limitadas legalmente, también es cierto que existe una gran cantidad de situaciones que ocurren frecuentemente fuera de los límites de la ley que consisten en indebidos tratamientos de datos personales con fines comerciales y, como se verá a continuación, también con fines criminales, los cuales no han podido ser controlados por el INAI como órgano garante de un derecho fundamental.

2. *Escenarios de transgresión a la normativa: con fines criminales*

Algunos de los usos indebidos más comunes que se le da a la información personal hoy en día tienen que ver con objetivos que están fuera de lo legal. Ejemplos tales como accesos no autorizados, vulneraciones a las bases de datos, robo de información y robo de identidad son algunos ejemplos de negocios altamente lucrativos y preocupantemente cotidianos.

México ocupa el tercer lugar en América Latina de los países donde existe una mayor incidencia del delito de robo de identidad[188]. No obstante, nuestra normativa no contempla las medidas para impedir que los datos personales que son almacenados y tratados por los responsables sean utilizados para la comisión de delitos.

---

[187] Convenio de colaboración entre la Asociación de Profesionales en Cobranza y Servicios Jurídicos A.C. y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, disponible en: *http://www.condusef.gob.mx/PDF-s/marco_juridico/convenio_apcob_condusef.pdf*.

[188] Hernández, Gerardo, "Se disparan casos de robo de identidad", *El Siglo de Torreón*, 12 de mayo de 2015, Sección Finanzas, disponible en: *http://www.elsiglodetorreon.com.mx/noticia/1113934.se-disparan-casos-de-robo-de-identidad.html*.

Contrario a lo que se podría pensar, no solamente grandes empresas están expuestas a la indebida utilización de los datos personales para fines criminales, como son los robos de bases de datos, los ataques cibernéticos, los robos de identidad, entre otros. En el año 2014, más de una tercera parte de los ciberataques en México tuvo como objetivo a pequeñas y medianas empresas, dado que es más fácil vulnerar sus sistemas, teniendo en cuenta que destinan presupuestos muchos menores, comparados con las grandes empresas, a la protección de sus bases de datos[189].

Se trata de un negocio ilegal que es altamente redituable. Se estima que en 2013, el costo del crimen cibernético en México ascendió a montos superiores a tres mil millones de dólares[190]. En el ámbito internacional, el cibercrimen a nivel global genera pérdidas de entre 375 y 575 mil millones de dólares al año[191]. El problema ha ido incrementando descontroladamente, debido a la gran cantidad de medios electrónicos con los que contamos actualmente y la falta de regulación y de concientización al respecto en muchas partes del mundo. En 2014, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) recibió 547,104 casos de reclamaciones por fraudes relacionados a suplantaciones de identidad y robos de datos bancarios a través de Internet[192].

El robo de identidad implica que una persona asuma las cualidades informacionales de otra y/o se haga pasar por otra persona, lo que puede ser incluso mediante la obtención de datos biométricos como huellas dactilares o de iris, o mediante la apropiación de certificados digitales como son la firma electrónica o la FIEL del SAT, entre otros ejemplos, con el fin de obtener un lucro[193].

> El robo de identidad es considerado el delito del siglo, ya que las principales vías donde se regalan datos personales son las redes sociales con un 77% y las

[189] *Idem*.
[190] *Idem*.
[191] Castillo García, Gustavo, "Este sexenio la policía cibernética dice haber impedido delitos por más de $2 mil millones", *La Jornada*, 25 de febrero de 2015, Sección Política, disponible en: *http://www.jornada.unam.mx/2015/02/25/politica/022n1pol*.
[192] Gallo, Irma, "Crece robo de datos bancarios en internet", *El Universal,* 25 de mayo de 2015, Sección Nación, disponible en: *http://www.eluniversal.com.mx/nacion-mexico/2015/crece-robo-de-datos-bancarios-en-internet-1102453.html.*
[193] *Idem*.

> compras por internet con un 62%. De acuerdo con datos del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), Distrito Federal y Estado de México son los territorios en donde se concentra la mayor cantidad de denuncias[194].

Tenemos ahora un panorama mucho más amplio de lo que significa la problemática en México en cuanto a la protección y tratamiento de los datos personales. En este contexto, resulta pertinente para los fines del presente capítulo, proponer un cambio que logre transformar y mejorar las condiciones existentes y, de ese modo, sugerir un modelo que asegure realmente una eficaz y eficiente protección de los datos personales en nuestro país.

III. CREACIÓN DE UN NUEVO ÓRGANO

1. *Instituto Nacional para la Protección de Datos Personales*

Teniendo como objetivo principal de este apartado proponer una solución para la problemática hasta ahora descrita, que resulte eficiente, útil y concreta para el contexto analizado, nace la idea del Instituto Nacional para la Protección de Datos Personales (INPRODAP), como un órgano constitucional autónomo, independiente del INAI, especializado en el tema de protección de datos personales y dedicado exclusivamente a salvaguardar este derecho constitucional. Es decir, una autoridad que pueda hacer valer este derecho de manera más eficiente que el actual INAI.

Para poder explicar las razones por las cuales se considera que el INPRODAP debe ser un órgano constitucional autónomo, es necesario dar un contexto breve, a pesar de no ser el tema coral del presente trabajo, sobre la naturaleza de los órganos constitucionales autónomos.

2. *Naturaleza de un órgano constitucional autónomo*

Los órganos constitucionales autónomos encuentran su surgimiento después de la Segunda Guerra Mundial[195]. Su existencia deriva de un florecimiento histórico que

---

[194] Hernández, Diana, "Robo de identidad en la web, considerado el delito del siglo", *Proyecto 40*, 5 de junio de 2015, disponible en: *http://www.proyecto40.com/programa/informativo-40-con-lilly-tellez/nota/2015-06-05-12-00/rodo-de-identidad-en-la-web--considerado-el-delito-del-siglo/*.

[195] Roldán Xopa, José, *Derecho Administrativo,* México, Oxford, 2008, p. 34.

buscaba superar las teorías clásicas de la división de poderes, las cuales postulaban al interior de un Estado que solamente había tres esferas de poder: la ejecutiva, la legislativa y la judicial. Actualmente se entiende que dentro de un Estado puede haber esferas distintas a las anteriores, así como funciones que deban ser desempeñadas por órganos distintos a los tradicionales[196]. La realidad estatal actual, la cual se ha tornado cada vez más compleja, ha hecho nacer la necesidad de perfeccionar la actuación de los entes públicos y el repartimiento de las funciones entre ellos. En este contexto comienzan se crean los órganos constitucionales autónomos.

El jurista y politólogo español, Manuel García Pelayo[197], expone que las características de los órganos constitucionales autónomos son las siguientes:

a) Se configuran inmediatamente por la Constitución. Es el propio texto constitucional el que prevé su existencia, determina su composición, los métodos de designación de sus integrantes, su estatus institucional y sus competencias principales. Esto es, cuentan con una esfera de atribuciones constitucionalmente determinada, lo cual significa una "garantía institucional" que tiene como resultado que tal esfera se encuentre fuera del alcance del legislador ordinario.
b) Tienen incidencia en la formación de la voluntad estatal, ya sea en los procesos de toma de decisiones o en la solución de conflictos al interior del Estado, por lo que llevan a cabo funciones esenciales dentro de los Estados modernos.
c) Se ubican fuera de la estructura orgánica de los poderes tradicionales. Esta característica es relevante, ya que significa que los órganos constitucionales autónomos no se adscriben orgánicamente a ninguno de los tres poderes clásicos; es decir, no forman parte de la Administración Pública, el Poder Legislativo ni del Poder Judicial. Su independencia orgánica se exterioriza a través de elementos como la ausencia de controles burocráti-

[196] Dromi, Roberto, *Tratado de Derecho Administrativo*, Buenos Aires, FDA, 2006, t. 4, p. 40.
[197] García Pelayo, Manuel, *Las transformaciones del Estado contemporáneo,* Madrid, Alianza, 1993.

cos, como por la existencia de una cierta independencia financiera a favor del órgano constitucional[198].

d) Cuentan con una igualdad de rango con los demás órganos y poderes, de modo que no se encuentran subordinados a ellos. Esto, sin perjuicio de que las decisiones de los órganos constitucionales autónomos puedan ser revisables, por ejemplo, por el Poder Judicial.

Habida cuenta que se propone que el INPRODAP sea un órgano constitucional autónomo, es preciso comentar brevemente las razones principales por las que dichos órganos encuentran motivada su creación. Entre ellas, están las siguientes dos razones:

a) Surgen de la necesidad de desarrollar funciones nuevas y complejas que el Estado no realizaba en tiempos anteriores y que por sus características no pueden llevar a cabo los órganos circunscritos en las teorías clásicas de la división de poderes[199]; y

b) Pueden surgir por cuestiones circunstanciales de un Estado, determinadas por necesidades particulares del momento político y/o histórico[200].

---

[198] De otra forma, la independencia orgánica podría verse fácilmente vulnerada a través de la asfixia en el suministro de los recursos económicos. La obligación para el legislador de otorgar los fondos necesarios para el desempeño de las funciones de los órganos constitucionales autónomos forma parte de una "garantía institucional" que la Constitución les asegura, pues no se trata solamente de tener un ámbito de competencias constitucionalmente determinado, sino también de que ese ámbito cuente con los medios suficientes para poder ser actuado y actuable en la realidad cotidiana del Estado.

[199] García de Enterría, Eduardo, y Fernández, Tomás Ramón, *Curso de Derecho Administrativo II*, 8ª. ed., Madrid, Civitas, 2002, p. 82.

[200] Un ejemplo de esto es el surgimiento de la Comisión Nacional de Derechos Humanos (CNDH) en 1990, la cual surge a partir de la necesidad de contar con un mecanismo no jurisdiccional de protección de los derechos humanos. El caso de la CNDH muestra que el surgimiento de un órgano constitucional autónomo puede darse también como una forma de evolución institucional. La Comisión surgió primeramente como un órgano con autonomía de decisión, pero adscrito orgánicamente a la Secretaría de Gobernación del Poder Ejecutivo Federal (en 1990) y posteriormente evolucionó su naturaleza jurídica para ser reconocido como órgano constitucional autónomo (primero en 1992, pero plenamente hasta 1999). Este ejemplo es relevante debido a que demuestra que los órganos públicos pueden evolucionar en la medida en que surgen nuevas necesidades de diseño institucional para llevar a cabo de manera plena su trabajo.

Luego de este breve repaso general, conviene pasar a analizar las razones que justifican la autonomía constitucional del órgano propuesto, el INPRODAP.

IV. LA AUTONOMÍA CONSTITUCIONAL DEL INPRODAP

Los derechos humanos o derechos fundamentales evolucionan incesablemente. Históricamente, es viable comprobar una tendencia hacia el perfeccionamiento y ampliación de las normas mediante las cuáles se reconocen dichos derechos, así como hacia el fortalecimiento de los dispositivos legales y estatales mediante los cuales se les brinda protección. Este fenómeno se ha materializado en una tendencia prevaleciente de ampliar el conjunto de los derechos humanos y fortalecer los instrumentos que les otorgan protección y garantía. En nuestro país, no solamente se han integrado nuevos derechos al ordenamiento nacional, sino que también hemos sido testigos de un continuo perfeccionamiento de las instituciones y los instrumentos de garantía de los mismos.

En esta línea, según lo establecen los autores Marco Aparicio Wilhelmi y Gerardo Pisarello[201], es posible afirmar que un derecho humano cuenta con dos tipos de garantías: las primarias y las secundarias. Las garantías primarias se denotan cuando dichos derechos son expresamente reconocidos en algún ordenamiento jurídico, el cual puede ser la Constitución misma, un tratado internacional o, incluso, una Constitución estatal o una ley general [202]; esto es, la garantía primaria es reflejo de la decisión del legislador de incluir dicho derecho en una norma con alto rango dentro del ordenamiento jurídico. Las garantías secundarias de los derechos humanos se refieren a la creación de mecanismos jurídicos e institucionales adecuados para protegerlos. Esto es, que los titulares de dicho derecho los puedan invocar ante la autoridad para que se adopten medidas de control, de reparación o de sanción que tutelen su ejercicio[203]. Dichos mecanismos de protección, o garantías

---

[201] Aparicio Wilhelmi, Marco, y Pisarello, Gerardo, *Los derechos humanos y sus garantías: Nociones básicas,* disponible en: *http://miguelcarbonell.com/artman/uploads/1/Aparicio_y_Pisarello_DD_HH_y_Garantias.pdf*.

[202] Como es el caso del derecho a la protección de los datos personales.

[203] Roberts, Alasdair, "La lucha por gobiernos abiertos", en Sandoval, Irma (coord.), *Corrupción y transparencia,* México, UNAM-Siglo XXI, 2009, p. 92.

secundarias, pueden ser de orden jurisdiccional o no jurisdiccional, dependiendo de su naturaleza y la del órgano encargado de ejercerlos. En el caso de las no jurisdiccionales, las ejercen autoridades de naturaleza administrativa que, finalmente, son instituciones que complementan el sistema de garantías mediante mecanismos administrativos de protección de derechos.

El INPRODAP es propuesto como un órgano de garantía secundaria del derecho humano o fundamental que es el derecho de protección de datos personales. Considero que debe tratarse de una autoridad administrativa, como lo es actualmente el INAI, que encuentre su fundamento constitucional en el Artículo 6o. de la Carta Magna, el cual establece, en su fracción VIII que:

> La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho… A la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

Este imperativo constituye el sustento constitucional para la existencia del INPRODAP. La autonomía institucional propuesta surge por la necesidad de brindar garantías efectivas a los derechos fundamentales a la protección de datos personales ya que, actualmente, el actual INAI no ha demostrado contar con la capacidad fáctica necesaria para dotar de garantías efectivas al derecho humano que nos atañe en este trabajo.

El derecho a la protección de los datos personales se encuentra en una etapa de maduración que demanda un fortalecimiento de la institución de garantía encargada de brindarle protección. Desde mi punto de vista, el actual INAI, dada su articulación dual en cuanto a sus ámbitos de competencia[204], no ha resultado suficiente para garantizar el desempeño que ese Instituto está destinado a realizar. Así las cosas, considero que el INPRODAP requiere de la misma naturaleza jurídica del INAI para poder realizar sus funciones en el contexto ante el cual nos enfrentamos.

---

[204] Acceso a la Información, por un lado, y protección de datos personales, por el otro.

La autonomía constitucional es una condición necesaria para garantizar que la función que encomendada al INPRODAP se realice con independencia e imparcialidad políticas, dado que un órgano de control y garantía como este requiere de un ámbito de decisión y operación propios para poder realizar su labor frente al gobierno. Es decir, resulta indispensable que se garantice la capacidad efectiva de control frente a los otros poderes estatales y, en general, ante cualquier autoridad, entidad, órgano y organismo, así como también ante poderes y entes privados. Esta situación hace menester una naturaleza constitucional de este tipo, debido a que la tarea de hacer valer este derecho fundamental debe estar caracterizada por la imparcialidad, la independencia y la especialización.

Así, la autonomía constitucional propuesta supone una garantía, tanto del derecho humano a la protección de los datos personales, como de la institucionalidad estatal de dicho órgano. Considero que la labor del INPRODAP no debe prestarse a interpretaciones de índole política o partidistas. De esta manera, las decisiones tomadas en esta materia seguirán siendo responsabilidad exclusiva de los directivos del INPRODAP (actualmente llamados "Comisionados", en el caso del INAI) sin que esta pueda ser atribuida a otros poderes públicos.

Siendo esto, se propone en el presente trabajo que la promoción, protección y garantía del derecho a la protección de los datos personales corresponda constitucionalmente al INPRODAP, no obstante que constituya una obligación a cumplir por todos los órganos del Estado mexicano.

Conviene recordar el derecho a la protección de los datos personales es un derecho fundamental de la persona cuya protección se asigna, en la presente propuesta, al INPRODAP. En el caso de la protección de datos personales la relación jurídica primaria se da entre privados: el titular del dato y el responsable del tratamiento de los datos. El INPRODAP se colocaría, como sucede actualmente con el INAI, como un tercero que resuelve, mediante un procedimiento administrativo seguido en forma de juicio, aunque sin tener carácter jurisdiccional, sobre las posibles afectaciones de los datos personales de una persona.

Que el INPRODAP, como órgano administrativo, sea el encargado de resolver sobre los procedimientos de protección de datos personales implica la asigna-

ción de una función relevante a su cargo, que si bien comprende el ámbito privado en que se desenvuelven dichos derechos, considera que los mismos tienen también una función de orden público. Este panorama envuelve el bien jurídico tutelado en una doble dimensión: la de ser un derecho de la persona y en la cual hay un ámbito de disponibilidad y, a la vez, un ámbito de orden público que debe ser protegido más allá del interés de los titulares de los datos. Dicho ámbito de orden público debe advertir, a la vez, la dimensión de actuación del INPRODAP, como es la posibilidad de actuar de oficio en los procesos de verificación y de imposición de sanciones con la que cuenta el INAI. En cuanto a los procedimientos ARCO, tanto la estructura del modelo actual del INAI como instancia administrativa de primer nivel, como sus procedimientos y los medios de defensa contra sus resoluciones, no se verían afectadas en el modelo del INPRODAP.

La reforma constitucional del 20 de julio de 2007 al Artículo 6o. constitucional significó un enriquecimiento jurídico del diseño constitucional del órgano garante de los derechos consagrados en dicho artículo. En específico, conviene observar el precepto en su fracción VIII, la cual establece:

> La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento de… la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley...

La fracción anterior se refiere a ciertas características asignadas al órgano garante. La primera de ellas que podemos comentar es la especialización, que significa que el órgano tenga como única función, en el caso del INPRODAP, la materia de la protección de datos personales. Otra característica relevante es la autonomía, que busca impedir la subordinación jurídica, orgánica y/o política a cualquier otra autoridad en el ámbito de su competencia.

Asimismo, la reforma a los Artículos 16 y 73, fracción XXIX-O constitucionales, los cuales reconocen el derecho a la protección de los datos personales como un derecho fundamental de todos los mexicanos, en concordancia con la expedición

de la LFPDPPP, por parte del Poder Legislativo el 5 de julio de 2010 en el DOF, fungen como base para el marco competencial del INPRODAP. De acuerdo con la LFPDPPP corresponde al actual INAI ser la autoridad de control, supervisión y garantía del derecho que nos concierne. En esta misma línea, en el Artículo 39, en sus fracciones II, IV y X, se establece que el INAI tiene entre sus atribuciones: interpretar en el ámbito administrativo la referida Ley; emitir criterios y recomendaciones para su funcionamiento y operación; así como desarrollar, promover y publicar análisis, estudios e investigaciones en materia de protección de datos personales en posesión de los particulares. En la propuesta actual, se propone que el INPRODAP conserve estas mismas atribuciones del INAI.

Dicho lo anterior, la propuesta del INPRODAP como un órgano con autonomía constitucional parece adecuada, de modo que se constituya como un organismo especializado e imparcial, con autonomía operativa, de gestión y decisión, con plena autonomía presupuestaria, que como hemos visto es una característica propia de los órganos constitucionales autónomos, que haga valer de manera efectiva el derecho a la protección de los datos personales.

En este punto, se tomarán en cuenta las funciones que le han sido atribuidas al INAI por la LFPDPPP, con la idea en mente de que el INPRODAP ejerza dichas funciones en materia de protección de datos personales. En este sentido, específicamente, los Artículos 38 y 39 de la Ley versan sobre las atribuciones del órgano garante:

> Artículo 38. El Instituto, para efectos de esta Ley, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.
>
> Artículo 39. El Instituto tiene las siguientes atribuciones:
>
> I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;
>
> II. Interpretar en el ámbito administrativo la presente Ley;

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

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

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

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

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

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

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

X. Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes;

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

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

Partiendo de un análisis de los fragmentos normativos antes expuestos, podemos dividir las funciones del órgano garante en cuatro clasificaciones o tipos: *a)* funciones resolutivas y reguladoras, *b)* funciones de supervisión y vigilancia, *c)* funciones de promoción y difusión y, por último, *d)* funciones operativas y administrativas. Hablando de las primeras, cabe decir que las funciones resolutivas y reguladoras son pieza fundamental para garantizar el derecho la protección de datos personales, ya que son clave para lograr aterrizar los esfuerzos hacia la protección del bien jurídico, mediante las resoluciones emitidas para los casos concretos, así como la expedición de lineamientos, recomendaciones, parámetros, etc. El órgano garante crea constantemente normas jurídicas individualizadas que establecen derechos y obligaciones a favor o a cargo de personas concretas (por ejemplo, entre el titular y el responsable de los datos personales), para los casos específicos en

que sea necesario hacer valer la tutela de la protección de los datos personales. Asimismo, como hace actualmente el INAI, el INPRODAP tendrá la capacidad de emitir normas jurídicas generalizadas y especializadas en materia de protección de datos personales, en específico para quienes se encuadren en los supuestos de las mismas[205].

La función de supervisión y vigilancia es esencial para impulsar avances en el cumplimiento efectivo de la normativa en materia de protección de datos personales. Se prevé que el INPRODAP sea la autoridad responsable de vigilar por el cumplimiento de las normas aplicables, por lo que es necesaria esta función para poder revisar, inspeccionar y vigilar a los responsables de los datos personales de los titulares, ya sea bien por iniciativa propia, o siguiendo los procedimientos iniciados por los mismos titulares.

La función de promoción resulta también esencial, en este caso para fomentar y difundir los beneficios del derecho a la protección de los datos personales, e impulsar una cultura donde, por un lado, los responsables conozcan y respeten sus obligaciones en la materia, evitando prácticas al interior de las organizaciones que mermen el derecho de los titulares. Por el otro lado, importa que se fomente una cultura en los titulares de los datos personales, donde conozcan los derechos con los que cuentan en este sentido, y los medios para hacer valer dichos derechos en cualquier momento. Este punto incluye la difusión del derecho protegido, capacitaciones, proporcionar apoyo técnico en el tema a quien lo solicite, elaborar investigaciones para ampliar el conocimiento del derecho a la protección de los datos personales, colaborar internacionalmente con organismos dedicados al tema, etc. Parece muy importante esta función, dado que tal parece que la efectividad con que se protege un derecho, tiene que ver con la internalización y el conocimiento de tal derecho por parte de los titulares que demandan y reclaman la observancia del mismo.

---

[205] Un ejemplo de esta normativa especializada, emitida por el INAI, son las "Recomendaciones en Materia de Seguridad de Datos Personales", publicadas en DOF el 30 octubre 2013.

El cuarto tipo de funciones, aquellas que se refieren a la operación y administración, son necesarias para asegurar el correcto funcionamiento del órgano regulador, bien en lo referente al funcionamiento del mismo, como a temas monetarios y presupuestales. Es decir, esta función se refiere a la gestión de los recursos humanos, financieros, generales, informáticos, jurídicos y de seguridad del órgano garante para que, efectivamente, pueda cumplir con las demás funciones antes mencionadas.

Con base en lo anterior se puede concluir que México necesita contar con un órgano constitucional autónomo que garantice el cumplimiento eficaz del derecho humano de acceso a la protección de datos personales, para lo cual es necesario la creación de un nuevo órgano, denominado Instituto Nacional para la Protección de Datos Personales, pues el INAI ha demostrado su ineficacia al momento de ejercer sus obligaciones de garantizar dicho derecho humano.

V. CONCLUSIONES

Muy brevemente, las conclusiones y recomendaciones que se desprenden del estudio que antecede se pueden sintetizar de la siguiente manera:

PRIMERA. La reforma constitucional de 2011 en materia de derechos humanos, así como la evolución que ha seguido el Instituto Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) partir de su creación, requiere una nueva y profunda reflexión sobre el actual diseño institucional de dicho organismo, a fin de que pueda seguir cumpliendo cabalmente con su mandato constitucional como garante de los derechos de acceso a la información pública y de protección de los datos personales.

SEGUNDA. En ningún momento de la historia de la humanidad, el tema de la protección de los datos personales ha sido tan relevante como lo es en la actualidad. En la era digital, en la cual nos hallamos, tanto la obtención como el almacenamiento de la información concerniente a las personas, sus gustos, hábitos, datos financieros, etc., son aspectos esenciales para el funcionamiento de los mercados, los gobiernos, sistemas de producción, de comercio y para múltiples otras esferas de la vida diaria.

TERCERA. Debido al gran avance de la tecnología y a la gran cantidad de información que constantemente divulgamos de nosotros mismos, muchas veces incluso sin saberlo, es altamente probable que exista, tanto almacenada como circulando, más información sobre un individuo de la que este tiene conocimiento. Hoy en día los datos personales de millones de titulares son utilizados por todo tipo de empresas, desde aseguradoras y bancos, hasta empresas de redes sociales, motores de búsqueda, empresas dedicadas al análisis de otorgamiento de créditos, etcétera. Este uso indiscriminado de la información personal atenta contra nuestra privacidad y contra nuestra autodeterminación informativa. Los datos personales han cobrado tanto interés que ha requerido que se regule el uso que se hace de estos datos. Es así como observamos, en primer lugar, que nos vemos ante la necesidad imperiosa de proteger los datos personales.

CUARTA. Se considera relevante la propuesta de una autoridad especializada en la materia, dado que actualmente no contamos en México con una cuya vocación esté integralmente enfocada al tema de protección de datos personales, sino que se dedica también, en la misma medida, a velar por la transparencia gubernamental que, como se ha visto, es un tema coralmente diverso.

QUINTA. La actual división de tareas para el INAI deviene lógicamente en una especialización menos enfocada al tema que nos avoca, debido a que la autoridad se ve en la necesidad de dividir tiempos, esfuerzos y recursos humanos y materiales, en atender y garantizar a los ciudadanos sus derechos en dos materias sustancialmente distintas. Lo anterior puede dar lugar también a que exista actualmente una indebida utilización de los datos personales, dado que es posible que aquellos que malversan con las bases de datos y cometen tratamientos indebidos con ellas, tanto para fines comerciales como criminales, se sientan en mayor libertad de trasgredir la esfera jurídica de los titulares de los datos personales, por no considerar alta la probabilidad de que la autoridad actual, con la gran carga de trabajo que tiene y los recursos divididos como están, llegue a detectar, y por lo tanto, menos aún, a perseguir dichas actividades. Es por esto que se considera útil crear un órgano independiente que se especialice en el tema de protección de datos personales y haga valer efectivamente este derecho constitucional.

SEXTA. La propuesta que se hace en el presente capítulo en relación a la creación de un órgano constitucionalmente autónomo, toma sentido por la indebida utilización de los datos personales, tanto por organismos públicos como privados. Se plantea esa naturaleza jurídica, bien por la desconfianza de la división de los poderes, pero sobre todo por la necesidad de tener un organismo especializado, el cual responderá a las necesidades actuales a las que nos enfrentamos y a los nuevos retos que se presentan en la vida cotidiana, en materia de protección de datos personales.

VI. FUENTES DE INFORMACIÓN

APARICIO WILHELMI, Marco, y PISARELLO, Gerardo, *Los derechos humanos y sus garantías: nociones básicas,* disponible en: *http://miguelcarbonell.com/artman/uploads/1/Aparicio_y_Pisarello_DD_HH_y_Garantias.pdf*.

CARBONELL, Miguel, y Salazar, Pedro, *La reforma constitucional de derechos humanos: un nuevo paradigma*, México, IIJ-UNAM, 2011.

CASTILLO GARCÍA, Gustavo, "Este sexenio la policía cibernética dice haber impedido delitos por más de $2 mil millones", *La Jornada*, 25 de febrero de 2015, Sección Política, *http://www.jornada.unam.mx/2015/02/25/politica/022n1pol.*

Convenio de colaboración entre la Asociación de Profesionales en Cobranza y Servicios Jurídicos A.C. y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros, *http://www.condusef.gob.mx/PDF-s/marco_juridico/convenio_apcob_condusef.pdf.*

DROMI, Roberto, *Tratado de Derecho Administrativo*, Buenos Aires, FDA, 2006, t. 4.

FIX-FIERRO, Héctor, y LÓPEZ AYLLÓN, Sergio, "La modernización del sistema jurídico (1970- 2010)", SERVÍN, Elisa, *Del nacionalismo al neoliberalismo*, México, CIDE-FCE, 2010.

GALLO, Irma, "Crece robo de datos bancarios en internet", *El Universal,* 25 de mayo de 2015, Sección Nación, *http://www.eluniversal.com.mx/nacion-mexico/2015/crece-robo-de-datos-bancarios-en-internet-1102453.html.*

GARCÍA DE ENTERRÍA, Eduardo y FERNÁNDEZ, Tomás Ramón, *Curso de Derecho Administrativo II*, 8ª. ed., Madrid, Civitas, 2002.

GARCÍA PELAYO, Manuel, *Las transformaciones del Estado contemporáneo,* Madrid, Alianza, 1993.

Guía para orientar el debido tratamiento de datos personales en la actividad de cobranza extrajudicial, Instituto Federal de Acceso a la Información Pública y Protección de Datos, *http://inicio.ifai.org.mx/nuevo/gu%c3%ada%20cobranza%20extrajudicial%20ifai.pdf.*

HERNÁNDEZ, Diana, "Robo de identidad en la web, considerado el delito del siglo", *Proyecto 40*, 5 de junio de 2015, *http://www.proyecto40.com/programa/*

informativo-40-con-lilly-tellez/nota/2015-06-05-12-00/rodo-de-identidad-en-la-web--considerado-el-delito-del-siglo/.

HERNÁNDEZ, Gerardo, "Se disparan casos de robo de identidad", *El Siglo de Torreón,* 12 de mayo de 2015, Sección Finanzas, *http://www.elsiglodetorreon.com.mx/noticia/1113934.se-disparan-casos-de-robo-de-identidad.html*.

LÓPEZ AYLLÓN, Sergio *et. al*., *Hacia una política de rendición de cuentas en México*, México, Auditoría Superior de la Federación-CIDE-Red por la Rendición de Cuentas, 2011.

LÓPEZ AYLLÓN, Sergio, *Globalización, Estado de derecho y seguridad jurídica. Una exploración sobre los efectos de la globalización en los Poderes Judiciales de Iberoamérica*, México, Suprema Corte de Justicia de la Nación, 2004.

LUNA PLA, Issa, *Movimiento social del derecho de acceso a la información en México*, México, IIJ-UNAM, 2009.

MORENO RAMÍREZ, Ileana, *Los órganos constitucionales autónomos en el ordenamiento jurídico mexicano*, México, Porrúa, 2005.

ROBERTS, Alasdair, "La lucha por gobiernos abiertos", en SANDOVAL, Irma (coord.), *Corrupción y transparencia*, México, UNAM-Siglo XXI, 2009.

ROLDÁN XOPA, José, *Derecho Administrativo*, México, Oxford, 2008.

SOBEL, David L. *et. al*., *El Instituto Federal de Acceso a la Información Pública en México y la cultura de la transparencia*, Pennsylvania, Annanberg School for Communications-University of Pennsylvania, 2006.

CAPÍTULO DÉCIMO
Drones (RPAS) y protección de datos

Rodrigo SOTO-MORALES[206]

SUMARIO

I. LA CONDICIÓN JURÍDICA DE LOS RPAS (DRONES)

Las aeronaves piloteadas a distancia comúnmente conocidas como drones son ya un fenómeno aeronáutico extendido tanto a cargo de la Aviación de Estado como de la Aviación Civil, es decir, al alcance de todos: grandes o pequeños operadores, agencias de gobierno o particulares. Los hay grande, medianos y pequeños.

[206] Abogado y Doctor en Filosofía Política. Su ejercicio profesional se despliega principalmente en las especialidades de Derecho Aeronáutico, Derecho Administrativo y Constitucional. Ha sido Coordinador General de la Licenciatura en Derecho de la Universidad Panamericana, campus Guadalajara. Actualmente es profesor asociado en la Universidad Panamericana, campus Ciudad de México, impartiendo las materias de Derecho Aeronáutico y Derecho de la Seguridad Nacional. Es profesor invitado del Colegio de Defensa Nacional (SEDENA, Popotla, Ciudad de México), es profesor del Posgrado en Derecho Aeroportuario de la Universidad Aeronáutica de Querétaro (UNAQ). Es miembro plenario de la Asociación Latinoamericana de Derecho Aeronáutico y Espacial (ALADA), con sede en Buenos Aires, Argentina. Es miembro de la Barra Mexicana de Abogados, asimismo, es miembro del Air and Space Law Forum, de la International Section y del México Committee de la American Bar Association (ABA), de los Estados Unidos de América. Certificado por la IATA en Derecho Internacional Aeronáutico (compraventa y arrendamiento de aeronaves, Derecho Internacional Aéreo, seguros de aeronaves y financiamiento, y contratos de aerolíneas).

Por sus siglas en inglés, los drones son conocidos como RPAS (*Remotely Piloted Aircraft).* Y esto no es cosa menor, pues de su denominación en inglés, la configuración de la doctrina y marco jurídico que regule estas operaciones depende de su "configuración ontológica" para la ciencia del derecho, esto es, su denominación se vuelve constitutiva de su ser jurídico.

Lo anterior es así, dado que para su correcta regulación se debe comenzar por aclarar, ¿qué es un dron? Un dron es antes que nada una aeronave. Una aeronave, puede definirse como *un aparato o máquina diseñada para poder sustentarse en el aire capaz de trasladarse a través del aire de un punto a otro de forma autónoma y segura.* La sustentación y el desplazamiento, a través del aire de forma segura, son elementos materiales esenciales para calificar a un objeto que surca espacio aéreo como una aeronave. La finalidad, tal como el transporte de personas, carga o correo, la fotografía, medición o vigilancia, son elementos secundarios a este. Debido a que las posibilidades técnicas que los RPAS representa y tienen cara al futuro, pueden llegar a ser tan variadas y numerosas que resultaría difícil limitarlas.

Donald H. Bunker señala, que al abordar el objeto desde el punto de vista de su estatuto jurídico para su venta y arrendamiento, una aeronave es:

> … un bien mueble móvil y es un artículo de propiedad personal… o cualquier máquina que pueda derivar el apoyo en la atmósfera de las reacciones que su diseño provoca en el aire, así como de las reacciones del aire contra la superficie de la tierra… El Diccionario Aeroespacial de Jane define a la aeronave como un dispositivo diseñado para mantenerse en la atmósfera sobre la superficie de la tierra a la que puede estar unido por una correa que no ofrece soporte…[207]

En ese sentido, Mario Folchi señala que: "en el conjunto de las instituciones típicas del Derecho Aeronáutico, la aeronave ocupa un lugar preponderante, por la sencilla razón de que es el aparato que realiza, en esencia, la actividad aeronavegatoria"[208].

---

[207] *International Aircraft Financing*, Montreal, International Air Transport Association, 2005, pp. 34-35. La traducción es del autor.

[208] Folchi, Mario, *Tratado de Derecho Aeronáutico y política de la aeronáutica civil*, Buenos Aires, Astrea, 2015, t. I, p. 283.

De este modo, un dron no se sustrae del marco jurídico convencional que el Derecho Aeronáutico le aplica al concepto de aeronave. No obstante, existen aparatos de tamaño diminuto, su operación cara a la seguridad operacional (*safety*) y a la seguridad pública (*segurity*), extraña responsabilidades legales de ámbito civil, administrativo y en algunos casos en materia penal. No solo por los daños, riesgo o amenazas que pudieran generar, sino porque uno de los usos más habituales para estas aeronaves es la video filmación, transmisión y fotografía de imágenes, constituyéndose también en un evidente invasor de la privacidad, propiedad privada, imagen e intimidad.

De ahí, surge la necesidad de contemplar el tema de la transparencia y la protección de datos, imagen e intimidad personal que pudieran ser transgredidos por la operación de estos aparatos.

Es importante asentar la doctrina jurídica al respecto del concepto de "dron", quedando identificado y definido en el Convenio de Chicago de 1944[209], ya que actualmente existe una referencia, un tanto vaga, en su Artículo 8o. con relación a las aeronaves sin piloto, pero para efectos de un vuelo internacional, sin establecer criterios para su naturaleza o concepción jurídica, por lo que, derivado de una interpretación laxa y sistemática, al no distinguir el texto del tratado, es posible asumir el tratamiento análogo a cualquier otro tipo de aeronave de las que se refiere el tratado tanto en su texto principal como en los anexos.

De esta forma, los países van abordando el tema con lentitud –si se toma en cuenta la velocidad con la que el mercado de estos aparatos se ha desarrollado–, falta unificación de criterios, aunque las coincidencias suelen darse en los siguientes aspectos, con miras a la seguridad operacional:

a) Clasificar los aparatos según su tamaño y peso;
b) Registrar los aparatos, con obligación bajo pena de sanción administrativa en caso de no hacerlo, a partir de determinando tamaño y peso;

---

[209] El Convenio de la Aviación Civil Internacional, mejor conocido como *Convenio de Chicago*, es el tratado que regula a nivel internacional la aviación civil. Fue firmado el 7 de diciembre de 1944 en la ciudad de Chicago, Ilinois, Estados Unidos de América. Consta de 191 Estados parte.

c) Delimitación e identificación de zonas prohibidas; y
d) Certificación y habilitación, es decir, necesidad de contar con licencia para operarlos, a partir de determinado tamaño y peso.

Lo anterior con miras a controlar y disminuir los riesgos de daños a terceros en la superficie.

En el caso de México, la operación de drones está regida solo mediante un ordenamiento administrativo de tipo "circular", por lo que urge robustecer el sistema jurídico para regular la correcta utilización de drones y garantizar la seguridad de los usuarios y terceros. Recientemente, la Secretaría de Comunicaciones y Transportes (SCT), a través de la Dirección General de Aeronáutica Civil (DGAC), anunció la implementación de nuevos instrumentos normativos que buscan regular el uso de RPAS en el espacio mexicano. La Circular obligatoria CO AV-23/10 es la norma vigente desde 2010 en este caso, la cual señala los procesos para el registro de drones y de sus usuarios autorizados, quienes luego de completar los requisitos indicados, obtienen la licencia de piloto certificado de RPAS[210].

Se considera que esta forma de regular en México es incorrecta y la regulación sobre drones merece un lugar dentro de la *Ley de Aviación Civil,* puesto que el espacio aéreo que utilizan estas aeronaves es un área de competencia federal. Lo anterior, siguiendo la definición de circular que propone Martínez Morales:

> La circular es "un documento interno por el cual se transmiten orientaciones, aclaraciones, información o interpretación legal o reglamentaria del funcionario jerárquicamente superior a los subordinados; dichos documentos disponen la conducta por seguir respecto de ciertos actos o servicios.
>
> En la escala jurídica, la circular está abajo de la ley y el reglamento, pero antes del acto concreto; es, básicamente, de naturaleza interpretativa. Según Maurice Boujol, las circulares pueden ser interpretativas, de carácter interno o reglamentario; éstas últimas son inadmisibles en Derecho mexicano[211].

---

[210] El 25 de julio de 2017, este documento alcanzó su cuarta revisión y por lo tanto se le denomina R4; clasifica a los drones conforme a su peso y uso, establece algunas pautas generales de operación, como la restricción de vuelo cerca de aeródromos, helipuertos y otros lugares públicos, o la limitación al transporte de ciertos objetos o mercancías, entre otras.

[211] Martínez Morales, Rafael I., *Diccionario de Derecho Administrativo y Burocrático*, México, Oxford, 2008.

Tratándose de este tipo de aeronaves, un marco jurídico mínimo podría consistir en un apartado dentro de la Ley de Aviación Civil que, mediante generalidades, establezca los principios que deben regir el accionante de los usuarios de RPAS, quienes hoy en día están representados por el ciudadano común que compra un dron. Puede dejarse las especificaciones técnicas y administrativas a la circular.

De acuerdo con la DGAC, para elaborar la Circular R4 se consideraron disposiciones y recomendaciones establecidas por la Organización de Aviación Civil Internacional (OACI), así como las mejores prácticas establecidas por autoridades aeronáuticas como la Administración Federal de Aviación (FAA) de los Estados Unidos. Sin embargo, sea para el caso mexicano u otro, la implementación de cualquier normatividad que regule el espacio aéreo es facultad inherente de la autoridad aeronáutica por lo que los principios-guía fundamentales que deberían regir la operación de drones deberán ser: *a)* quien realice el vuelo esté capacitado y cuente con licencia; *b)* que la aeronave esté registrada; y *c)* que se respeten las normas de seguridad.

Además –en el caso mexicano– se encuentra en proceso, la elaboración de una NOM (Norma Oficial Mexicana) para complementar a la circular R4[212]. Las normas oficiales, habitualmente, lo que hacen es establecer estándares, condiciones y características técnicas de un producto o servicio. Y cada secretaría según su ámbito de acción, tiene facultad de emitir las respectivas normas oficiales[213].

A continuación, se transcribe una breve entrevista que fue realizada al autor de estas líneas por una agencia de información para la industria del transporte aéreo sobre el tema:

> Al realizar una búsqueda en Internet con la frase "accidentes drones", aparecen miles de videos con situaciones que, de formas muy elocuentes, muestran el potencial peligro que representa, ya sea para los mismos usuarios o para

[212] La SCT también señaló que se está gestionando la publicación en el Diario Oficial de la Federación del proyecto de Norma Oficial Mexicana (NOM) número 107, con el fin de someterla a consulta pública durante un periodo de 60 días. *Cfr. https://www.gob.mx/sct/prensa/trabaja-la-sct-en-la-regulacion-sobre-sistemas-de-aeronaves-pilotadas-a-distancia-rpas-tambien-llamadas-drones.*

[213] En suma, se podría decir que las armas legales con que cuentan los usuarios de drones en México hasta el momento son: la Circular R4, la página de Internet con instructivo y los formatos para el registro en línea de RPAS, y una subsección de la misma en la que se pueden realizar reportes de seguridad operacional. Necesitamos un marco más robusto: no basta con una circular.

terceros, la mala utilización de estos equipos tecnológicos. De ahí la preocupación de varios gobiernos –incluyendo el mexicano– de crear marcos normativos que regulen la operación segura de los sistemas de aeronaves pilotadas a distancia (RPAS por sus siglas en inglés).

Sin embargo, los instrumentos legales con que actualmente cuenta nuestro país (la llamada Circular Obligatoria CO AV-23/10 y los formatos para reportes de daños e invasión de RPAS en espacio aéreo prohibido) no contemplan los protocolos necesarios para neutralizar amenazas graves al bienestar de la ciudadanía en general, consideró Rodrigo Soto-Morales, experto en Derecho Aeronáutico de la Universidad Panamericana.

"Es un tema que está pendiente… por un lado, están surgiendo las escuelas de pilotaje de drones, también la certificación y la licencia para volar equipos de mayor tamaño y peso... la Circular parece ser técnicamente muy completa. Pero, desde el punto de vista de la seguridad, necesitas capacidades operativas que, en caso de una infracción grave al ordenamiento, forzosamente puedan poner la aeronave en tierra y eliminar una amenaza", señaló el especialista.

Este tipo de procedimientos de seguridad son usuales en la aviación comercial, como en el caso reciente de un vuelo de Korean Air que cubría la ruta entre Seúl y Zúrich. Mientras la aeronave Boeing 777 que sobrevolaba Alemania, perdió contacto por radio con los controladores aéreos, por lo que tuvo que ser escoltado a tierra por dos aviones caza de la Fuerza Aérea germana.

Luego entonces, ¿qué tipo de acciones correctivas debe establecer la ley para evitar las amenazas con drones?

"Esos protocolos, que ya existen, se tienen que diseñar para el tema de los drones. Y no están muy claros en la Circular. Entonces, ¿cómo combates la tecnología? Con tecnología. ¿Cómo paras un coche en carretera? Con otro coche. ¿Cómo bajas un avión? Con otros aviones. Aquí tenemos que ver cuáles son las capacidades operativas que tiene la autoridad, tanto desde el punto de vista de salvaguardar la integridad del público como desde la seguridad operacional, para contrarrestar o confrontar drones que invaden zonas de restricción".

Soto-Morales citó ejemplos de medidas que se han implementado en otros países para garantizar esta respuesta a las amenazas. Como en Estados Unidos, cuyas autoridades han obligado a los fabricantes de drones a incorporar

el geoperimetraje, una tecnología con base en sistemas GPS que funciona como un escudo invisible que impide a los RPAS acceder a áreas prohibidas como aeropuertos o cárceles.

Sin embargo, este instrumento tiene la desventaja de que su software debe actualizarse cada vez que las áreas de restricción se modifiquen, o que puede ser alterado por el mismo usuario para evitar ser inhibido.

"Necesitamos también inhibidores de señal en tierra para que el dron baje, que ya existen. O como en Holanda, que es bien sabido, donde han entrenado a las águilas reales para frenar drones de cierto tamaño. Ejércitos o fuerzas armadas de otros países tienen baterías antiaéreas (pequeños misiles teledirigidos) aplicables a drones. Entonces, insisto, la tecnología se combate con tecnología, y necesitas una respuesta acorde, en su materia, en su forma y en sus capacidades, a la amenaza".

¿El poder de la denuncia?

Pero, ¿qué pasa si me doy cuenta de que alguien está volando RPAS cerca de la terminal aérea de mi ciudad? ¿O si soy testigo de un accidente que afecte a terceras personas?

"La Circular obligatoria emitida por la Dirección General de Aeronáutica Civil establece como acciones de vigilancia y seguridad ante estas infracciones que "cualquier persona física o moral, o cualquier entidad federal o local" envíe un reporte inmediato a los puntos de contacto en las comandancias de los aeropuertos.

Y en el caso de que un dron cause heridas o la muerte de alguna persona, el ciudadano tiene hasta 10 días calendario, de ocurrido el evento, para denunciar el hecho 'con el mayor detalle posible'.

Con el formato (de la DGAC) lo que aplica es un principio legal general de responsabilidad civil, de responsabilidad administrativa, y en el caso de la comisión de un delito, de responsabilidad penal. Como yo le digo de broma, un 'zape[214] drónico', puede llegar a matar a alguien", puntualizó el experto.

---

[214] En lenguaje coloquial en México, zape es lo que se define en el Diccionario de la Real Academia Española como "colleja", es decir: golpe que se da en la nuca con la palma de la mano.

> Aquí entramos al turbulento espacio jurídico de la seguridad pública, el cual seguiremos abordando en futuras entregas[215].

En el caso de la Agencia Federal Aeronáutica (FAA, *The Federal Aviation Administration*) de los Estados Unidos de América, los drones han supuesto una nueva responsabilidad para la misma en su categoría de Autoridad de la Aviación Civil de ese país.

En el año 2012, el Congreso de los Estados Unidos de América instruyó que la FAA desarrollara las reglas para la integrar los UAS (*Unnamed Aircraft Systems*), como se les denominaba entonces. La denominación internacional más extendida sigue siendo *Remotely Piloted Aircraft System* (RPAS), sin embargo, la FAA ha mantenido el UAS[216], y esto es jurídicamente consonante con el problema de asentar un concepto jurídico determinado para referirse a este tipo de aeronaves, pues mientras eso no suceda, sin una definición específica y determinada, en ámbito administrativo y judicial, estamos ante un concepto jurídico indeterminado, innominado.

Las reglas que la FAA, por instrucción del Congreso, debería desarrollar serían considerando este tipo de aeronaves dentro del sistema de espacio aéreo nacional, lo cual debería quedar asentado para el 30 de septiembre de 2015, según la *FAA Modernization an Reform Act of 2012, Pub. L. No. 112 Stat. 11.* Lo cual así sucedió[217]. La misión consistía en desarrollar los estándares aceptables de operación y certificación de estar aeronaves:

> … asegurar que cualquier UAS de usos civil incluyera una capacidad de sensor para evitar obstáculos [y zonas restringidas], establecer una línea de tiempo de fases de integración al sistema nacional de espacio aéreo y establecer un proceso para desarrollo de certificación, estándares de vuelo y navegación, así como requisitos de tráfico aéreo para los UAS[218].

---

[215] Publicado por *Aviación 21*, el 17 de agosto de 2017, *cfr. http://a21.com.mx/aeroespacial/2017/08/17/faltan-protocolos-en-mexico-para-operacion-segura-de-drones.*

[216] *Cfr. https://www.faa.gov/uas/.*

[217] *Cfr.* Hefferman, D., y Connor, B., *Aviation Regulation in the United States,* Chicago, American Bar Association, 2014, p. 269.

[218] *Ibidem,* p. 269. La traducción es del autor.

Hoy en día, la FAA ejerce jurisdicción sobre los RPAS con base a los criterios tradicionales de tamaño, peso, desempeño y alcance. Aquellos RPAS utilizados con fines recreativos o de entretenimiento permanecen no regulados, no así las zonas restringidas a estos aparatos, que continuamente están siendo monitoreadas y publicadas en caso de determinarse nuevas. Las aeronaves de Estado, es decir, RPAS utilizados para agencias de gobierno, sean federales, estatales o municipales, también son reguladas por la FAA y pueden ser operadas después de un proceso de aprobación minucioso y de acuerdo a la emisión de un certificado de autorización FAA o de un certificado de exención o autorización de operaciones, según el caso (seguridad pública, rescate, incendios, etc.)[219]. En la página web oficial de la FAA se puede acceder a las reglas pormenorizadas de cómo y cuándo volar un dron según su tipo, tamaño, alcance y la intención del vuelo.

Esto es, después de haber comentado la regulación desde aspectos generales tanto en México como en los Estados Unidos de América, vemos que los principios generales para la regulación son coincidentes: *a)* certificación de acuerdo a estándares de seguridad operacional; *b)* registro según estándares de tamaño, peso, alcance y desempeño; *c)* licencia y certificación del piloto u operador; *d)* respeto a los estándares de seguridad en vuelo y zonas restringidas; y *e)* responsabilidad administrativa, civil y en su caso penal con relación a provocar daños a terceros, sean de tipo físico, patrimonial o moral (como podría ser el caso de invasión a la privacidad).

II. LA CONDICIÓN JURÍDICA DE LA GEOLOCALIZACIÓN

El espacio humano, sea urbano o rural, desde el principio ha sido diseñado para permitir la convivencia y el despliegue de la vida a lo *largo y ancho* de la superficie terrestre aéreo, pero hoy, con el desarrollo amplio –y en tan breve tiempo– del transporte aéreo, a las dos dimensiones tradicionales de convivencia e interacción habrá que incluir a la tercera. Así, la anchura, la profundidad y la altura son dimensiones del actuar humano a través de la tecnología y no me refiero a la tecnología de la realidad virtual o a las ilusiones ópticas, sino a la tecnología operativa real que se despliega a través de los drones.

---

[219] *Ibidem*, p. 270.

Un dron –no debe olvidarse– es un sistema, es decir, un conjunto de elementos que interactúan entre sí para lograr un objetivo, en este caso operacional, de desplazamiento en el aire de una máquina que transmite información y recibe información. Existe aeronave, operador y sistema de operación remota a través de emisión y recepción recíproca entre el operador y la aeronave. La aeronave en sí misma –al igual que la base de control del operador–, es emisor y receptor, no solo de señal sino de información adicional (posición, velocidad, altura), al igual que una aeronave convencional de transporte de pasajeros, o de fotografía aérea, medición, topografía, etc. Es por ello, que el dron es un agente operativo en el aire que es capaz de "geolocalización".

Esta última se entiende como el proceso para lograr obtener datos exactos sobre la situación que ocupa un objeto en el espacio y se mide en coordenadas de latitud (x), longitud (y) y la altura (z). Se utiliza en programas y sistemas informáticos para almacenar datos de referencia geográfica[220].

Los drones o RPAS son aparatos que resultan muy *ad hoc* para obtener esta información. Al igual que los teléfonos móviles, es posible que mediante el sistema de GPS se obtengan las coordenadas de latitud, longitud y altura, pero de una manera más rápida y exacta dada su versatilidad y velocidad de desplazamiento, además de poder evitar obstáculos de una manera más ágil.

Legalmente, en México se puede abordar el tema de la localización geográfica de acuerdo con las disposiciones constitucionales tales como los Artículos 6o. y 16, apartado A; y de leyes tales como la Ley Federal de Telecomunicaciones, en su Artículo 90, y el Código Nacional de Procedimientos Penales, en su Artículo 303[221]. Ambas disposiciones tienen en mente la telefonía móvil como el medio más habitual para obtener dicha referencia y aceptar la posibilidad de que el Ministerio

[220] *Cfr.* Salgado Perrilliat, Ricardo, y Martínez Becerril, Rigoberto, "La geolocalización y el derecho a la privacidad", *Revista el Mundo del Abogado*, México, vol. 182, 2014, p. 20.

[221] Dicho Artículo señala que cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil, asociados a una línea que se encuentre relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien delegue la facultad, podrá solicitar al Juez de Control del fuero correspondiente en su caso, por cualquier medio, requiera a los

Público pueda obtener tal información sin que medie orden judicial. Es criterio señalado como constitucional por la Segunda Sala del máximo Tribunal del país:

> LOCALIZACIÓN GEOGRÁFICA EN TIEMPO REAL DE LOS EQUIPOS DE COMUNICACIÓN MÓVIL PREVISTA EN EL ARTÍCULO 190, FRACCIÓN I, DE LA LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN. AUTORIDADES COMPETENTES PARA SOLICITARLA Y PRESUPUESTOS QUE LA AUTORIZAN.
>
> Si bien la mencionada disposición legal hace referencia expresa a las "instancias de seguridad, procuración y administración de justicia" como las autoridades con que los concesionarios de telecomunicaciones y los autorizados deben colaborar en la localización geográfica en tiempo real de los equipos de comunicación móvil, lo cierto es que a fin de lograr un óptimo grado de certidumbre jurídica a los gobernados, así como enmarcar adecuadamente la actuación de las autoridades en esta materia, se considera que las autoridades a que se refiere la porción normativa aludida son: (I) el Procurador General de la República, así como los Procuradores de las entidades federativas y, en su caso, los servidores públicos en quienes deleguen esta facultad, en términos del artículo 21 de la Constitución Federal; (II) la Policía Federal, conforme a lo previsto en el artículo 8, fracción XXVIII, de la ley que la regula; y, (III) la autoridad encargada de aplicar y coordinar directamente la instrumentación de la Ley de Seguridad Nacional en los supuestos establecidos en su artículo 5. Así, sólo las autoridades referidas podrán solicitar la localización geográfica en tiempo real de los equipos de comunicación móvil cuando se presuma que existe un peligro para la vida o la integridad de las personas, lo que implica que dicha facultad no se circunscribe a un catálogo de delitos determinado, sino que encuentra su razón jurídica en la tutela de los derechos humanos a la vida y a la integridad personal, como valor supremo a cargo del Estado mexicano.

---

concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. *Código Nacional de Procedimientos Penales,* México, Diario Oficial de la Federación, 5 de marzo de 2014, última reforma, 17 de junio de 2016.

Amparo en revisión 964/2015. Carlos Alberto Brito Ocampo y otros. 4 de mayo de 2016. Cinco votos de los Ministros Eduardo Medina Mora I., Javier Laynez Potisek, José Fernando Franco González Salas, Margarita Beatriz Luna Ramos y Alberto Pérez Dayán; se apartaron de consideraciones Margarita Beatriz Luna Ramos y José Fernando Franco González Salas, este último respecto a las consideraciones relacionadas con los datos estructurados (megadatos). Ponente: Alberto Pérez Dayán. Secretario: Isidro Emmanuel Muñoz Acevedo.

Esta tesis se publicó el viernes 5 de agosto de 2016 a las 10:05 horas en el Semanario Judicial de la Federación.

Aunque no se trata de un criterio de jurisprudencia, la tesis asoma el argumento que sostiene la viabilidad de la obtención de esta información por parte de la autoridad encargada de la procuración de justicia, y por tanto de modo restringido a casos en los cuales se presume que existe un peligro a la vida o integridad de las personas, "lo que implica que dicha facultad no se circunscribe a un catálogo de delitos determinado, sino que se encuentra su razón jurídica en la tutela de los derechos humanos a la vida y a la integridad personal".

De este modo, la geolocalización, al menos en México, no es una facultad irrestricta del Estado, siendo privilegiada y solo limitándose a un caso urgente y grave la excepción de prestarla, siendo contrario al dictado constitucional el vulnerarla. Esto es así, pues la ubicación geográfica en tiempo real es considerada –al menos de manera implícita– un dato privado, es decir, una información relacionada de forma directa e indisociable con el sujeto y su esfera privada.

Entonces, ¿la referencia de geolocalización de una persona determinada en un momento determinado es un dato personal, privado? La respuesta es: sí. Lo es, pues también es un "metadato", es decir, un dato que describe otro dato; datos acerca de otros datos. Y que es sujeto de almacenamiento, análisis y difusión, pero en casos específicos, puede aportar si se obtiene de manera recurrente y continuada, información de hábitos, relaciones e interacciones que forman parte del aspecto privado de la vida de una persona, de la localización geográfica de sus bienes, posesiones e incluso de su ámbito íntimo.

Cuando la propiedad privada y su intimidad son invadidas por un dron que comparte o transmite imágenes de la vida privada, vida íntima y además localiza

geográficamente ese "*situ*", sin autorización de las personas o personas cuya imagen y referencia se transmite, ¿se violan derechos humanos?

El Código Civil Federal, en su Artículo 1916, es claro en señalar la tutela de la imagen cuando esta es atacada, dando lugar a la reparación del daño moral que se pueda sufrir como consecuencia. El manejo de la propia imagen es un derecho de la personalidad y en el ámbito jurídico esto ya se ha discutido prolijamente durante las cuatro décadas pasadas[222].

Pero, ¿y la geolocalización? Hoy en día las aplicaciones en los teléfonos, o navegadores con GPS integrados en los automóviles, así como en las computadoras personales requieren el consentimiento del usuario para recabar este dato geográfico de referencia cuando está utilizando algún software de servicio de navegación o localización, sea como una herramienta de trabajo o en aplicaciones recreativas. Y si no requiere el consentimiento de manera expresa, los dispositivos ponen en el sistema operativo la posibilidad de deshabilitar la opción de geolocalizar en el equipo de que se trate.

En el caso de los RPAS, el *sujeto pasivo*, es decir, la persona o individuo que es captado y cuya ubicación es reportada a un tercero sin su consentimiento, pudiendo incluso, de acuerdo con la posición de la aeronave brindar información de referencia geográfica de dicho *sujeto pasivo*; cuando el *sujeto activo* operador del RPAS no es una autoridad en ejercicio de sus funciones, y como hemos visto –para poder ser fundada y motivada–, dicha acción debe tener lugar en un contexto de seguridad pública o procuración de justicia, o en un contexto de búsqueda para rescate y salvamento, esto debido a la clara prevalencia del orden público y la seguridad en el primer caso, y de la vida e integridad física en el segundo.

El debate radica en que la superioridad operativa del dron, su versatilidad y su tamaño pueden convertirlo en una herramienta para la obtención de aspectos

---

[222] El derecho a la vida privada o intimidad, al honor e incluso a la imagen propia son considerados como derechos humanos fundamentales por diversos instrumentos internacionales, tales como la Declaración Universal de los Derechos Humanos aprobada por la Asamblea General de las Naciones Unidas de 1948, en su Artículo 12; el Pacto Internacional de los Derechos Civiles y Políticos de 1966, Artículos 17 y 19; la Convención Americana sobre Derechos Humanos de 1969, Artículos 11 y 13, por mencionar algunos.

de la vida privada de las personas, y el *metadato* de la geolocalización de esa persona, sus bienes y su ámbito de relaciones, lo cual, realizado sin su consentimiento, es una completa conculcación de su esfera personal de derechos, como prerrogativas fundamentales. Un ejemplo sobre esta posición es el breve artículo publicado en la Revista Nexos, de Luis Fernando García[223], en el cual sostiene que la jurisprudencia europea sí reconoce los *metadatos* como un elemento que recibe protección extensiva cual derecho a la privacidad y comunicaciones privadas:

> ¿Los "metadatos" están protegidos por el derecho a la inviolabilidad de las comunicaciones privadas?
>
> Para algunos existe controversia respecto de si el derecho a la inviolabilidad de las comunicaciones privadas, reconocido en los párrafos decimosegundo y décimo tercero del artículo 16 constitucional, protege únicamente el contenido de las comunicaciones o también se refiere a los datos que identifican una comunicación.
>
> No obstante, la Suprema Corte, la Corte Interamericana de Derechos Humanos y organismos de protección internacional de derechos humanos han establecido reiteradamente que los metadatos también se encuentran protegidos por el derecho a la inviolabilidad de las comunicaciones privadas.
>
> Esta protección equivalente parte del hecho de que los metadatos revelan información tan sensible como el contenido de las comunicaciones. Como lo ha señalado el Tribunal de Justicia de la Unión Europea (TJUE): "Estos datos, considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan".
>
> En este sentido, el acceder, conservar o registrar los metadatos de comunicaciones constituye una interferencia con el derecho a la inviolabilidad de las comunicaciones privadas y, por ende, debe cumplir con los requisitos que

[223] García, Luis Fernando, "La Suprema Corte y el peligro de conservar metadatos de comunicaciones", *Revista Nexos,* 2016, *http://eljuegodelacorte.nexos.com.mx/?p=5754#_edn1.*

establece el artículo 16 constitucional, principalmente, la necesidad de una autorización judicial.

Cabe señalar además que las leyes entienden que el concepto de "intervención de comunicaciones privadas" incluye tanto el acceso al contenido, como el acceso a los datos que identifican una comunicación, como es el caso del artículo 291 del Código Nacional de Procedimientos Penales. Aunque nos referiremos con mayor detalle a las cuestiones relacionadas con el acceso a los datos en otra ocasión[224].

Las resoluciones a las que se refiere el articulista son:

- SCJN. 1a. Sala. Amparo Directo en Revisión 1621/2010 y Contradicción de Tesis 194/2012; "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA COMUNICACIÓN". Tesis 1a. CLV/2011, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, t. XXXIV, agosto de 2011, p. 221.
- Corte Interamericana de Derechos Humanos. Caso Escher y otros vs. Brasil. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia de 6 de julio de 2009. Serie C, No. 200, párrafo 114.
- ONU. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de expresión Frank La Rue, 17 de abril de 2013, A/HRC/23/40, párrafo 15.
- Tribunal de Justicia de la Unión Europea. Digital Rights Ireland vs. Minister of Communications, Marine and Natural Resources y otros. Casos Conjuntos C-293/12 y C-594/12, 8 de abril de 2014, párrafo 26.

Creo que el argumento resulta todavía más convincente si se plantea la hipótesis de que esta información, ahora a través de la utilización de RPAS es fácilmente obtenible por un tercero particular al que hemos llamado "sujeto activo", no una autoridad en materia de seguridad y justicia en ejercicio de sus funciones. Pues el metadato de referencia geográfica obtenido de forma ilícita y por ende sin consentimiento de su titular, a ese titular *sujeto pasivo* en situación de vulnerabilidad, ya

---

[224] *Idem.*

sea con relación a su derecho de imagen, de intimidad, o en su integridad física o moral, por el posible mal uso que pueda dársele. Por lo que es dable y consistente entender el metadato de referencia geográfica sea tanto en telecomunicaciones o servicios de telefonía móvil, como el obtenido a través de un dron en operación aérea.

III. RETOS Y PERSPECTIVAS

Los RPAS o drones son todavía un pendiente jurídico para la legislación aeronáutica y el derecho de daños. Actualmente las herramientas legales con las que se cuenta, a falta de *lex specialis*, son las genéricas –*ex generalis*– para daños a terceros en la superficie, responsabilidad civil y en el caso de que se conculquen derechos de la personalidad y se consume a través de su operación un menoscabo a los derechos de la privacidad, intimidad e imagen, se deben aplicar las reglas conducentes al daño moral, la responsabilidad civil, penal y administrativa, según se configuren los hechos.

¿Por qué se podría justificar una *lex specialis*? Pues para evitar conflictos normativos. La versatilidad y los elementos interrelacionados con los RPAS lo exigen. La altura, la velocidad, la masa, la aceleración, utilizar una vía general de comunicación como es el espacio aéreo –de jurisdicción federal–, los estándares de diseño, vuelo, registro y certificación del operador encuadran el fenómeno en el ámbito propio de la aviación civil. Además, ya es una realidad que estas aeronaves "sin piloto", o piloteadas a distancia pueden, al igual que aquellas aeronaves convencionales, transportar pasajeros, carga o correo, como tradicionalmente se enuncia en la doctrina del Derecho Aeronáutico en la aviación comercial.

Esa condición de versatilidad que lo puede convertir en arma eficaz, en amenaza latente, en vulnerador de derechos personales, patrimoniales y del orden público hace del dron algo más que un "vehículo" o "juguete".

Por otra parte, una actitud restrictiva o inhibidora del desarrollo de la industria de los drones resulta un enfoque equivocado pues son muchas más sus ventajas y beneficios que sus riesgos. Nos solo para efectos recreativos, sino también para acciones de seguridad, agrimensura y topografía, medición, exploración, transmisión, fotografía, filmación, servicios médicos, primeros auxilios, y así po-

dríamos seguir con una innumerable lista de beneficios, por lo que el enfoque debería dirigirse a lograr la prevención y fortalecer un sistema no solo legal sino operativo de cumplimiento de la normatividad. La tecnología se regula y se controla con tecnología, es decir, a la par del desarrollo de este tipo de aparatos, se debe desarrollar –de hecho ya se ha avanzado mucho al respecto– la tecnología de inhibición, control y derribo en caso de riesgo o amenaza por parte de estas amenazas. Involucrar activamente a los fabricantes de estos aparatos en incluir la tecnología, sistemas o dispositivos que los hagan sujetos subordinados a la tecnología que debe poseer el Estado a través de su autoridad o dependencia competente para su efectivo control.

Asimismo, de acuerdo con su finalidad de uso, clasificar las zonas de vuelo de drones, para que todo el espacio aéreo –en la medida de lo posible– sea espacio aéreo controlado.

IV. ALGUNOS PRINCIPIOS PARA LA ELABORACIÓN DE UN MARCO NORMATIVO ADECUADO

Aunque ya lo hemos mencionado, resulta oportuno insistir en que valdría la pena que las leyes de aviación civil y sus reglamentos, así como disposiciones normativas y administrativas menores contemplen sus apartados especiales para los RPAS o drones, donde se vaya explicitando los principios generales previstos en la Ley General hasta su esfera reglamentaria administrativa por parte de la autoridad competente.

Tales principios generales para un breve y sucinto articulado serían:

1. Principios con relación a los estándares de seguridad operacional
   a) *Clasificar los aparatos según su tamaño y peso;*
   b) *Registrar los aparatos –con obligación bajo pena de sanción administrativa en caso de no hacerlo–, a partir de determinado tamaño y peso;*
   c) *Delimitación e identificación de zona prohibidas;*
   d) *Certificación y habilitación –es decir, necesidad de contar con licencia para operarlos– a partir de determinado tamaño y peso.*

2. Principios con relación a la responsabilidad civil, administrativa y penal aun cuando se haga remisión a la ley que corresponda según el caso.
   a) *Daños a terceros en la superficie;*
   b) *Daño moral e invasión de la privacidad y datos personales;*
   c) *Alteración del orden público;*
   d) *Lesiones, homicidio u otros ilícitos penales;*
   e) *Actos ilícitos contra la aviación sea civil o de Estado.*
3. Principios con relación a la responsabilidad del fabricante
   a) *Control y regulación de normas de diseño y seguridad operacional;*
   b) *Matriculado, control y rastreo;*
   c) *Inhibición y sistemas de sensores y evasión de obstáculos;*
   d) *Bloqueo y desbloqueo en recepción y transmisión de señal;*
   e) *Bloqueo de navegación en zonas restringidas;*
   f) *Protección y defensa frente al hackeo de software de operación e información.*

Por buena técnica legislativa, el intento no debería ser exhaustivo, sino complementario a la doctrina general existente del Derecho Aeronáutico. Dos o tres artículos para un apartado espacial en la Ley de Aviación Civil que luego puedan ser detallados en el modo de cumplirse y hacerse cumplir a través del Reglamento, normas oficiales y circulares bastaría.

Queda pues esta sugerencia como pequeño ánimo de alentar –y no lo contrario– el desarrollo de la industria de estos aparatos tan maravillosos, pero con la consiguiente exigencia para las autoridades de contar con las capacidades operativas y los respaldos legales para fundar y motivar el control equilibrado del vuelo de estas auténticas aeronaves por nuestro espacio aéreo, soberano y exclusivo.

V. FUENTES DE INFORMACIÓN

1. *Bibliografía*

BOUJOL, Maurice, *Diccionario de Derecho Administrativo y Burocrático*, México, Oxford, 2008.

BUNKER, Donald H., *International Aircraft Financing,* Montreal, International Air Transport Association, 2005.

Diccionario de la lengua española, Real Academia Española, 23ª. ed., Madrid, 2014.

FOLCHI, Mario, *Tratado de Derecho Aeronáutico y política de la aeronáutica civil*, Buenos Aires, Astrea, 2015, t. I.

GARCÍA, Luis Fernando, "La Suprema Corte y el peligro de conservar metadatos de comunicaciones", *Revista Nexos,* 2016, *http://eljuegodelacorte.nexos.com.mx/?p=5754#_edn1.*

HEFFERMAN, D., y CONNOR, B., *Aviation Regulation in the United States,* Chicago, American Bar Association, 2014.

International Aircraft Financing, Montreal, International Air Transport Association, 2005.

MARTÍNEZ MORALES, Rafael I., *Diccionario de Derecho Administrativo y Burocrático*, México, Oxford, 2008.

SALGADO PERRILLIAT, Ricardo, y MARTÍNEZ BECERRIL, Rigoberto, "La geolocalización y el Derecho a la Privacidad", *Revista el Mundo del Abogado*, vol. 182, 2014.

2. *Otros*

https://www.faa.gov/uas/.

http://a21.com.mx/aeroespacial/2017/08/17/faltan-protocolos-en-mexico-para-operacion-segura-de-drones.

https://www.gob.mx/sct/prensa/trabaja-la-sct-en-la-regulacion-sobre-sistemas-de-aeronaves-pilotadas-a-distancia-rpas-tambien-llamadas-drones.

CAPÍTULO DÉCIMO PRIMERO
Desafíos de un internet seguro

Alfredo A. REYES KRAFFT[225]

SUMARIO

I. *Introducción.* II. *Internet de las cosas*. III. *Globalización*. IV. *Redes sociales*. V. *La larga cola*. VI. *Internet abierto*. VII. *Big Data.* VIII. *Cómputo en la nube*. IX. *Fraude tecnológico, abuso en línea y usurpación de identidad*. X. *Inteligencia Artificial*. XI. *Criptomonedas y blockchain*. XII. *Fuentes de información*.

I. INTRODUCCIÓN

La sociedad es en donde nacemos, en la que estamos inmersos cotidianamente; la sociedad virtual es intangible, depende de la real pero posee sus propias características. La sociedad tiene límites locales, fronteras geográficas y políticas;

[225] Experto en temas de firma electrónica, contratación electrónica, factura electrónica, protección de datos personales y al mando de una de las áreas más destacadas del despacho E-Business Law. Ha sido reconocido a nivel nacional e internacional por su gran aportación al Derecho de las Tecnologías de la Información y Comunicación (TICs). Doctor en Derecho con mención *Cum Laude* por la Universidad Panamericana. Estudios en alta dirección en el IPADE, especialidad en contratos y daños por la Universidad de Salamanca, múltiples especialidades en la Universidad Panamericana, autor y coautor de muchos libros relacionados con las TICs. Amplia experiencia laboral en el ámbito financiero, innovación, negociación y contratación electrónica, la mejor opción en México. Es experto certificado en materia de protección de datos personales por NYCE (Normalización y Certificación Electrónica) y en España por el Data Privacy Institute. Catedrático de las universidades más prestigiadas del país y destacado conferencista a nivel nacional e internacional.

pero la virtual traspasa esas demarcaciones y fluye en ámbitos transfronterizos, su referente es global[226].

Es en el ciberespacio, donde se mueve la sociedad virtual, donde se modifica la percepción espacio-tiempo; los usuarios, los actores, los observadores de la sociedad virtual crecen exponencialmente y clarifican sus derechos, los comparten y los refuerzan; el ciberespacio se vuelve un terreno educativo, de investigación, de transacciones comerciales y de mercado, de política económica, de denuncia, de lucha social y de crimen...[227].

Esta sociedad crea nuevas identidades, nuevos ciudadanos: los *netizen*, término formado por net = red y cit(izen) = ciudadano; en consecuencia, se generan nuevos términos, nuevas ocupaciones y quizá, hasta nuevos delitos, como los llevados a cabo por los *hackers* y los contra-*hackers*, así como los introducidos por los virus y los antídotos, para defenderse de los ataques de quienes, por gusto, curiosidad, reto, o maniobra destructiva bajo contrato, se hacen de bienes, trabajo y conocimiento de otros...[228].

Toda esta conversación conectada está transformando también al público. Como Narciso, también nos dejamos seducir por nuestra propia imagen *online* y la tentación de tener cada vez más lazos sociales[229].

Es posible que en estos tiempos de máxima conectividad social existan menos conexiones reales que antes. Marshall McLuhan (1968 y 1973), prestigioso teórico de los medios de comunicación, ya pronosticó esta posibilidad hace más de cuarenta años, cuando afirmó que "la extensión conduce a la amputación". Con los

---

[226] Morales Campos, Estela, "Internet y sociedad: Relación y compromiso de beneficios colectivos e individuales", *Revista Digital Universitaria*, vol. 5, número 8, 10 de septiembre de 2004, *http://www.revista.unam.mx/vol.5/num8/art49/art49.htm.*

[227] *Cfr*. Bonilla, Carlos, "Liderazgo en la sociedad virtual*", Revista Mundo Ejecutivo*, *http://mundoejecutivo.com.mx/management/2015/03/11/liderazgo-sociedad-virtual.*

[228] Morales Campos, Estela, *op.cit.*

[229] Hirshberg, Peter, "Primero los medios y luego nosotros. Cómo ha cambiado Internet la naturaleza fundamental de la comunicación y su relación con el público", *19 ensayos fundamentales sobre cómo el internet está cambiando en nuestras vidas*, Madrid, BBVA, 2014.

teléfonos móviles y los dispositivos sociales estamos conectados a pantallas y de forma virtual con amigos en los cinco continentes, pero tal vez a costa de una conexión auténtica con el mundo. Pudiéramos llegar a un llamado estado de "soledad compartida"[230] Nos "acercan con los lejanos pero nos alejan de los cercanos".

II. INTERNET DE LAS COSAS

En el pasado podíamos desconectarnos de los medios apagando el dispositivo, saliendo del sistema. Ahora, eso constituye la excepción a la regla y, para muchos, motivo de conflictos. Ante la sugerencia de que se desconecte, un joven de hoy nos dirá: "¿Desconectarse?, ¿qué es eso?" o "¿por qué me castigas?". Casi siempre estamos conectados a un dispositivo con acceso a Internet, bien sea un teléfono inteligente, un monitor de ejercicio, un *iPod*[231], una tableta, un videojuego o una pantalla. Tenemos extensiones de nuestro cuerpo en forma de sensores, señales y servidores que registran cantidades enormes de datos acerca de cómo vivimos nuestro día a día, la gente que conocemos, los medios que consumimos y la información que buscamos. En efecto, los medios nos siguen a todas partes y cada vez somos menos conscientes de su presencia.

Mantenemos relaciones muy íntimas con nuestros dispositivos conectados. A los pocos minutos de habernos despertado, la mayoría ya estamos consultando el teléfono móvil. Lo consultamos más de 150 veces a lo largo de la jornada y pasamos el equivalente a cerca de dos horas diarias con un móvil pegado a la oreja. A medida que estos aparatos se han vuelto omnipresentes, cada vez hay más datos de nuestra vida almacenados de manera casi permanente en servidores y que pueden ser consultados por otros (incluidas empresas y agencias del gobierno)[232].

La idea de que todo puede medirse, cuantificarse y almacenarse representa un cambio fundamental para la condición humana. Durante miles de años hemos vivido según la idea de que somos responsables ante un Dios omnipotente que

---

[230] Islas, Octavio, "Marshall Mcluhan y la complejidad digital", *Revista razón y palabra,* número 63, *http://www.razonypalabra.org.mx/n63/varia/oislas.html.*

[231] Marca Registrada de Apple Inc.

[232] *Cfr.* Castells, Manuel, "El impacto de Internet en la sociedad: Una perspectiva global", *19 ensayos fundamentales sobre cómo el Internet está cambiando en nuestras vidas*, *op. cit*.

todo lo ve y que nos vigilaba por nuestro propio bien, para garantizar nuestra salvación. Por esa, entre otras razones, resulta tan efectiva la religión. Ahora, en cambio, en solo unos miles de años hemos reproducido esa red omnipotente que todo lo ve aquí en la Tierra… Impulsados por motivos menos elevados y quizá aún más efectivos, comercialmente hablando[233].

También estamos inmersos en una era de invención mediática sin precedentes. Hemos pasado del primer Internet basado en la web al mundo, siempre conectado, posterior a la computadora personal. Pronto entraremos en la era de la informática generalizada, en la que todos los aparatos y objetos construidos estarán conectados y serán interactivos, con capacidad de recoger y emitir datos.[234] Es lo que se ha dado en llamar "Internet de las cosas".

En el pasado reciente el ritmo del cambio tecnológico ha sido rápido, pero se está acelerando. Las cifras hablan por sí solas. En 1995 había aproximadamente 50 millones de aparatos conectados a Internet. En 2011 el número de conexiones pasaba de los 4,300 millones (más o menos la mitad eran máquinas). Aquel año nos quedamos sin direcciones de Internet y ahora se emplea otro mecanismo para direcciones llamado IPv6. Este modelo permitirá crear 340,000 millones de millones de millones de millones de direcciones IP únicas. Se trata probablemente de la cifra más grande jamás manejada por los seres humanos en el diseño de algo. En orden de magnitud, el número de átomos que contiene el universo solo es 40 veces superior el número de direcciones de Internet existentes, pero el hombre no inventó el universo[235].

Pero sí hay una cifra que tendremos que abordar, y pronto: en unos años es probable que exista más de un billón de dispositivos conectados a Internet. Nada crece más rápido sobre la Tierra que este medio, es decir, el número de dispositivos conectados y los datos que estos emiten. Por supuesto que, la mayoría, no son de personas, pero no debemos subestimar el impacto en nuestro mundo mediatizado de un billón de aparatos emitiendo señales y enviando información[236].

---

[233] *Cfr*. Hirshberg, Peter, *op.cit.*
[234] *Idem.*
[235] *Idem.*
[236] *Cfr*. Hirshberg, Peter, *op.cit.*

III. GLOBALIZACIÓN

La tendencia hacia la globalización viene impuesta por el carácter interdependiente, *multicéntrico* y multicultural de los fenómenos que gravitan sobre el horizonte presente de la reflexión jurídica. La "globalización" es el término con el que se alude a los actuales procesos integradores de la economía: financiación, producción y comercialización[237].

Inquieta pensar que hace más de cincuenta años McLuhan ya había adelantado las consecuencias de este entorno saturado de medios de comunicación. Cuando hablaba de la "aldea global" no se refería exactamente a que estaríamos conectados unos con otros. Lo que le preocupaba más bien era que todos conociéramos los asuntos de los demás, que perdiéramos parte de nuestra privacidad como resultado de vivir en un mundo con un conocimiento tan íntimo de las vidas ajenas. A esto McLuhan lo llamó "retribalización" y con ello quería decir que los medios de comunicación modernos nos llevarían a imitar el comportamiento de las aldeas tribales. Hoy en día los efectos de este fenómeno nos ayudan a definir el entorno mediático. Nos gestionamos a nosotros mismos de manera consciente, como si fuéramos marcas en línea, nos preocupan más que nunca los asuntos de los demás y tenemos más probabilidades de que nos hagan reproches o nos pongan en evidencia que en la desparecida (y más anónima) era de la comunicación de masas.

IV. REDES SOCIALES

La mayor parte de la actividad en Internet pasa por las redes sociales, que se han convertido en las plataformas de preferencia para todo tipo de fines, no solo para relacionarse y charlar con amigos, sino también para marketing, comercio electrónico, enseñanza, creatividad cultural, medios de comunicación y ocio, aplicaciones médicas y activismo sociopolítico. Se trata de una tendencia muy importante que abarca a casi toda la sociedad[238].

---

[237] Pérez Luño, Antonio Enrique *et. al*., *Nuevas tecnologías y derechos humanos*, México, Tirant Lo Blanch, 2014.

[238] Castells, Manuel, *op. cit.*

Las redes sociales las construyen sus propios usuarios a partir de criterios específicos de grupo. Existe un espíritu emprendedor en el proceso de creación de sitios web, que después, cada persona elige en virtud de sus intereses y proyectos particulares. Los propios miembros de las redes van configurándolas, aplicando diferentes niveles de perfil y privacidad. La clave del éxito no es el anonimato, sino más bien la *autopresentación* de una persona real que está conectada con personas reales (se han dado casos de exclusiones en una red social por el uso de una identidad falsa). Por tanto, estamos ante una sociedad autoconstruida mediante la conexión en red con otras redes. Pero no se trata de una sociedad virtual. Existe una estrecha conexión entre las redes virtuales y las redes vivas. Es un mundo híbrido, un mundo real. No es un mundo virtual ni un mundo aparte.

El público como distribuidor, conservador y árbitro. Todos podríamos encontrar lo que buscáramos porque alguien grande como Microsoft ya lo habría publicado. La idea de que lo que gustara o interesara al público se convertiría en un factor clave en la distribución, era inimaginable. Haría falta que aparecieran Google y su algoritmo PageRank para dejar claro que lo que interesaba a todo el mundo era una de las herramientas más importantes (y disruptivas) en el mundo de los medios de comunicación. A principios de la década de 2000, con el auge de los medios sociales, después convertidos en redes sociales, esta idea se convirtió en central[239].

V. LA LARGA COLA

Si lo pensamos ahora, resulta evidente: en un mundo de tiendas de discos y videoclubes, almacenar mercancía física acarreaba grandes costos. Por eso resultaba más rentable almacenar éxitos que contenidos menos populares. Con la llegada del mundo *online*, donde los contenidos de todo el mundo pueden almacenarse en servidores; los números cambiaron: el material menos popular ya no resultaba más caro de almacenar que el superventas. En consecuencia, el público se fraccionaría y encontraría *online* hasta los contenidos más extraños con mayor facilidad que en un *Blockbuster*[240]. En 2003 fue el año de la fundación de Amazon, empresa que mejor

[239] Hirshberg, Peter, *op.cit.*
[240] Marca registrada de Blockbuster, LLC.

ha capitalizado esta tendencia. Amazon ha sido uno de los fenómenos de mayor alcance y más disruptivos de Internet. Y es que la larga cola no solo ha puesto todo a nuestra disposición, sino que, al eliminar la mediación de los canales de distribución tradicionales, ha concentrado el poder en las manos de los nuevos gigantes mediáticos: Apple, Amazon, Google y Facebook (Microsoft todavía lucha por hacerse un hueco en el negocio).

VI. INTERNET ABIERTO

No supimos ver que la arquitectura de Internet sería abierta y que el poder se distribuiría. Que cualquier nodo podría ser un servidor o que un directorio no funcionaría jerárquicamente, como lo habían hecho la industria o las empresas de medios de comunicación. Internet se concibió para fines militares y académicos, pero llevaba dentro el germen de una serie de valores concretos referidos al acceso abierto sin puntos centrales de control. Y este acceso abierto ha sido determinante para el rápido crecimiento de todo tipo de medios nuevos. Diversidad y apertura han definido el entorno de los medios de última generación. Y no ha sido por casualidad, no había ningún determinismo tecnológico en juego[241].

VII. BIG DATA

"Big Data" se refiere al aprovechamiento de grandes conjuntos de datos con tres características principales: *volumen* (cantidad), *velocidad* (velocidad de creación y utilización) y *variedad* (tipos de fuentes de datos no estructurados, tales como la interacción social, video, audio, cualquier cosa que se pueda clasificar en una base de datos)[242].

Lo anterior permite el cruce de información, identificar hábitos, creación de perfiles y predecir tendencias, mediante el uso de matemáticas aplicadas.

Como un ejemplo, podemos comentar el caso de la tienda *Target*, la cual mediante el uso de esta tecnología pudo identificar de su base de clientes a mujeres

---

[241] Hirshberg, Peter, *op. cit*.

[242] *Cfr.* Galimany, Aleix, *La creación de valor en las empresas a través del Big Data*, Universidad de Barcelona, julio de 2014, *http://diposit.ub.edu/dspace/bitstream/2445/67546/1/TFG-ADE-Galimany-Aleix-juliol15.pdf*.

embarazadas a través de sus hábitos de consumo, llegando al extremo de que los papás de una adolescente se enteraron del embarazo de su hija, por los cupones de descuento que le enviaba esta empresa.

VIII. CÓMPUTO EN LA NUBE

El cómputo en la nube, como modelo de tecnológico[243], es clave para la optimización en la presentación de servicios de computación (software, plataformas o infraestructura) y, por tanto, contar con la capacidad de cómputo necesaria para la realización de nuestras actividades. Los cinco rasgos característicos del cómputo de la nube son:

a) Basado en servicios. El usuario tiene capacidad de infraestructura y servicios en la nube listos para ser usados;
b) Escalable y elástico. El servicio puede adaptarse a las necesidades del usuario de forma automática y sin que este tenga que dimensionar sus capacidades. La escalabilidad es una característica de la infraestructura y de las plataformas de software. La elasticidad se asocia no solo con la escala sino con un modelo económico que permite la escalabilidad bidireccional de forma automática;
c) Compartido. Los servicios comparten un pool de recursos con vistas a construir economías de escala. Todos los usuarios de la nube comparten infraestructura, software y plataformas;
d) Estimación por uso. Para calcular el importe de la facturación, los proveedores de servicios se estima el uso efectivo que se ha hecho de la plataforma; y
e) El uso de las tecnologías de Internet. El servicio se suministra utilizando identificadores de Internet, con sus formatos y protocolos, como URLs, HTTP, IP y otro tipo de arquitecturas similares.

[243] ISO/IEC 27018:2014

La nube existe desde que nace la virtualización de las máquinas, pero el modelo de negocio ha evolucionado de tal manera que los servicios prestados a través de la nube se prestan prácticamente en tiempo real. La evolución del cómputo en la nube es continua.

El uso de la nube, permite una importante rebaja en el costo de las operaciones relacionadas con la tecnología derivada tanto de las economías de escala como del uso bajo demanda (solo se paga lo que se utiliza). En el caso de nubes privadas permite la compartición de los recursos entre las diferentes áreas de las empresas y entidades que la solicitan.

La Regla de Moore establece que cada dos años se duplica la capacidad de las máquinas. Por ello, la inversión en infraestructura propia para la provisión de servicios compromete inversiones futuras, ya que estos deben ser renovados constantemente para mantenerse al nivel del mercado. Si estos servicios se contratan en la nube, los gastos de actualización se eliminan.

Al tratarse de servicios bajo demanda, las tareas de planeación y gestión de recursos también se simplifican, es decir, no es necesario contratar o prever la contratación de capacidades adicionales para momentos en los que se tengan picos de actividad, porque los servicios *software as a service* ya prevén la posibilidad de que existan picos imprevistos.

Pero el cómputo en la nube también permite acelerar las actividades de innovación y la puesta en marcha de proyectos que requieren niveles de computación más ambiciosos/amplios. La nube hace posible disfrutar de infraestructuras, plataformas o servicios necesarios para llevar a cabo nuevos proyectos, pero también para desarrollar pilotos y hacer pruebas.

Los clientes digitales exigen inmediatez en los servicios que la entidad presta y no aceptan la no disponibilidad o el retraso. El cómputo en la nube permite dar respuesta a sus peticiones, de forma flexible planificar las necesidades técnicas para un servicio 100% disponible sin el sobreprecio de un costo sobredimensionado por la incapacidad de ajustar la infraestructura en cada momento. En definitiva, se mejora la experiencia de cliente y la calidad del servicio al no verse afectado por el bajo rendimiento en picos de demanda.

La nube responde a los siguientes tipos, que pueden clasificarse de la siguiente manera:

a) *Nube pública.* La infraestructura de nube se pone a disposición del público en general y es propiedad de una organización que vende los servicios;
b) *Nube privada.* La infraestructura de nube se gestiona únicamente para una organización;
c) *Nube comunitaria.* La infraestructura de la nube la comparten diversas organizaciones con requerimientos similares; y
d) *Nube híbrida.* Composición de dos o más nubes, que se mantienen como entidades separadas pero unidas por tecnología estandarizada.

En definitiva, el cómputo en la nube parece surgir y alimentarse de la convergencia de distintos elementos determinantes del momento que vivimos. Algunas voces apuntan a que no solo provocará un cambio disruptivo en la industria de TI, sino que también alterará en forma significativa la manera en que la gente trabaja y las empresas operan.

IX. FRAUDE TECNOLÓGICO, ABUSO EN LÍNEA Y USURPACIÓN DE IDENTIDAD

La ciberdelincuencia podemos definirla como cualquier tipo de actividad ilegal en la que se utilice Internet, una red privada o pública o un sistema informático. Aunque muchas formas de ciberdelincuencia giran en torno a la obtención de información sensible para usos no autorizados, otros ejemplos son la invasión de la intimidad del mayor número posible de usuarios de computadoras. La ciberdelincuencia comprende cualquier acto criminal que utilice computadoras y redes. Además, también incluye delitos tradicionales realizados a través de medios tecnológicos. Por ejemplo: los delitos motivados por prejuicios, el fraude por Internet, la suplantación de identidad y el robo de cuentas de tarjetas de crédito cuando las actividades ilegales se llevan a cabo utilizando equipos de cómputo e Internet. Por tanto, el concepto de *ciberseguridad* ha sido asimilado desde sus orígenes a la seguridad en el ámbito de los medios informáticos, e incluso hasta bien recientemente se consideraba como un elemento esencial para la protección de toda clase de infraestructuras.

Sin embargo, dicho concepto hoy en día se ha modificado, dotándolo de una mayor y más amplia proyección, en cuanto que supone la protección específica del ciudadano en internet, mediante una estrecha colaboración con la Administración Pública y con las empresas, que se materializa en múltiples manifestaciones, que van desde la identidad digital, pasando por la firma electrónica, o los centros de alerta temprana (CERTs) hasta llegar a cualquier clase de servicio público o privado de información al ciudadano. Esta protección también se hace indispensable para toda clase de organizaciones, donde tienen su acomodo en múltiples aplicaciones, y, del mismo modo, debe destacarse su importancia en relación en las llamadas "infraestructuras críticas", donde cobra una especial importancia en los desarrollos e implantación de planes de *ciberseguridad* para centrales nucleares, sistemas de control, refinerías, oleoductos, gaseoductos, presas y sistemas de distribución de agua, redes eléctricas, entre otras muchas instalaciones, etc.

Ante este panorama son muy numerosas las políticas que se diseñan para garantizar y prevenir la seguridad a través del ciberespacio frente a los ataques que se dirigen contra los más diversos objetivos. Así, entre los más recurrentes, y vulnerables, cabe señalar los siguientes:

a) La prevención de los ataques a los sistemas de información. Estos ataques motivados, principalmente, por afán de lucro como la extracción de datos personales de manera ilegal, sin que el usuario sea consciente de ello. O el secuestro de información contenida en nuestras computadoras y dispositivos (Ransomware);
b) Los retos relacionados con la difusión de los dispositivos móviles. Este problema viene potenciado por aumento de los dispositivos móviles y de los servicios basados en la utilización de redes móviles;
c) Los retos relacionados con el advenimiento de los "entornos inteligentes". Estos "entornos inteligentes" suponen un punto importante dentro de la sociedad de la información. Los expertos esperan que en un futuro inmediato, los dispositivos inteligentes apoyados en las tecnologías de la computación y de las redes se conviertan en una presencia permanente en la vida diaria. A pesar de las obvias ventajas que conllevan estos

avances, también pueden suponer un riesgo hacia la seguridad y la vida privada; y

d) Los retos relacionados con la sensibilización de los usuarios. Uno de los problemas a los que enfrentamos es la extendida infravaloración que otorgan los usuarios a los riesgos que corren. El reto es conseguir presentar la seguridad como un activo y no como un costo de manera que los usuarios no lo consideren un aspecto negativo como viene sucediendo, en cierta medida, hasta el día de hoy.

Por ello, la *ciberseguridad* ha de contemplarse tanto desde la perspectiva de la prevención y de la vigilancia, y a su vez como reacción cuando el delito se ha producido, cuando lo que está en riesgo es la defensa de las personas y del medio ambiente, la prevención y control del fraude, la necesidad de mantener la eficacia y la eficiencia en los procesos de negocio, la preservación de la confidencialidad de la información, la integridad de los datos almacenados o transmitidos, la autenticación de los usuarios y los sistemas, la trazabilidad de los actos de negocio, el cumplimiento de las leyes, las regulaciones y los estándares nacionales o internacionales, la gestión de los procesos de seguridad, y otros procesos análogos, y ello sin desdeñar otros aspectos importantes, como pueden ser la salvaguardia de los bienes propios o ajenos o la protección de la reputación de las personas, marcas o de las empresas.

X. INTELIGENCIA ARTIFICIAL

Siguiendo a Don Javier Puyol, ya señalaba Rabindranath Tagore que: "el hombre necesita la máquina y la organización, pero tiene que dominarlas y humanizarlas en vez de resignarse a ser mecanizado y deshumanizado por ellas. El verdadero peligro para el hombre, no está en los riesgos que corre la seguridad material, sino en el oscurecimiento del hombre mismo en su propio mundo humano"; y como recuerda Lopezserrano Reyes, los avances tecnológicos y científicos de gran magnitud siempre han chocado en su etapa inicial con instituciones que controlan y rigen el orden de la sociedad, y esto incluye a la religión. Recordemos el caso de Galileo, torturado y apresado por tener el atrevimiento de declarar que la Tierra no solo

no era el centro del universo, sino que tampoco era plana. Este miedo al cambio y a lo nuevo se puede traducir en un rechazo programado hacia aquello que lo represente. Y en este panorama, la Inteligencia Artificial puede ser al mismo tiempo, víctima y culpable de su propio proceso de evolución[244].

La Inteligencia Artificial conjunta una serie de disciplinas con objetivos comunes entre ellos la resolución de problemas o la realización de tareas complejas por requerir un cierto grado de inteligencia. Lo anterior puede llegar a tener una importante connotación ética por el posible perjuicio que pudieran tener directamente o indirectamente las personas (la vida, la salud y el medio ambiente, la libertad, la intimidad, el puesto de trabajo o la dignidad de alguien, y en general a su bienestar físico y mental). En el ámbito jurídico no podemos dejar de considerar la confidencialidad de la información en Internet, la protección de datos personales, big data, el interfaz con los distintos tipos de usuarios, la seguridad informática, la investigación cibernética, los derechos de autor, la responsabilidad, la cadena de bloques (*blockchain*), etc.

Un ejemplo claro es el reciente accidente con un automóvil TESLA de conducción asistida en el que resultó muerto el distraído conductor. ¿Hasta qué punto debe confiarse a una máquina la toma de decisiones? ¿Quién es el responsable de las mismas? La cuestión entonces se centra en si sería ético "crear" *vida inteligente* en un espacio virtual sin hacer a estos "*seres*" partícipes de su propia naturaleza.

XI. CRIPTOMONEDAS Y BLOCKCHAIN

Este tema recoge las consideraciones respecto de las *criptomonedas*, como medio digital de intercambio, así como la tecnología en que estas se sustentan, el *blockchain*, en el que está proponiéndose de manera transversal, el desarrollo del Marco de Innovación Regulatoria (Regulatory Sandbox) para operar en el mercado bajo asistencia del Supervisor.

---

[244] Puyol, Javier, "No hay que temer a la inteligencia sino a la estupidez humana", *Revista Confilegal, https://confilegal.com/20150928-hay-temer-inteligencia-artificial-estupidez-humana-28092015-0930/*.

Dos líneas de negocio que, a pesar de ser diferentes, deben estar necesariamente interconectadas. Por un lado se incluyen todas aquellas entidades relacionadas con las *criptocurrencies* o *criptomonedas*, entendiendo por dicho concepto un medio digital de intercambio que surge como alternativa al uso de dinero fiduciario. Dichas *criptomonedas* funcionan a través de la tecnología *blockchain*, que permite identificar en todo momento quién es el titular de la moneda, de forma que se dificulta su uso con fines ilícitos. El uso de este tipo de instrumentos facilita determinados negocios o servicios relacionados con *bitcoins* (la clase más conocida de *criptomonedas*) tales como su compraventa, operaciones de corretaje (*brokerage*) con las mismas, o incluso la creación de una tarjeta virtual con ellas que permita realizar pagos.

A medida que nuestras actividades incorporan un componente digital, la división entre los dominios físico y virtual se vuelve cada vez más indistinguible. De cómo se maneje ese futuro digital, con qué criterios y prioridades se desarrolle la tecnología y qué políticas públicas se implementen, dependerá en gran medida el perfil de ese futuro y sus implicaciones para la seguridad, los derechos humanos, la democracia y la justicia social[245].

En cualquier caso, no cabe duda de que la sociedad de la información comporta nuevos retos para las personas, entre los que destacamos:

a) El cambio continuo, la rápida caducidad de la información y la necesidad de una formación permanente para adaptarse a los requerimientos de la vida profesional y para reestructurar el conocimiento personal;
b) La inmensidad de la información disponible, la necesidad de organizar un sistema personal de fuentes informativas, tener unas técnicas y criterios de búsqueda y selección;
c) La necesidad de verificar la veracidad y actualidad de la información;
d) Gestionar nuestra presencia en el ciberespacio;

---

[245] "Hacia una Internet ciudadana", *Revista Americana Latina en Movimiento,* abril de 2015, *http://www.alainet.org/es/articulo/169652.*

e) Los nuevos códigos comunicativos, que debemos aprender para interpretar y emitir mensajes en los nuevos medios;
f) La tensión entre el largo y el corto plazo en un momento en el que predomina lo efímero y se buscan rápidas soluciones pese a que muchos de los problemas requieren de estrategias a largo plazo;
g) La tensión entre tradición y modernidad: adaptarnos al cambio sin negarnos a nosotros mismos y perder nuestra autonomía;
h) Convertirnos en ciudadanos del mundo (y desarrollar una función social) sin perder nuestras raíces (tensión entre lo global y lo local); y
i) Debemos considerar que los delincuentes también utilizan este medio y sofistican día a día sus formas de delinquir.

XII. FUENTES DE INFORMACIÓN

BONILLA, Carlos, "Liderazgo en la sociedad virtual", *Revista Mundo Ejecutivo*, *http://mundoejecutivo.com.mx/management/2015/03/11/liderazgo-sociedad-virtual.*

CASTELLS, Manuel, "El impacto de Internet en la sociedad: Una perspectiva global", *19 ensayos fundamentales sobre cómo el Internet está cambiando en nuestras vidas*, Madrid, BBVA, 2014.

GALIMANY, Aleix, *La creación de valor en las empresas a través del Big Data*, Universidad de Barcelona, julio de 2014, *http://diposit.ub.edu/dspace/bitstream/2445/67546/1/TFG-ADE-Galimany-Aleix-juliol15.pdf.*

"Hacia una Internet ciudadana", *Revista Americana Latina en Movimiento,* abril de 2015, *http://www.alainet.org/es/articulo/169652.*

HIRSHBERG, Peter, "Primero los medios y luego nosotros. Cómo ha cambiado Internet la naturaleza fundamental de la comunicación y su relación con el público", *19 ensayos fundamentales sobre cómo el Internet está cambiando en nuestras vidas*, Madrid, BBVA, 2014.

ISLAS, Octavio, "Marshall Mcluhan y la complejidad digital", *Revista razón y palabra,* número 63, *http://www.razonypalabra.org.mx/n63/varia/oislas.html.*

MORALES CAMPOS, Estela, "Internet y sociedad: Relación y compromiso de beneficios colectivos e individuales", *Revista Digital Universitaria*, vol. 5, número 8, 10 de septiembre de 2004, *http://www.revista.unam.mx/vol.5/num8/art49/art49.htm*.

PÉREZ LUÑO, Antonio Enrique *et. al*., *Nuevas tecnologías y derechos humanos*, México, Tirant Lo Blanch, 2014.

PUYOL, Javier, "No hay que temer a la inteligencia sino a la estupidez humana", *Revista Confilegal*, *https://confilegal.com/20150928-hay-temer-inteligencia-artificial-estupidez-humana-28092015-0930/.*

CAPÍTULO DÉCIMO SEGUNDO
El derecho al olvido en el ámbito digital

Olivia Andrea MENDOZA ENRÍQUEZ[246]

SUMARIO

I. INTRODUCCIÓN

Hablar de nuevos derechos configurados desde el ámbito digital, es cada vez más común, atendiendo al vertiginoso desarrollo tecnológico y a las nuevas manifestaciones y ejercicio de derechos humanos. Uno de estos ejemplos es el denominado derecho al olvido, el cual, en principio deriva del ya conocido derecho a la protección de datos personales, particularmente en relación a los derechos de cancelación o supresión de datos personales.

La concepción del derecho al olvido, como una forma de manifestación del derecho a la protección de datos personales, encuentra su pertinencia de análisis en la postura de algunos tribunales y en la necesidad de incorporarlo a las legislacio-

[246] Investigadora Titular de tiempo completo y Coordinadora Académica de la Maestría en Derecho de las TICs del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (INFOTEC). Miembro del Sistema Nacional de Investigadores, Nivel 1.

nes nacionales; sin embargo, algunas particularidades deben resaltarse, cuando se configura el derecho al olvido, sobre todo en el ámbito digital, ya que su garantía, podría derivar en la vulneración de otros derechos, como la libertad de expresión, el derecho a la verdad y el acceso a la información.

Derivado de lo anterior, resulta pertinente abordar en las siguientes líneas, los antecedentes internacionales de la figura del derecho al olvido, las reflexiones que en México han surgido en relación al tema, el nuevo debate en torno a la naturaleza jurídica y alcances de este derecho, su reconocimiento y protección en México, para finalmente abordar las complejidades y desafíos de la salvaguarda de este derecho en el ciberespacio, con el objetivo de que el lector cuente con un panorama general de esta figura en el ámbito digital.

II. ANTECEDENTES DEL DERECHO AL OLVIDO

Cuando nos referimos acerca del derecho al olvido, debemos recordar que esta figura tiene su origen en la Sentencia T-414 de 16 de junio de 1992, dictada por la Corte Constitucional de la República de Colombia, así como su incorporación en legislaciones nacionales, como el caso del Artículo 10 de la Ley 787 de 2012, de la República de Nicaragua, y el Artículo 11 del Decreto 37554 de 2012, de la República de Costa Rica.

Por otro lado, si bien no se reconoce el derecho al olvido, el derecho a la desindexación tiene su origen en dos fuentes principales: el caso Google España de 2014, resuelto por el Tribunal de Justicia de la Unión Europea (en el que se exigió al buscador eliminar determinados resultados de información) y recientemente en el Reglamento General de Protección de Datos de la Unión Europea[247].

A partir de ese momento, más países de Latinoamérica plantearon la necesidad de incluir el derecho al olvido a sus ordenamientos jurídicos nacionales, lo cual se explica, entre otras cosas, por la necesidad de lograr niveles óptimos de

[247] Es importante señalar que el derecho al olvido tiene un ámbito de salvaguarda mucho más amplio que el derecho de desindexación, ya que este último, simplemente implica que los buscadores en Internet, eliminen los enlaces a determinadas páginas web, pero no garantiza el efectivo olvido en el ciberespacio, ya que la información permanecerá alojada en los sitios de Internet, con la salvedad de no estar ligadas a un buscador de uso común.

protección de la información, requisitos para realizar transferencias de datos o establecer pactos comerciales.

El derecho al olvido está relacionado directamente con la concepción del derecho de protección de datos personales, que tenemos desde los países que integramos la familia jurídica romano-germánica, por lo que la dimensión del derecho al olvido será distinta en lo que respecta a los países que conforman la familia jurídica del *Common Law*, ya que para ellos la protección de datos, no es un derecho humano o fundamental, sino un derecho del consumidor, regulado sectorialmente. Se debe considerar que la mayoría de buscadores, tienen su origen en países de esta última tradición jurídica.

Por otro lado, el primer antecedente del derecho al olvido en México, se encuentra en la postura del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), respecto a una solicitud de protección de derechos, formulada por un ciudadano mexicano, que analizaremos en el siguiente apartado.

III. PRIMER ACERCAMIENTO DEL DERECHO AL OLVIDO EN MÉXICO

La Institución encargada de garantizar el derecho de protección de datos personales en México anunció, en enero de 2015, un proceso sancionatorio contra Google México, ya que dicho buscador no atendió la solicitud de ejercicio del derecho de cancelación de datos de un ciudadano mexicano. La misma Institución ordenó a Google remover enlaces de información de esta persona, haciendo referencia en su argumentación al llamado *derecho al olvido*[248].

Este recurso fue promovido por un empresario mexicano, quien primero solicitó a Google, eliminara varios resultados de búsqueda relacionados con su nombre –alegando que la información afectaba su esfera más íntima y también sus relaciones financieras actuales–, ya que uno de esos enlaces llevaba al reportaje periodístico "Fraude en Estrella Blanca alcanza a Vamos México", publicado en el

[248] *Resolución del proceso sancionatorio abierto por el INAI contra Google México,* disponible en: *http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf.*

2007 por la revista Fortuna[249]. En esta nota, el empresario es mencionado como uno de los implicados en presuntos actos de corrupción.

La legislación mexicana en materia de datos personales en el sector privado, establece que en caso de que la solicitud de derecho de cancelación no sea atendida por el particular (en este caso Google), el titular del dato podrá acudir a través de la denominada solicitud de protección de derechos, ante el órgano garante, a fin de iniciar una investigación y, de ser el caso, iniciar un procedimiento sancionatorio contra el particular.

Uno de los argumentos que dio el buscador al órgano garante, en relación a la no atención de cancelación del dato, fue el no tener facultades para determinar el tipo de información podría indexar a su buscador, ya que Google no era responsable de la información en la fuente original.

Esta fue una oportunidad única para incidir en la construcción del derecho al olvido en el país, ya que por una parte, se concedía al buscador un rol de administrador de la información accesible a través de Internet –al determinar la relevancia de la información y con ello la facultad de afectar la neutralidad de la Red–[250], y por otro la sociedad civil estaba preocupada respecto a la afectación al derecho de libertad de expresión. En este sentido, la oficina en México de Artículo 19, manifestó que el acto de suprimir los enlaces de la nota (a pesar de no eliminar la información en su fuente original), establecía un mecanismo de censura, por tanto un atentado al derecho de libertad de expresión y de información.

Al presentarse la oportunidad única de establecer el primer precedente de derecho al olvido en México, la organización de la sociedad civil denominada Red de Defensa de los Derechos Digitales, representó a la revista Fortuna (medio informativo que constituía la fuente original de la información) para promover un

---

[249] Disponible en: *http://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm.*

[250] Como parte de las buenas prácticas de buscadores en Internet, particularmente de Google, hay excepciones de la postura tradicional respecto al derecho al olvido, ya que, atendiendo a la urgencia y a la naturaleza de la información, se eliminan ligas relacionadas, por ejemplo, a la pornografía infantil, o cuando se publican datos personales como el pasaporte, grupo sanguíneo, o cuando hay una violación a los derechos de autor.

amparo, ya que a pesar de todos los análisis descritos, el órgano garante nunca llamó al medio informativo a un derecho de audiencia respecto a la afectación que iba tener (desindexación de la nota periodística del buscador de Google), respecto a la medida de censura impuesta.

La estrategia jurídica consistió en presentar una demanda de amparo por violación a los derechos de libertad de expresión y garantía de audiencia. Google por su parte, impugnó la resolución que emitió la autoridad que garantiza la protección de datos personales en México (INAI), ante el otrora Tribunal Federal de Justicia Fiscal y Administrativa.

El tribunal en materia de amparo, negó esta demanda, por lo que la Revista Fortuna (representada por la organización de la sociedad civil, Red de Defensa de los Derechos Digitales), solicitó la revisión de la sentencia, y al turnarse a una segunda instancia (Tribunal Colegiado), se otorgó el amparo por falta al debido proceso (derecho de audiencia). Con esto, la resolución original del INAI, quedó sin efectos y se ordenó iniciar un nuevo procedimiento, garantizando derechos para los involucrados.

IV. UN NUEVO DEBATE DEL DERECHO AL OLVIDO

En 2016 el debate público en relación al derecho al olvido surgió de nueva cuenta, para discutirse desde el Senado de la República la necesidad de incorporar esta figura de manera expresa a las legislaciones en materia de protección de datos personales[251]. Ante esta discusión, se hizo un llamado a expertos de la academia, de la industria y del sector público, a fin de discutir las dimensiones del derecho al olvido. Uno de los grandes planteamientos fue la necesidad de informar que la garantía del derecho al olvido, podría derivar de la afectación de otros derechos humanos como el de libertad de expresión, el derecho a la verdad e información, y que esta tensión de derechos se resuelve mediante la necesaria ponderación de la garantía del derecho al olvido.

---

[251] *http://comunicacion.senado.gob.mx/index.php/informacion/boletines/30363-analizan-senado-e-inai-alcances-e-implicaciones-del-derecho-al-olvido.html.*

En este sentido, uno de los ejemplos más comunes es el relacionado a la exigibilidad del derecho al olvido *versus* los derechos de libertad de expresión o de acceso a la información en Internet, en donde se deberán considerar factores como el grado de exposición pública del solicitante, si se trata de información incorrecta, si involucra a un niño, niña o adolescente, o si la petición atenta contra la divulgación de información de interés público.

Aunado a lo anterior, se destaca que en México se ha hecho referencia al concepto de derecho al olvido para referir a la eliminación de información en el ciberespacio, pero a opinión de la autora, más bien estamos frente a un "derecho de desindexación", ya que, hasta el momento, se ha exigido a los buscadores desindexar la información, pero no se ha obligado a las fuentes originales a suprimir información. Una excepción a lo dicho, refiere a una solicitud de derecho al olvido en Colombia, en la que una ciudadana solicitó a Google eliminara resultados de búsqueda que la relacionaban con una investigación de trata de personas, de la que no fue hallada culpable y en la que la justicia colombiana, en lugar de ordenar al buscador la desindexación de información, ordenó directamente al medio informativo aclarara, en otra nota, que de la investigación se determinó la no responsabilidad en el delito mencionado de la titular de la solicitud; es decir, no se atenta contra el derecho a la verdad, "una persona estuvo involucrada en una investigación de trata de personas, pero en una nota aclaratoria se precisa que no fue determinada culpable por la autoridad competente"[252].

V. NATURALEZA JURÍDICA DEL DERECHO AL OLVIDO

Como se ha dicho, el derecho al olvido tiene su origen principalmente en dos fuentes: el caso Google España, de mayo de 2014, resuelto por el Tribunal de Justicia de la Unión Europea (en el que se exigió al buscador eliminar determinados resultados de información de un ciudadano español) y recientemente, en el Reglamento General de Protección de Datos de la Unión Europea.

---

[252] Disponible en: *https://www.ambitojuridico.com/BancoConocimiento/Educacion-y-Cultura/noti-141809-04-derecho-al-olvido-y-lista-clinton.*

En adición a lo anterior, el derecho al olvido también encuentra un antecedente importante en las legislaciones nacionales que reconocieron el derecho de protección de datos personales, incluyendo el derecho de cancelación y oposición que tiene el titular de un dato, respecto al tratamiento del mismo[253].

Para entender la naturaleza jurídica del llamado derecho al olvido, resulta pertinente dar una aproximación conceptual al mismo, considerando que, por lo novedoso de la denominación en el ámbito jurídico, existen pocas referencias bibliográficas que lo definan.

En este sentido, de acuerdo a Álvarez Caro, podría definirse el derecho al olvido, como el derecho a equivocarse o que una equivocación pasada no marque y determine la vida de un individuo que, por definición, no es otra cosa que un proceso evolutivo, una secuencia de aciertos y errores, siempre en proceso de conformación, de cambio y de evolución constante[254].

De acuerdo a la misma autora, se conoce como derecho al olvido, a un interés jurídicamente protegido de los ciudadanos que consiste en lograr efectivamente que sus datos personales no sean localizados por los buscadores en la Red. Es importante decir, que esta aproximación conceptual, refiere más bien, a la desindexación de la información en buscadores de Internet, sin que esto signifique que la información sea borrada de manera permanente, en el ciberespacio.

En este sentido, se plantean dos ámbitos de ejercicio de este derecho: el mundo físico y el ciberespacio, en el cual habría que diferenciar –como se dijo en líneas previas–, entre solicitudes de eliminación de información dirigidas a las fuentes originales que contienen dichos datos, o en su caso, solicitudes de desindexación de la información, dirigidas a los buscadores en Internet.

---

[253] En este sentido, el derecho de cancelación reconocido en las legislaciones nacionales en materia de protección de datos personales, tampoco garantiza un efectivo derecho al olvido en su dimensión más amplia, ya que la información se cancelará de la fuente de información en la que se contenía; sin embargo, eso no exime de la posibilidad de que dichos datos se hayan replicado a otras áreas en las que no se pueda tener más el control sobre la información, por lo que en la práctica, resultaría muy complejo salvaguardar este derecho.

[254] Álvarez Caro, María, *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital*, Madrid, Reus, 2015, p. 68.

Esta diferenciación resulta importante, ya que nos permite identificar discrepancias entre el ejercicio del derecho al olvido, y las peticiones de desindexación de información, que no garantizan el borrado de la información en Internet, y el objeto que persiguen, es simplemente, que no se pueda encontrar dicha información, a través de las búsquedas que se hagan en los motores destinados para tal fin.

Más aún, encontramos una aproximación conceptual del derecho al olvido en la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, en la que se reconoce este derecho, a través de la prerrogativa que tiene el titular del dato personal, para solicitar que se bloqueen en las listas de resultados de los buscadores, los vínculos que lleven a informaciones que le afecten, que sean obsoletas, falsas, erróneas, incompletas o irrelevantes, o simplemente no sean de interés público[255].

En relación al Reglamento General de Protección de Datos de la Unión Europea, el derecho al olvido se recoge como la consecuencia del derecho que tienen los titulares de datos personales a solicitar, y obtener de los responsables, que los datos personales sean suprimidos cuando, entre otros casos, estos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita.

En términos generales, se puede explicar el contenido del derecho al olvido, cuando de manera lícita se publica información, que posteriormente le perjudica de manera objetiva al titular de esos datos personales, y que el medio material que contiene esa información, resulta de acceso a todos (ciberespacio), teniendo un grado de exposición mayor, por lo que, en principio, el derecho al olvido, permite al titular del dato, oponerse a que su información continúe a disposición de terceros.

VI. DERECHO AL OLVIDO EN MÉXICO

La protección de datos personales en México, tiene un modelo híbrido que dicta disposiciones a través de dos leyes particulares, la primera aplicable al sector público y la segunda al sector privado; asimismo, se tienen disposiciones normativas

[255] Sentencia disponible en: *http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES.*

a nivel sectorial, que por ejemplo dictan mandatos respecto a los datos financieros, clínicos y fiscales.

Actualmente, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (ordenamiento que dicta las disposiciones a seguir para proteger los datos en el sector privado), reconoce los denominados derechos ARCO (derecho de acceso, rectificación, cancelación y oposición de datos personales). Para efectos de este análisis, los dos últimos citados, tienen finalidades similares a los objetivos del derecho al olvido, por lo que, a pesar de no estar mencionado con tal denominación, la legislación de datos para el sector privado reconoce el derecho a cancelar la información de una persona u oponerse al tratamiento de la misma.

Por otro lado, de acuerdo a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, también en el sector público, se deberá garantizar el derecho de cancelación de datos personales, siempre y cuando se señalen las causas que motiven solicitar la supresión de datos personales en registros o bases de datos del responsable de la información y el derecho de oposición del tratamiento de datos personales siempre que el titular de la información manifieste causas legítimas o la situación específica que motive la solicitud del cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.

En la legislación del sector público, se establecen los siguientes límites para el ejercicio del derecho de cancelación u oposición:

- No acreditar la titularidad del dato o la debida representación legal para solicitar la cancelación u oposición de la información;
- Cuando exista algún impedimento legal (ejemplo: en el caso de la negativa a solicitudes de cancelación de datos relacionados a la obligación de una autoridad de tratar información derivado de una de sus facultades conferidas por ley);
- Cuando se afecten derechos de terceros;
- Cuando se obstaculicen actuaciones judiciales o administrativas;

- Cuando exista resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la cancelación u oposición de los mismos;
- Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;
- Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular (ejemplo: solicitar la cancelación de datos relativos a la solicitud de un crédito otorgado por el Estado mexicano);
- Cuando en función de sus atribuciones legales, el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano; y
- Cuando los datos personales sean parte de la información de las entidades sujetas a la regulación y supervisión financiera.

Ante la negativa de algún representante del Estado mexicano respecto a la cancelación u oposición de datos personales, el titular de estos puede acudir al órgano garante a través de un recurso de revisión, para que el órgano especializado determine si la negativa es acorde a lo dispuesto por la norma, o en su caso, ordene la garantía de estos derechos.

Otro aspecto importante radica en que de acuerdo a la Ley de datos del sector público, los que estén en posesión del Estado mexicano deben cumplir el principio de calidad, y se entiende que este principio se agota cuando se proporcionaron directamente por el titular y hasta que este no manifiesta lo contrario.

VII. DERECHO AL OLVIDO EN EL CIBERESPACIO

La importancia que tiene el derecho al olvido en la economía digital, se explica considerando el valor que ha adquirido la información en el ciberespacio, ya que se pueden recolectar, procesar y transmitir grandes cúmulos de información, en tiempo real. Esto no ha sido ajeno para derechos como el de la privacidad y la protección de datos personales, ya que el grado de exposición en el que se pone al usuario de servicios tecnológicos es muy alto.

Como se ha dicho en líneas previas, el ejercicio del derecho al olvido, se puede hacer en ámbitos físicos y digitales. En este apartado analizaremos algunas de las complejidades jurídicas, relativas a borrar o desindexar información en Internet, precisando que, por las características de la Red, y la facilidad de compartir información en el ciberespacio, resultaría casi imposible hablar de una efectiva garantía –en un sentido amplio– del derecho al olvido.

En este sentido, podemos diferenciar dos aspectos: el técnico y el jurídico. El aspecto técnico, referirá a solicitudes de desindexación de la información en los motores de búsqueda, y el segundo aspecto relativo al ámbito jurídico, normalmente refiere al ejercicio del derecho de cancelación del dato personal, o incluso en algunas situaciones particulares, al derecho de oposición respecto al tratamiento de datos personales, aunque la información se conserve, de manera oculta, en la fuente original de la información, es decir, sin que se garantice un borrado permanente de la misma.

Para entender el fenómeno de supresión de la información en Internet, y las complejidades jurídicas y técnicas que esto conlleva, es importante señalar que el reconocimiento de los derechos humanos y su incorporación a las legislaciones nacionales, se hicieron previo al auge del desarrollo tecnológico, por lo que la lógica de la norma, atiende a contextos distintos, que, a los retos planteados hoy día, desde el ciberespacio. También es relevante mencionar que el derecho al olvido, no es un derecho en sentido genérico, y tampoco garantiza borrar toda la información en Internet.

Una vez que se ha planteado lo anterior, resulta importante decir que los derechos humanos e Internet, comparten una característica común: ambos son globales y universales; sin embargo, la incorporación de los derechos humanos a los textos normativos en los ámbitos nacionales, hace complejo que se pueda garantizar desde la jurisdicción y competencia de los países, lo que sucede en el ciberespacio, y el derecho al olvido no es la excepción.

Un ejemplo de ello, lo constituye la autoridad garante del derecho de protección de datos personales en México, que, a través de diversos intentos, ha buscado que Google México, reconozca la aplicación de la legislación nacional en la materia, y atienda a las recomendaciones que desde dicha institución se hacen; sin

embargo, el buscador, como parte de su tradicional estrategia legal, no reconoce las jurisdicciones locales en la materia. Esta problemática ha sido resuelta por la Unión Europea, a través de normas comunitarias sólidas en materia de protección de datos personales, cuyo cumplimiento está vinculado directamente a acuerdos comerciales, por lo que estando en un continente con pocos intentos de integración regional, más allá de los temas comerciales, se podría pensar en los acuerdos de colaboración, las buenas prácticas y los esquemas de gobernanza, como instrumentos de protección de los datos digitales de las personas.

No obstante lo anterior, la garantía del derecho al olvido no puede ser general y plena, ya que habrá información que es del interés de todos conocer, y que, atendiendo a su naturaleza, podrá privilegiarse derechos como la libertad de expresión, libertad informativa, acceso a la información y el derecho a la verdad, en Internet. Esto también está vinculado al principio de neutralidad de la Red, el cual busca reservar la estructura original de Internet, y no privilegiar cierta información, respecto a otra, de acuerdo, por ejemplo, a la zona geográfica en la que se realice una búsqueda en Internet.

En este sentido, tanto las fuentes originales de la información, así como los buscadores de Internet, juegan un papel importante en garantizar derechos como la libertad de expresión, ya que, de los protocolos de atención a las solicitudes de cancelación y supresión de datos, se podría garantizar o no, la construcción colectiva de la verdad, o garantizar espacios de ejercicio del derecho de libertad de expresión en Internet.

Con el objetivo de conocer las solicitudes de privacidad en Europa, relativas a las retiradas de resultados de búsqueda, Google ha recibido 586,926 solicitudes de retirada de resultados en su motor de búsqueda. De ese número, dictaminó que el 56.8% de esas solicitudes no eran procedentes y el 43.2% de solicitudes concluyó en la retirada de información. Uno de los ejemplos de solicitudes que sí fueron concedidas, giran en torno a retirar información de responsables de delitos menores en Reino Unido[256].

---

[256] *Reporte de Transparencia Google 2016, https://www.google.com/transparencyreport/removals/europeprivacy/?hl=es.*

Respecto al ejercicio del derecho al olvido por parte de niñas, niños y adolescentes en Internet, el Reglamento General de Protección de Datos de la Unión Europea, establece que la edad en la que los menores pueden otorgar por sí mismos su consentimiento para el tratamiento de sus datos personales en el ámbito de los servicios de la sociedad de la información (por ejemplo, redes sociales) es de 16 años. Sin embargo, permite reducir esa edad y que cada Estado miembro establezca la suya propia, estableciendo un parámetro límite de 13 años. Por debajo de esa edad, será necesario el consentimiento de padres o tutores. Esto quiere decir, que la representación del ejercicio del derecho al olvido, en caso de que hubiera una solicitud de supresión en pugna, tendría que ejercerse por los padres o tutores.

Un elemento interesante del derecho a la supresión de datos personales, establecido en el Reglamento General de Protección de Datos de la Unión Europea, es que su ámbito de aplicación será a responsables y encargados del tratamiento de datos establecidos en la Unión Europea, y habrá extraterritorialidad de la norma, respecto a los responsables y encargados no establecidos en el continente europeo, pero que realicen tratamientos derivados de oferta de bienes y servicios o del monitoreo del comportamiento de ciudadanos de la Unión Europea, en ámbitos digitales.

Se ha hablado mucho del Reglamento General de Protección de Datos de la Unión Europea, pero es importante mencionar que la mayoría de países en Iberoamérica, se encuentran desarrollando legislaciones en materia de protección de datos personales y dimensionando el derecho al olvido, por lo que el grado de discusión no ha permeado, a las categorías de análisis que se tendrían que realizar las autoridades garantes del derecho de protección de datos personales, a fin de discernir entre la información que debe o no, ser borrada en Internet.

Finalmente, la transparencia por parte de los buscadores en Internet, desempeña un papel muy importante para la confianza de los usuarios de servicios digitales y para la garantía de derechos como el de la libertad de expresión, ya que en la medida que se conozcan los tipos de solicitudes vinculadas al derecho al olvido que reciben los buscadores, el número de solicitudes atendidas, los criterios y motivos de atención o negativa de la solicitud, podremos establecer precedentes

en el ejercicio de este derecho, buscando siempre un balance entre la supresión de datos, la libertad de expresión e informativa y el acceso a la información.

VIII. CONCLUSIÓN

A manera de conclusión de este análisis, decimos que el derecho al olvido por sí mismo, no puede garantizarse de manera general, ya que se deberán establecer categorías, –verbigracia, las relacionadas a derechos de la personalidad, derechos patrimoniales o libertades informativas–. Asimismo, hoy día, en el Derecho tradicional, existen figuras jurídicas que podrían ayudar frente a la divulgación excesiva de información de la vida personal, información errónea o incorrecta; como son el derecho de réplica, el derecho de propia imagen y las compensaciones del Derecho Civil por daños morales.

Se enfatiza la necesidad de no dictar reglas generales en la garantía del derecho al olvido y ponderar entre los derechos humanos que se encuentren en tensión.

También, la ley deberá diferenciar la figura del intermediario con la del Responsable de los datos divulgados por usuarios. En el mismo sentido, las legislaciones deberán garantizar un control del procedimiento contra el exceso de eliminación de la información, a fin de lograr equilibrio entre la protección tradicional otorgada a derechos como la libertad de expresión y el derecho a la verdad frente argumentos relacionados a la intimidad, la privacidad, la vida privada y la protección de datos personales. En el mismo sentido, bajo la premisa de pensar global y actuar local, se deberá privilegiar la neutralidad de Internet.

Por otro lado, destacar que la información puesta a disposición a través del ciberespacio, puede ser replicada en muchos otros sitios más, por lo que tener el control de la misma no resulta fácil[257].

Finalmente, a pesar de que se utilicen como sinónimos, existen claras diferencias en el alcance de conceptos como derecho al olvido, derecho de supresión, derecho de cancelación y oposición, y derecho de desindexación, mayormente utilizado este último, para el ámbito digital.

---

[257] En opinión de la autora, solo la técnica podrá hacer frente al borrado de la información en Internet, sin que esto signifique que la ley, por sí misma, podrá resolver el gran planteamiento del derecho al olvido.

IX. FUENTES DE INFORMACIÓN

1. *Bibliografía*

ÁLVAREZ CARO, María, *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital*, Madrid, Reus, 2015.

Reporte de Transparencia Google 2016, *https://www.google.com/transparencyreport/removals/europeprivacy/?hl=es.*

Resolución del proceso sancionatorio abierto por el INAI contra Google México: http://inicio.ifai.org.mx/pdf/resoluciones/2014/PPD%2094.pdf.

2. *Sitios de Internet*

https://www.ambitojuridico.com/BancoConocimiento/Educacion-y-Cultura/noti-141809-04-derecho-al-olvido-y-lista-clinton.

http://comunicacion.senado.gob.mx/index.php/informacion/boletines/30363-analizan-senado-e-inai-alcances-e-implicaciones-del-derecho-al-olvido.html.

http://revistafortuna.com.mx/opciones/archivo/2007/febrero/htm/fraude_estrella_blanca_vamos_mexico.htm.

CAPÍTULO DÉCIMO TERCERO
Inteligencia Artificial y protección de datos

Ángel David SUMANO CORREA[258]

SUMARIO

I. INTRODUCCIÓN

El que escribe las siguientes líneas tiene el propósito de que sus palabras sean amigables y de fácil comprensión, no solo para los abogados, sino para cualquier persona que le apasionen temas como la tecnología o los datos personales. Como abogados debemos comprender que el mundo del Derecho es uno *antes* y *después* de Internet, así como el mundo de la música fue uno antes y después de los Beatles, quienes revolucionaron la industria musical *rompiendo paradigmas* e inspiraron a las nuevas generaciones a crear nuevos estilos musicales, la tecnología por su parte, inspira a las nuevas generaciones de nuestros días, a crear el próximo Apple, Uber,

[258] Abogado especialista en Inteligencia Artificial aplicada al Derecho. Egresado por la Facultad de Derecho de la UNAM, con ocho años de experiencia en protección de datos personales. Especialista en aspectos legales del comercio electrónico. Cofundador de Fractal Abogados, Startup Legaltech, que ha programado el primer *chatbot* a nivel LATAM, que brinda asesorías legales en registro de marcas, constitución de empresas y despidos laborales. Ha impartido diversas ponencias sobre I.A. aplicada al Derecho en universidades y foros legales.

Tesla, o Airbnb. Y entonces, ¿quiénes somos nosotros, como abogados, para *cortarles las alas* a quienes buscan impactar de manera positiva a la sociedad a través del uso de la tecnología, si nos centramos solo en el argumento de que ésta es un riesgo para la privacidad de nuestros datos personales? Steve Jobs decía: "La computadora es la herramienta más notable que el hombre ha inventado y es el equivalente de una bicicleta para nuestras mentes"[259].

Esto lo dijo mientras explicaba un estudio científico que había leído, acerca de la medición de la eficiencia de la fuerza de movimiento de varias especies en el planeta, incluido el ser humano. Dentro del estudio, el cóndor aparecía en la cima de la lista al ser la especie que menos energía utilizaba para desplazarse a lo largo de un kilómetro, mientras que el ser humano aparecía por debajo ocupando el tercer lugar; pero cuando hicieron la misma medición dándole al hombre una bicicleta, éste rebasó por mucho la eficiencia de fuerza del movimiento del cóndor. Justamente a eso se refería Steve Jobs, la tecnología *amplifica* dramáticamente nuestras habilidades innatas. Entonces, ¿por qué hoy generamos marcos regulatorios que pareciera tienen el objetivo de inhibir el avance tecnológico? Pienso que parte de la respuesta tiene que ver con el contexto en el que vivimos, a diferencia de hace veinte años, el uso de la tecnología no permitía tener acceso a cantidades inconmensurables de datos personales, como los que hoy es posible tener acceso todos los días. Dicho lo anterior y con esto en mente, quiero compartir con el lector un punto de vista, acerca de la Inteligencia Artificial y la protección de datos personales, no solamente con un enfoque jurídico, sino también en parte técnico, emprendedor y con tintes de innovación. Porque si de algo estoy convencido, es que el Derecho es por esencia un cúmulo de esos tres factores, aunque de pronto se nos olvide a los abogados más de lo que debería.

---

[259] Jobs, Steve, *La computadora es como una bicicleta para nuestras mentes*, *http://www.planeta-apple.com/2011/07/steve-jobs-la-computadora-es-como-una.html.*

II. LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y NUESTRA PRIVACIDAD: ¿"AGUA" Y "ACEITE"?

Las herramientas que el hombre ha fabricado a lo largo de la historia para lograr evolucionar como sociedad son, precisamente eso, herramientas que permiten progreso constante. Un objeto, por sí mismo, no produce un daño intencional a otra persona, sino más bien es el uso que el ser humano puede darle, para que provoque menoscabos a un tercero. En el año de 1903, cuando los hermanos Wright soñaban conquistar los cielos y se convirtieron en los pioneros de la aviación moderna, nadie imaginaría que en el siglo próximo alguien idearía utilizar ese *objeto de progreso* como un arma letal, en aquel fatídico atentado del 11 de septiembre de 2001, en contra de las Torres Gemelas en la Ciudad de Nueva York, Estados Unidos. A raíz de ello, la seguridad y las normas de vuelo se tornaron mucho más estrictas, pero nadie propuso prohibir el uso de los aviones, eso hubiera resultado ilógico, ¿cierto? (no se castiga a la tecnología, sino a quien realiza un mal uso de ella). En este sentido, el fin último de las leyes es regular la conducta de las personas en sociedad, para evitar que actúen transgrediendo los derechos y libertades de terceros y, cuando no es posible lograr dicho fin, las leyes aplican las sanciones que en ellas se establecen, pudiendo ser sanciones pecuniarias, privativas de la libertad, o incluso costar la vida, dependiendo la legislación de la región en que se aplique.

Antes del surgimiento de Internet y la irrupción de las tecnologías de la información, las leyes de cada país eran diseñadas únicamente para regular dentro de un territorio perfectamente delimitado, por tanto, no había mayor problema en establecer el alcance territorial de cada ley respetándose la soberanía de cada país.

Sin embargo, el escenario actual ha cambiado, ya que pasamos de vivir en un mundo globalizado, a vivir en un mundo *hiperconectado,* lo cual representa grandes retos para los gobiernos de todos los países del mundo... ¿A cuáles retos me refiero? En realidad son varios, pero en particular me refiero a uno de los más importantes: *la privacidad y protección de nuestros datos personales*. Analicémoslo de una manera sencilla. En los años ochenta nuestra información se encontraba plasmada en papel y la documentación que contenía nuestros datos personales, se hallaba en espacios

físicos como archiveros, cajones de escritorio, en el buró de nuestra sala, etc. De pronto, en 1991 con el nacimiento de la *World Wide Web*, nuestra información comienza a compartirse a través de la Red y entrando por primera vez al mundo del *ciberespacio*. Pero aún faltaba un brinco exponencial, cuando en 1998 nace Google[260], quien no solo revolucionaría los modelos de negocio en la era digital, sino que dio en el *clavo* al comprender que nuestros datos personales en la Red representaban un tremendo activo por el cual las empresas estaban (*y siguen estando*) dispuestas a pagar millones de dólares, surgiendo con ello el nuevo petróleo: *nuestros datos personales en la Red*[261]. A raíz de la gran relevancia que cobró el tratamiento de nuestra información a través de Internet, los gobiernos de todo el mundo, principalmente Europa a través de la Directiva 95/46/CE de 1995, buscaron legislar al respecto sobre este nuevo fenómeno relacionado al flujo masivo de datos personales en un nuevo territorio equiparable a una nación: Internet.

En el año 2010, se expidió en México la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), cuya influencia europea, particularmente de la Ley de Protección de Datos Española, erige como un derecho humano a la protección de datos personales dentro de nuestra Constitución Política, ubicándolo en los Artículos 6o. y 16 en las reformas llevadas a cabo a cada uno de ellos en los años 2007 y 2009, respectivamente. De esta manera, México se alineaba al compromiso internacional de países europeos, tales como Alemania, España, Francia, e igualmente Latinoamericanos como Argentina, Chile, Uruguay, Brasil, por mencionar algunos, en su compromiso por la protección de nuestros datos personales. Vale la pena hacer mención al lector brevemente, que en el año 2002 fue creada la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (que precedió a la LFPPP), dentro de la cual se reconoce por primera vez la protección de los datos personales, aunque limitándose únicamente a las bases de datos del sector público a nivel federal. Así las cosas, la citada reforma al Artículo 16 constitucional, además de reconocer y dar contenido al derecho a la pro-

[260] Disponible en: *https://es.wikipedia.org/wiki/Google.*

[261] Remolina Angarita, Nelson, *XIV Congreso Iberoamericano de Derecho e Informática,* 2010, *https://www.youtube.com/watch?v=sdP9I60Olfw.*

tección de datos personales, estableció los derechos que tiene cualquier persona para ejercer el acceso, rectificación, cancelación y oposición sobre sus datos personales (denominados por su acrónimo como derechos ARCO) frente a cualquier persona física o moral que dé tratamiento a estos con fines de obtener un lucro económico, por supuesto lícito.

Entonces, llegado este punto en el que se ha hecho mención sobre las acciones legislativas a nivel internacional, incluido por supuesto México, que se han llevado a cabo para proteger nuestros datos personales, principalmente en Internet incluidas también hoy las nuevas tecnologías de la información debido al *boom* que han tenido en los años recientes; se abre la interrogante para reflexionar acerca de si el Internet y las nuevas tecnologías de la información son polos opuestos a la privacidad de nuestros datos personales, dicho en una expresión coloquial, ¿son como el *agua* y el *aceite*? Podría pensarse que sí, pero aquí abro una nueva pregunta para la reflexión, ¿concibes tu mundo hoy sin Facebook, WhatsApp, Netflix, YouTube, Uber, Google, por mencionar algunos? Todas y cada una de las empresas antes citadas, como muchas más en esta era de la economía digital, viven y crecen gracias al consumo masivo de nuestros datos personales, pero al mismo tiempo, mejoran su calidad de servicio y nuestra experiencia de usuario gracias a ello. Con lo anterior no estoy pretendiendo que la privacidad de nuestros datos personales deba quedar expuesta, sino simplemente tal vez sea que en la presente época de las nuevas tecnologías de la información e Internet, el concepto de lo privado, entendido *(de acuerdo a la Real Academia Española)*, como aquello que se ejecuta a vista de pocos, familiar y domésticamente sin formalidad, hoy se está transformando. ¿Cuántas veces no hemos publicado imágenes, pensamientos e incluso sentimientos en redes sociales por voluntad propia? ¿Cuántas aplicaciones móviles gratuitas no hemos descargado a cambio de compartirles nuestros datos personales? ¿A cuántos sitios de comercio electrónico (nacionales y extranjeros) hemos accedido en los que ni siquiera leemos el aviso de privacidad? Si hoy la moneda de cambio de las nuevas tecnologías de la información e Internet son nuestros datos personales, por qué no evolucionar hacia una definición integral sobre la privacidad de nuestra información en el entorno digital; construir una definición más allá de lo netamente jurídi-

co, que involucre también disciplinas del mundo de la programación, ciencias de datos, marketing digital, y aquellas especializadas en manejo de datos personales automatizados, con el objetivo de comprender de mejor manera lo que se entiende por privacidad de nuestra información en tiempos de Internet y las nuevas tecnologías de la información... Recordemos que el *objeto de progreso* no hace daño por sí mismo a terceros, sino es el ser humano quien da un uso indebido pudiendo generar daños, entonces, no sería más bien que, ¿el ser humano y la privacidad, son el "*agua"* y el "*aceite"*?

III. INTELIGENCIA ARTIFICIAL

Cuando en los años cuarenta se pusieron a funcionar las primeras computadoras (esos roperos de metal, llenos de bulbos), se les llamó "cerebros electrónicos", ya que podían hacer sumas. Esto hizo imaginar a muchos: "Mañana las máquinas conversarán con nosotros". Y entonces el cine, los dibujos animados y la televisión se poblaron de robots "inteligentísimos", aunque de movimientos algo torpes, que acompañaban a los humanos en toda clase de mundos[262]. Queda clara la fascinación del ser humano por desarrollar sistemas inteligentes que puedan tener autonomía propia con capacidad de procesamiento cognitivo, recientemente películas como "Ex Machina" (2015), "*Her*" (2013), "I, robot" (2004), nos muestran un mundo en donde la convivencia entre humanos y Sistemas de Inteligencia Artificial será algo tan común como respirar. Pero, ¿qué es la Inteligencia Artificial? En 1956, John McCarthy, profesor de la Universidad de Stanford, acuñó esa expresión y la definió como: "La ciencia y la ingeniería de fabricar máquinas inteligentes, en especial programas inteligentes de computación", entendiendo por "inteligente", "la parte de la informática orientada a obtener resultados".

Coloquialmente, también el término Inteligencia Artificial se aplica cuando una máquina imita las funciones cognitivas que los humanos asocian con otras mentes humanas, como por ejemplo: "aprender" y "resolver problemas". Vincent Tora, Doctor en Informática por la Universidad Politécnica de Cataluyna e inves-

[262] Gómez Herrera, Renato, *La Inteligencia Artificial. ¿Hacia dónde nos lleva?*, *http://www.comoves.unam.mx/assets/revista/2/la-inteligencia-artificial-hacia-donde-nos-lleva.pdf.*

tigador científico del Instituto de Investigación en Inteligencia Artificial explica, aunque existen diferentes puntos de vista sobre qué es la Inteligencia Artificial, hay un acuerdo importante sobre cuáles son los resultados atribuibles a esta rama de la Informática, así como a la clasificación de los métodos y técnicas desarrollados, los cuales divide en cuatro grandes temas:

1. Resolución de problemas y búsqueda. La Inteligencia Artificial tiene como objetivo resolver problemas de índole muy diferente. Para poder cumplir este objetivo dado un problema, es necesario formalizarlo para resolverlo. Este tema se centra en cómo hacer lo primero y las formas de resolución;
2. Representación del conocimiento y sistemas basados en el conocimiento. Es frecuente que los programas en Inteligencia Artificial necesiten incorporar conocimiento del dominio de aplicación (por ejemplo, en Medicina) para poder resolver los problemas;
3. Aprendizaje automático. El rendimiento de un programa puede incrementarse si este aprende de la actividad realizada y de sus propios errores. Se han desarrollado métodos con este objetivo. Existen también herramientas que permiten extraer conocimiento a partir de bases de datos.
4. Inteligencia artificial distribuida. Durante sus primeros años, la Inteligencia Artificial era monolítica. Ahora, con los ordenadores multiprocesador e Internet, hay interés en soluciones distribuidas. Estas van desde versiones paralelas de métodos ya existentes, a nuevos problemas relacionados con los agentes autónomos (programas software con autonomía para tomar decisiones e interaccionar con otros).

Los expertos señalan que, un sistema basado en la Inteligencia Artificial debe disponer de un sistema codificado de reglas para resolver los supuestos que se le plantean, a partir de la comprensión de la expresión de esa tarea, e igualmente debe ser capaz de interactuar con el usuario, para precisar o refinar el alcance de la tarea solicitada y, finalmente, debe ser capaz de aprender, dejando identificadas para el futuro las mejores opciones para un supuesto concreto, a la vez que descar-

ta las menos aconsejables. Lo anteriormente explicado, ha tenido sus aplicaciones prácticas en el mundo real, tal es el caso, por ejemplo, de *Deep Blue*, que en el año de 1997 derrotó al campeón mundial Gary Kaspárov[263]. Asimismo, también el sistema de inteligencia artificial *Watson*, fue capaz de vencer a los mejores y más brillantes participantes humanos en un concurso de cultura general norteamericano, llamado "Jeopardy", en el año 2011[264].

IV. ¿LA INTELIGENCIA ARTIFICIAL PONE EN RIESGO LA PRIVACIDAD DE NUESTROS DATOS?

Actualmente, en todo el mundo se debate acerca de los pros y contras que puede traer consigo el desarrollo de la Inteligencia Artificial, siendo uno de los puntos que más preocupa la falta de regulación sobre estos sistemas inteligentes que día a día van ganando más terreno en nuestra sociedad. Uno podría pensar que aún no estamos viviendo entre robots, siendo que la realidad es otra. Tal vez no estamos coexistiendo entre robots con forma humana, pero ya interactuamos con ellos e incluso les brindamos nuestra información. ¿Cuántas veces al día hablas con *Siri*, el asistente de reconocimiento de voz de Iphone, para pedirle que haga una llamada telefónica o agende una reunión en tu calendario? O, ¿cuántos kilómetros corriste con tu reloj inteligente puesto, que mide tu ritmo cardiaco para darte las mejores recomendaciones para tu entrenamiento? En el primer caso, estás interactuando con un sistema de Inteligencia Artificial de reconocimiento de voz, que entre otras cosas, puede determinar tu estado de ánimo atendiendo a factores como el volumen e intensidad de tu voz. En el segundo, estás brindando información de salud a un sistema inteligente que conoce y reconoce datos relacionados a tu salud y podría detectar si eres potencial sujeto de padecer alguna afectación cardíaca. Todo esto, por mencionar solo algunos ejemplos, pero si además, esto lo llevamos multiplicado a la "n" potencia, por las millones de personas que a diario realizan estas mismas actividades, podemos darnos una idea de la cantidad industrial de datos

---

[263] García, Leontxo, "'Deep Blue' gana a Kaspárov al estilo de Kárpov", *El País,* Nueva York, 5 de mayo de 1997, *https://elpais.com/diario/1997/05/05/deportes/862783217_850215.html.*

[264] *Supercomputadora de IBM vence a campeones de Jeopardy*, Redacción BBC Mundo, *https://www.bbc.com/mundo/noticias/2011/02/110217_ibm_computadora_jeopardy_en.*

personales que hoy estamos brindado a la Inteligencia Artificial, muchas veces sin ser conscientes de ello, tal vez, porque consideramos que no se trata de un robot solo por el hecho de no tener una forma humana.

En este sentido, en el Foro Económico Mundial celebrado durante 2017 en China, uno de los temas a debatir fue precisamente el relacionado con la aplicación de la Inteligencia Artificial en nuestra sociedad. El panel que trató sobre el mismo fue denominado: "*Artificial Intelligence Unleashed*" (Inteligencia Artificial Desatada); dentro del cual participaron, por supuesto, expertos sobre la materia. Realmente se trató de un debate apasionante, en donde cada uno de los panelistas, a través de fundamentados y científicos puntos de vista, más que ir en contra de la Inteligencia Artificial y percibirla como una amenaza a nuestra privacidad, plantearon que si bien no existe aún legislación relativa a los temas de Inteligencia Artificial o comienzan a surgir de manera incipiente, la solución no es legislar al respecto de una manera restrictiva, sino más bien, primero debe comprenderse correctamente cómo funcionan estos sistemas inteligentes, su estructura e inclusive quiénes o cómo operan, refiriéndose con ello a los ingenieros en sistemas, programadores, desarrolladores, científicos de datos, mineros de datos, entre otros.

Uno de los puntos clave fue cuando se mencionó que, a diferencia de hace 20 años, un ingeniero en sistemas o un programador no necesitaban tener desarrolladas habilidades relativas a la Ética sobre el manejo de datos personales, es decir, jamás como hoy, sus perfiles y roles habían tenido un papel crucial, fundamental y directo en el manejo de nuestra información.

Dentro del mismo Foro se mencionó que tal vez las regulaciones concernientes a nivel internacional relativas al tema de protección de datos personales, pueden estar un poco anticuadas u obsoletas debido, justamente, a que no se ha comprendido técnicamente por parte del legislador, cómo funcionan estos sistemas inteligentes, ya que realmente se trata de un tema técnico de alto nivel que debe ser comprendido desde adentro, es decir, desde el código de programación, para posteriormente plantearlo de manera inteligente y documentada en el código de la ley.

Si bien es cierto, estos sistemas de Inteligencia Artificial, efectivamente procesan y aprenden de nuestra información, los panelistas expertos coincidieron en que

realmente aquella no representa un peligro, a diferencia de lo que muchas personas piensan, argumentando sin fundamento que estos sistemas inteligentes podrían tornarse en nuestra contra (al estilo *Skynet*), más bien no se trata de las máquinas en contra de nosotros, sino de las máquinas ayudándonos a nosotros como especie. Efectivamente, los datos personales que se procesan generan un valor tremendo, pero no por ello quiere decir que esto representa un peligro en sí mismo, más bien, otra de las claves fundamentales, mencionada por los expertos en el panel fue insistir en sensibilizar a los ingenieros que operan estos sistemas inteligentes. De tal suerte que, es fundamental generar un sentido de confianza y seguridad desde los valores éticos y morales de los profesionales en quienes se encuentra depositado el acceso y procesamiento de nuestros datos personales. Finalmente, se mencionó también que deben impulsarse políticas que ayuden a garantizar el cumplimiento de estos objetivos, pero de ninguna manera ir enfocadas a frenar y restringir el avance de la Inteligencia Artificial. Es decir, debemos re-educarnos en cuanto a la cultura de la protección de nuestros datos personales, tanto quienes somos usuarios de la Inteligencia Artificial, como quienes son los responsables de su creación, manejo y optimización. Nuevamente se insiste en que, no es el objeto de progreso malo por sí mismo, sino quienes lo utilizan para un fin indebido, en este caso, el manejo de nuestros datos personales a través de la Inteligencia Artificial.

V. INTELIGENCIA ARTIFICIAL, ¿APLICADA AL DERECHO?

Si hay un tema actualmente que cause más controversia que la Inteligencia Artificial, es la Inteligencia Artificial aplicada al Derecho. No es la intención abordar, por el momento, éste tema a detalle toda vez que nos estamos enfocando mayormente a lo relativo a la relación entre Inteligencia Artificial y privacidad de datos, no obstante, es de hacer notar que sí existe una relación íntima con éste tema. ¿Cómo? Primero, el mundo del Derecho deber evolucionar y aprovechar las ventajas que representan hoy los sistemas inteligentes. Segundo, echar mano de ellos representaría un beneficio en la impartición de justicia al automatizar procesos que hoy en día, solamente generan gasto de tiempo y de dinero a los tribunales. El mundo del Derecho es una gran fotografía, ya que existen varios actores, no solamente los juz-

gados y tribunales, sino también los despachos y firmas de abogados, a quienes no parece interesarles mucho involucrarse en temas de Inteligencia Artificial.

Richard Susskind, señala en su libro *Tomorrow´s Lawyer*: "Lawyers have a 'window of opportunity' before technological changes in the 2020's transform the way they work".

Esto refiere precisamente a que muchas de las funciones que el abogado lleva a cabo en su día a día, ya pueden ser aprendidas por la inteligencia artificial. Uno de ellos, las asesorías legales. ¿Cómo? Si lo analizamos como abogados, cuando brindamos una asesoría legal siempre seguimos un mismo patrón, independientemente del tema del que se trate la asesoría:

- Analizar;
- Consultar;
- Valorar; y
- Resolver.

Es a lo que he denominado el principio "ACVR" por su acrónimo. Siguiendo esta estructura, el abogado "analiza" la consulta que le hace el cliente; posteriormente, "Consulta" en la ley, jurisprudencia, expedientes o con sus demás colegas, cuál es la mejor respuesta a la consulta planteada; luego, "valora" con los elementos que obtuvo de su consulta para generar la mejor respuesta; y, finalmente, "resuelve" dando una respuesta a quien le está realizando la consulta.

Esto mismo puede ser aprendido por un sistema de Inteligencia Artificial. Aunque insisto, tal vez no es objeto de este estudio propiamente el tema aquí abordado, sin embargo, como abogados no podemos ser ajenos a los avances de la tecnología, por tanto, si hemos venido hablando de privacidad de datos en tiempos de las nuevas tecnologías de la información e Internet, ¿no sería sensato que los abogados nos involucráramos más en temas tecnológicos, desde la raíz? Es decir, el tema de privacidad de datos requiere igualmente un perfil técnico, por tanto, si como abogados nos adentramos en el uso de estas tecnologías, podremos comprender de mejor manera cuáles son los posibles riesgos que habría que regular, sin generar un riesgo inhibidor del avance tecnológico, ya que nosotros mismos

estaríamos comprendiendo cómo funcionan estos sistemas, es decir, qué mejor que abogados y programadores colaborando conjuntamente en temas de Inteligencia Artificial, para diseñar también las estrategias, políticas, leyes y planes necesarios, que promuevan la protección y privacidad de nuestra información. Al menos, este es el punto de vista que quien escribe estas líneas le comparte al lector.

VI. CONCLUSIÓN

Vivimos en una era de avances tecnológicos sin precedentes, donde la expresión: "El cielo es el límite para la imaginación", considero ha quedado corta. Más que nunca, se trata de comprender a la tecnología, no solo de regularla o incluso, coartarla. Si bien, nuestros datos personales son de gran relevancia para ser protegidos y tutelados por la leyes, no debemos perder de vista que el objetivo principal en esta era de las nuevas tecnologías de la información, es transformar los datos que diariamente se generan, en mayores avances para la humanidad, claro ejemplo de ello, es la Medicina, área en la cual la tecnología ha permitido que sistemas de inteligencia artificial puedan actuar de manera preventiva diagnosticando a pacientes de una mejor manera en que lo haría un médico, todo gracias al gran banco de información que poseen estos sistemas inteligentes.

México tiene una gran oportunidad de ser pionero en temas de legislación en protección de datos, y puedo afirmarlo con conocimiento de causa, ya que el desarrollo exponencial de emprendimientos por el que atraviesa nuestro país, gracias al impulso de diversas incubadoras públicas y privadas, que fomentan el desarrollo de proyectos de emprendedores de alto impacto o de base tecnológica, están colocando a México como punta de lanza en temas de innovación en esa materia a nivel Latinoamérica, pero hay un *pequeño* detalle, la inmensa mayoría de estos proyectos, hallan su fortaleza y modelos de negocio en el procesamiento automatizado de datos personales e inclusión de inteligencia artificial, y por lo tanto, si nuestras leyes en este aspecto, son restrictivas previo a ser comprensivas, estamos nosotros mismos como país, "*poniéndonos el pie*" como coloquialmente se dice.

Entonces, la pregunta es, ¿qué vamos a hacer al respecto? ¿Nos vamos a in-

volucrar de una mejor manera en aspectos tecnológicos los abogados para generar legislaciones actuales? Es momento de abrirnos a nuevas disciplinas, de entender, nos guste o no, el software se comió al mundo, y que hoy una de las formas más inteligentes de resolver los retos que tenemos en materia de protección de datos personales en nuestro país, relacionado al uso de las nuevas tecnologías de la información, Internet e Inteligencia Artificial, es vivirlas desde adentro, no solo detrás del ordenador, redactando leyes que, comparadas con la velocidad y avance tecnológico, muy probablemente quedarán obsoletas para cuando hayan sido publicadas.

VII. FUENTES DE INFORMACIÓN

1. *Bibliografía*

GARCÍA, Leontxo, "'Deep Blue' gana a Kaspárov al estilo de Kárpov", *El País*, Nueva York, 5 mayo 1997, *https://elpais.com/diario/1997/05/05/deportes/862783217_850215.html.*

GÓMEZ HERRERA, Renato, *La Inteligencia Artificial. ¿Hacia dónde nos lleva?*, *http://www.comoves.unam.mx/assets/revista/2/la-inteligencia-artificial-hacia-donde-nos-lleva.pdf.*

JOBS, Steve, *La computadora es como una bicicleta para nuestras mentes*, *http://www.planeta-apple.com/2011/07/steve-jobs-la-computadora-es-como-una.html.*

REMOLINA ANGARITA, Nelson, *XIV Congreso Iberoamericano de Derecho e Informática*, 2010, *https://www.youtube.com/watch?v=sdP9I60Olfw.*

Supercomputadora de IBM vence a campeones de Jeopardy, Redacción BBC Mundo, *https://www.bbc.com/mundo/noticias/2011/02/110217_ibm_computadora_jeopardy_en.*

2. *Normatividad*

Constitución Política de los Estados Unidos Mexicanos, http://ordenjuridico.gob.mx/constitucion.php.

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), *https://www.boe.es/doue/2016/119/L00001-00088.pdf.*

3. *Sitios de Internet*

https://es.wikipedia.org/wiki/Google.

CAPÍTULO DÉCIMO CUARTO
Gobernanza digital y datos abiertos

Ernesto IBARRA[265]

SUMARIO

I. INTRODUCCIÓN

El desarrollo habitual de las actividades de las personas se ha visto impactado por las tecnologías de la información y comunicación (en adelante TIC); el uso generalizado de estas tecnologías, el acceso a la información junto con la libertad de expresión y la gran oportunidad para la innovación, desarrollo económico y social son componentes propios de este paradigma llamado s*ociedad de la información* y del *conocimiento*. La innovación con la expresión de ideas, son una necesidad humana básica y, con el apoyo adecuado de la tecnología, permite incrementar exponencialmente los resultados y alcances con un impacto favorable en el desarrollo económico, político y sociocultural.

[265] Licenciado en Derecho por la FES Acatlán-UNAM y Maestro en Derecho por la Facultad de Derecho-CU-UNAM. Cursó la Maestría en Ciencias Jurídicas y está doctorando en la Universidad Panamericana, Campus Ciudad de México, con la investigación "Derecho, ciberseguridad y protección de datos personales". Es docente de la materia de Gobierno Digital de la Maestría en Derecho de las TICs del INFOTEC-CONACYT. Es asociado de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI) y socio fundador de la Academia Multidisciplinaria de Derecho y TIC AMDETIC. Desde 2013 a la fecha es abogado en la Coordinación de Estrategia Digital Nacional de la Oficina de la Presidencia de la República.

Las decisiones del gobierno, de las organizaciones privadas y de las personas se basan en el flujo de la información que tienen a su alcance, con mayor o menor grado de utilidad y conocimiento. La información se está volviendo parte de nuestro día a día, es el insumo de muchas decisiones triviales y de alta relevancia para un país, como la política pública.

Ese gran poder, se complementa con el aporte de las TIC, principalmente con Internet como una plataforma colaborativa, horizontal y descentralizada, con lo cual los datos se explotan de mejor manera y se traducen en información útil para individuos, organizaciones y gobierno.

En la sociedad actual, se ha enfatizado el poder de la información y los datos para la mejor toma de decisiones. La economía, la política y una gran variedad de las actividades de la sociedad contemporánea, en los diferentes sectores de la economía mundial, se benefician de las TIC y el poder de la información.

La era digital ha representado y seguirá siendo un detonador de grandes oportunidades de crecimiento económico, de modernización y de transformación sociocultural; ha sido también fundamental para la transformación del quehacer de las instituciones públicas, en la construcción de un gobierno más eficiente, inteligente, un gobierno digital que se acerque cada vez más a la sociedad atendiendo sus necesidades de una manera más eficaz.

El desarrollo de eficiencia en la gestión pública, se ha beneficiado del desarrollo tecnológico, la digitalización y sistematización, la cual ha sido consecuencia de varios temas que aún cuentan con áreas de oportunidad. Como la libertad de expresión, el derecho de acceso a la información, el empoderamiento de la ciudadanía, la participación ciudadana, la apertura de las instituciones y un conjunto de las mismas, y leyes que han acercado la tarea pública y el interés público a la sociedad en general.

Hoy día, se genera, almacena, transfiere y procesa un gran volumen de información y datos relacionados con todas las actividades que realiza la sociedad, de los diferentes sectores de los ámbitos público y privado; toda esa información contiene datos en diferentes grados de desagregación que pueden constituir, y de hecho lo hacen, grandes oportunidades de generar más inteligencia sobre cómo

atender alguna situación, cómo prevenir mejor ciertos fenómenos y cómo predecir consecuencias para generar más oportunidades en aspectos sociales, económicos y políticos.

La interacción de las personas –individuos, organizaciones privadas y públicas– con los medios digitales –conectadas a Internet, con sistemas informáticos, bases de datos y micro datos en un entorno global–; constituyen el ecosistema digital sobre el cual se desenvuelve la dinámica social contemporánea de la revolución de los datos.

La revolución de datos –y el ecosistema digital–, de la que surgen grandes oportunidades y muchas otras que ahora son inimaginables, tienen como contexto aspectos como: el desarrollo democrático, el fortalecimiento de la libertad de expresión, el empoderamiento de la ciudadanía, una sociedad más participativa y corresponsable de los asuntos públicos, un escenario de innovación mayormente cercano a pequeñas empresas y a la sociedad en general, un gobierno digital cada vez más abierto y cercano a la sociedad, empresas con una ideología de negocios vinculada a la inteligencia de los datos. Además de una sociedad digitalizada en gran medida gracias al poder democratizador de Internet y su gobernanza, basada en un modelo de múltiples partes interesadas donde las políticas, legislación y normas técnicas deben impulsar un Internet abierto, descentralizado, único y neutral.

Dicho lo anterior, en este trabajo se pretende compartir un panorama de interrelación entre la gobernanza digital y los datos abiertos, haciendo mención de la visión más general de cómo la gobernanza de Internet, la interacción de los diversos actores con las tecnologías, así como las políticas y regulación en materia de datos abiertos representan una gran oportunidad para el desarrollo sostenible de México y el mundo.

La dinámica en la sociedad contemporánea, cada vez más global, multicultural e hiperconectada, está caracterizada por la interacción de diferentes actores de la vida en el ciberespacio. Cada actividad que realizamos acompañada de algún dispositivo o conectados a Internet, genera un dato y deja un rastro, lo cual constituye un insumo de información que puede conformar una base de datos, eventualmente en formato abierto explotable para distintos fines.

Se ha modificado en gran manera la forma de generar información y de consumirla; la forma de vender, de comprar, de pagar y realizar un sinnúmero de actividades de individuos y organizaciones públicas y privadas; hoy día es información para inteligencia de negocios que puede explotarse con el análisis de datos y desarrollar grandes ventajas competitivas y mejorar la prestación de los servicios públicos. En ese sentido, resulta importante conocer cómo funciona Internet, cómo es su interacción, y cómo podemos, a partir de comprender su complejidad y funcionamiento, sacar más provecho en la oferta y demanda de los datos abiertos, sean de información pública o privada, y contribuir con ello al desarrollo sostenible. A lo anterior nos referiremos como gobernanza digital y datos abiertos.

Estamos ante una gran oportunidad que nos brinda la ciencia y la tecnología para que individuos, empresas privadas e instituciones públicas podamos obtener mejores resultados en favor de la humanidad, derivado de la información y conocimiento para generar inteligencia, que nos ofrecen hoy día los datos y las formas, rapidez y precisión en su análisis. ¿Nos encontramos a la altura los operadores políticos, jurídicos, los agentes económicos y la sociedad en general?

Para poder comprender la interrelación de la gobernanza digital y los datos abiertos, es primero importante conocer aspectos como: gobernanza de Internet –cómo funciona–, lo que involucra las diferentes capas y actores, es decir, el ecosistema en que se desenvuelve y su gobierno. Si bien es cierto que al referir a la gobernanza digital hablamos del conjunto de tecnologías y no exclusivamente de Internet, consideramos relevante explicar someramente qué es este último concepto, dado que la revolución digital en gran medida está vinculada a dicha Red. Toda vez que a través de ella se desarrollan los servicios digitales y el poder para que los actores y las tecnologías puedan interactuar en el uso y reutilización de los datos abiertos.

Aunado a lo anterior, conoceremos superficialmente el origen y desarrollo de los datos abiertos en el terreno internacional, para posteriormente conocer cómo ha sido el avance del uso de datos abiertos en México. Ello se analizará a partir del desarrollo institucional, de la política pública y del marco normativo aplicable, así como su intersección con el derecho a la protección de datos personales.

II. GOBERNANZA DIGITAL

1. *Internet*

En principio es necesario preguntarnos, ¿qué es Internet? A esta pregunta caben varias respuestas, toda vez que cada usuario entenderá al Internet conforme al uso que le otorgue. Primero haremos referencia que Internet es un conjunto de redes de comunicación y telecomunicaciones interconectadas entre sí de manera descentralizada. Es una herramienta que entendemos como un medio de comunicación y difusión de ideas e información de cualquier tipo. La cual nos permite la búsqueda y transferencia de información eliminando las barreras de tiempo y espacio mediante distintos contenidos o productos digitales.

Desde nuestra perspectiva, miramos Internet como una Red de redes, que se refiere a una herramienta poderosa de comunicación entre personas de todo el mundo, e incluso aquella que la considera como un elemento sociocultural de grandes implicaciones en las relaciones de poder dentro de la sociedad; entre otras cosas tiene el potencial como medio de lograr el desarrollo o un gran caos de la sociedad (Leiner, 1997).

Ahora bien, como en muchos de los grandes desarrollos, debemos detenernos en reflexionar y preguntarnos también, ¿qué queremos con Internet? ¿Cómo queremos que esta herramienta esté presente en nuestras vidas? Se señaló en líneas que anteceden, estimamos al Internet como un gran instrumento para el desarrollo de las personas y los pueblos, pero no está por demás ser pensativos sobre el cauce que estamos dando a esta tecnología, pues el hombre siempre ambiciona y tiene, dentro de sí, la capacidad de determinar, ética o moralmente, el uso de las tecnologías. Del mismo modo, esta reflexión debe alcanzar, en concreto, al tratamiento de los múltiples tipos de datos: micro datos, sea en nuevos modelos, en nuevos modelos tecnológicos, dígase minería de datos, *Big Data*, Inteligencia Artificial, Internet de todo o ciudades inteligentes.

Dicho lo anterior, planteamos desarrollar una reflexión sobre cómo empoderar a la sociedad sobre el uso responsable y consciente de las TIC, conocer el ecosistema del Internet y cómo ejercer desde diferentes ámbitos un rol en favor de un

Internet que beneficie a todos, cómo usar los datos abiertos para el desarrollo sostenible y en buscar el equilibrio entre los intereses de los actores del ecosistema digital.

2. *Gobernanza*

Debemos hacer una propia distinción entre gobernar y gobernanza de Internet, para no errar y confundir los términos. Como se mencionó en el apartado anterior, Internet es la Red de redes, y esta refiere a un conjunto interconectado de redes a través de la cual las personas, desde cualquier punto donde se conecten, puedan desarrollar infinidad de actividades basadas en la información. Internet es un medio más que un fin en sí mismo, su uso depende de la persona que desarrolla la tecnología, así como quien procesa y analiza la información (datos).

Ahora bien, retomando lo anterior, analizaremos los conceptos de gobierno y gobernanza de Internet.

Gobierno, indica el Diccionario de la Real Academia Española (RAE), propiamente significa: "Acción y efecto de gobernar o gobernarse" (RAE, 2017). A su vez, gobernar, del latín *gubernāre*, y este del griego κυβερνᾶν kybernân, propiamente se entiende como "pilotar una nave" (RAE, 2017).

Ahora bien, la siguiente cuestión a analizar es, ¿cómo construir a partir del término "gobierno", que se refiere a las acciones de las autoridades que gobiernan o administran los recursos y a la sociedad en sus bienes, derechos y bienestar, un esquema o modelo de gobernanza?

Durante el devenir del Estado y sus diferentes formas de entender este, sus cambios de ideologías y de modelos económicos, ha existido una línea creciente en la concepción del Estado en relación con el gobierno, generando clara distinción entre el gobernante y el gobernador, enmarcado en un distanciamiento vertical entre unos y otros, aunado a una especie de exclusividad de los asuntos públicos a unos cuantos. La transformación de las instituciones, el fortalecimiento de los derechos humanos (en adelante DDHH), la globalización contemporánea y la modernización de la sociedad empujaron una transformación en la manera de gobernar, redefiniendo la gestión de lo público y la participación social en los asuntos públicos. Dentro de esta transformación algunos han señalado la existencia de un modelo de gobierno

cada vez más horizontal, donde la sociedad tiene un rol más activo y con mayor injerencia en la vida pública. Todo esto en el marco de un escenario de mayor fomento y protección de los DDHH, una sociedad digital y en una comprensión mayor de la interdependencia de actores en la economía del conocimiento.

Si la sociedad cambia constantemente su interacción, si la economía se modifica con la globalización y el uso de las TIC, es propio que la gestión pública también se adapte a las nuevas circunstancias de una sociedad más participativa.

Aunque se han dado múltiples debates académicos y en diálogos internacionales, no existe una definición universalmente aceptada del término gobernanza. Sin embargo, este ha estado presente en relación a la buena gestión de lo público. Prueba de ello es el Programa de Naciones Unidas para el Desarrollo, el cual concibe la gobernanza como un mecanismo y "sistema complejo de políticas, reglas, valores e instituciones, en las que se da la interacción entre diferentes actores: el Estado, la sociedad civil y el sector privado para la toma de decisiones de manera colectiva sobre asuntos de política, economía, socioculturales, ambientales, entre otros (PNUD, 2000)"[266].

Lo anterior, tomando en consideración que los mecanismos, procesos e instituciones son cada vez más complejos, pero identificando la gobernanza como un mecanismo a través del cual la sociedad civil, el sector privado y las instituciones públicas se articulan en torno a su interés, y buscan mediar sus diferencias y ejercer sus derechos y obligaciones que establece la ley. Los principios de buena gobernan-

---

[266] Obtenido del documento: *Discussion Paper - Governance for Sustainable Development. "Governance is the system of values, policies and institutions by which a society manages its economic, political and social affairs through interactions within and among the state, civil society and private sector. It is the way a society organizes itself to make and implement decisions, achieving mutual understanding, agreement and action. It comprises the mechanisms and processes for citizens and groups to articulate their interests mediate their differences and exercise their legal rights and obligations. It is the rules, institutions and practices that set limits and provide incentives for individuals, organizations and firms. Governance, including its social, political and economic dimensions, operates at every level of human enterprise, be it the household, village, municipality, nation, region or globe. See further UNDP Strategy Note on Governance for Human Development, 2000". Cfr. Governance Principles, Institutional Capacity and Quality*, p. 20, *http://www.undp.org/content/dam/undp/library/Poverty%20Reduction/Inclusive%20development/Towards%20Human%20Resilience/Towards_SustainingMDGProgress_Ch8.pdf.*

za incluyen el respeto a los DDHH, apertura política, la participación, la tolerancia, la capacidad administrativa y la eficiencia.

También se reconoce que la buena gobernanza trae consigo la creación de asociaciones efectivas para garantizar que las prioridades políticas, sociales y económicas se fundamentan en el diálogo, el consenso de la sociedad, donde las voces de los más pobres y más vulnerables sean escuchadas en los procesos de toma de decisiones. La gobernanza incluye dimensiones sociales, económicas y políticas que opera en todos los niveles de los derechos humanos, desde el interior de las casas, las comunidades, a nivel país, regional y global[267].

De lo anterior podemos identificar una transición en la forma de cómo se conciben los procesos de toma de decisiones de los asuntos públicos y cómo ha evolucionado el valor de la participación de los diferentes actores en la política, la economía y lo social. Se pasa de un "gobierno" referido al ejercicio mediante autoridad o conjunto de autoridades que de manera unilateral deciden sobre los asuntos públicos, a un esquema donde no existe solamente un sujeto detentador del poder, sino a un gobierno basado en acuerdos, diálogo de intereses diversos, donde las autoridades son facilitadoras de un proceso donde la sociedad civil y el sector privado pueden expresarse desde su individualidad y defender sus intereses mediante consenso, y bajo el entendimiento de la compleja interrelación de actores y factores.

Es decir, se concibe que los asuntos públicos por ser cada vez más complejos –como es el caso de la economía digital– deben asumirse también desde una perspectiva de cooperación y corresponsabilidad. Lo anterior resulta en un ejercicio de suma de voluntades donde cada actor aporta su experiencia para lograr el interés general, superando cualquier modelo tradicional donde el Estado determina lo que la sociedad debe realizar. Aunado a lo anterior, el modelo de gobernanza permite

---

[267] Obtenido de ONU. "The United Nations Development Programme (UNDP), in its 1997 policy paper, defined governance as "the exercise of economic, political and administrative authority to manage a country's affairs at all levels. It comprises the mechanisms, processes and institutions, through which citizens and groups articulate their interests, exercise their legal rights, meet their obligations and mediate their differences"; *http://hdr.undp.org/sites/default/files/zh-dr2000-governance.pdf.*

alcanzar el estadio de empoderamiento de la sociedad en un esquema descentralizado que permite construir un entramado de actores que, en conjunto, formen un sistema de desarrollo de soluciones a fenómenos globales como la sociedad del conocimiento[268].

Para inicios del milenio, en la Declaración del Milenio y los Objetivos del Desarrollo del Milenio (ODM), la gobernanza estaba contemplada para el desarrollo sobre el eje de derechos humanos dirigido a problemas o fenómenos de importancia global. En este sentido, dentro de las Naciones Unidas ya se identificaba a las TIC, en particular a Internet, como un elemento importante para contribuir al desarrollo y cumplimiento de los ODM. Resulta interesante que Internet pueda equipararse a un recurso público global por su naturaleza y su impacto en el desarrollo sostenible.

3. *Gobernanza en Internet*

El Internet es una tecnología relativamente nueva y compleja, por su relevancia es fundamental comprender sus diferentes capas, así como su modelo de gobernanza.

El término de gobernanza en Internet se refiere a los procesos y normas que afectan la forma en que se gestiona y se usa este último. Pretendemos explicar superficialmente cómo en la complejidad de Internet se llevan a cabo modelos de gobierno tradicional, es decir, de gobernanza y cómo se relaciona con la generación, uso y aprovechamiento de los datos abiertos.

---

[268] UNESCO, "Sociedades del conocimiento comprende dimensiones sociales, éticas y políticas mucho más vastas. El hecho de que nos refiramos a sociedades, en plural, no se debe al azar, sino a la intención de rechazar la unicidad de un modelo *listo para su uso* que no tenga suficientemente en cuenta la diversidad cultural y lingüística, único elemento que nos permite a todos reconocernos en los cambios que se están produciendo actualmente. Hay siempre diferentes formas de conocimiento y cultura que intervienen en la edificación de las sociedades, comprendidas aquellas muy influidas por el progreso científico y técnico moderno. No se puede admitir que la revolución de las tecnologías de la información y la comunicación nos conduzca –en virtud de un determinismo tecnológico estrecho y fatalista– a prever una forma única de sociedad posible". *Hacia las sociedades del conocimiento, http://uiap.dgenp.unam.mx/apoyo_pedagogico/proforni/antologias/UNESCO%20sociedades%20del%20conocimiento.pdf*.

Jovan Kurbalija opina que: "la complejidad de la Gobernanza de Internet se sustenta en su naturaleza multidisciplinaria, ya que abarca una serie de aspectos que incluyen tecnología, los temas socioeconómicos, el desarrollo, la legislación y la política" (Kurbalija, 2005).

Podemos decir que, el Internet como fenómeno global requiere cambio de paradigma en la atención de su desarrollo, pues es el motor más grande de transformaciones socioculturales de las últimas cuatro décadas. Respecto a este tema, en una conferencia que impartió Elinor Ostrom, premio Nobel de Economía, mencionó que para fenómenos globales se requiere que en lugar de una "gran solución global", debamos pensar en alternativas de múltiples escalas, con el reconocimiento que, como individuos, podemos hacer la diferencia, pues los cambios más significativos requieren acciones desde diferentes frentes. Es decir, habló de descentralizar la gobernanza de manera que se trabaje a nivel comunitario, por muy pequeña que sea, así como en todos los ámbitos y niveles de gobierno, para que la sociedad participe en su esfera de actuación más cercana (Ostrom, 2012).

El mensaje de Elinor deja claro como el Internet puede equipararse a sistema complejo, y desde nuestra perspectiva puede entenderse como un recurso común o bien público global, y clarifica la importancia de garantizar el acceso a este, puesto que los fenómenos complejos cotidianos requieren posibles soluciones que no pueden quedar solo en manos del Estado, sino de un sistema que interactúa a diferentes niveles, y ejercer un modelo de gobernanza *"policéntrica" o descentralizada*, esto implica conformar el entendimiento de un ecosistema de Internet en favor de los diferentes actores, bajo un enfoque colaborativo y con la finalidad del desarrollo humano.

La garantía del acceso a Internet se ha llegado a instrumentar, a partir de comienzos del siglo XXI, en forma de auténtico derecho ciudadano, el derecho de acceso a las TIC, una vía al conocimiento global, lo cual implica también el derecho a la privacidad y a la protección de los datos personales.

Varias organizaciones internacionales han venido considerando el acceso a Internet como un derecho básico o fundamental, es el caso de la Unión Europea,

desde el Paquete de Directivas sobre Telecomunicaciones del año 2002[269]. También la Asamblea General de Naciones Unidas, a través de dos iniciativas: la primera de ellas calificaba el acceso a Internet como un derecho instrumental, consecuencia de la libertad de expresión, a raíz de un informe en mayo de 2011, de la Oficina del Alto Comisionado para los Derechos Humanos; otra más relevante y más reciente, fue la Resolución A/HRC/32 del Consejo de Derechos Humanos de las Naciones Unidas de 5 de julio de 2012[270], en cuanto proclama que los mismos derechos que las personas tienen "offline" deben también protegerse online, en particular la libertad de expresión. Derivado de lo anterior, varios Estados reconocieron el derecho fundamental de acceso a Internet. En México, con la reforma constitucional, en materia de telecomunicaciones, que adicionó el tercer párrafo al Artículo 6o.[271], se reconoce el derecho de acceso a las TIC, incluido Internet y banda ancha.

---

[269] La Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de las comunicaciones electrónicas. Incluyó el acceso "de forma funcional" a Internet dentro de la rúbrica del servicio universal de telecomunicaciones (Artículo 4.2), *http://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A32002L0022*.

[270] La Resolución A/HRC/32/L.20, *"Promoción, protección y disfrute de los derechos humanos en Internet"* señala: "Considerando la importancia decisiva de la colaboración de los gobiernos con todos los interesados pertinentes, incluidos la sociedad civil, el sector privado, la comunidad técnica y el sector académico, en la protección y promoción de los derechos humanos y las libertades fundamentales en Internet. 1. Afirma que los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos; 2. Reconoce la naturaleza mundial y abierta de Internet como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas, incluido el logro de los objetivos de desarrollo sostenible; 3. Exhorta a todos los Estados a que promuevan y faciliten la cooperación internacional encaminada al desarrollo de los medios de comunicación, y los servicios y tecnologías de la información y las comunicaciones en todos los países; 4. Afirma que la calidad de la educación cumple un papel decisivo en el desarrollo y, por consiguiente, exhorta a todos los Estados a fomentar la alfabetización digital y facilitar el acceso a la información en Internet, que puede ser una herramienta importante para la promoción del derecho a la educación; 5. Afirma también la importancia de que se aplique un enfoque basado en los derechos humanos para facilitar y ampliar el acceso a Internet, y solicita a todos los Estados que hagan lo posible por cerrar las múltiples formas de la brecha digital"; *http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_32_L20.pdf.*

[271] Artículo 6o. constitucional señala: "… El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y teleco-

Es natural que algunos vean en Internet, como elemento clave de las TIC, uno de los dos factores determinantes del surgimiento de toda una nueva generación de derechos, los llamados derechos "de cuarta generación"[272].

En el mismo sentido, considero que para temas cada vez más complejos se requieren de una actitud más abierta a la complejidad y multiculturalidad, e Internet no es la excepción. Se deben considerar dimensiones tan variadas como sea posible en el enfoque multidisciplinario, en la naturaleza y número de actores que, bajo un modelo de participación incluyente y democrática, genere conciencia de que a cualquier nivel que aportemos, podemos impactar en la gobernanza global de Internet, desarrollando un sistema similar a lo que Ostrom llama "gobernanza policéntrica" –o descentralizada y democrática– de los bienes comunes ante fenómenos globales, con un enfoque de lo global a lo local y viceversa.

Retomando la definición u origen de la frase "gobernanza de Internet", no es sino hasta la primera fase de la Cumbre Mundial de la Sociedad de la Información y del Conocimiento, donde en la Declaración de Principios se señala que (CMSI, 2013)[273]:

> Internet se ha convertido en un recurso global disponible para el público, y su gestión debe ser una de las cuestiones esenciales del programa de la Sociedad de la Información. La gestión internacional de Internet debe ser multilateral, transparente y democrática, y contar con la plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales. Esta gestión debería garantizar la distribución equitativa de recursos, facilitar el acceso a todos y garantizar un funcionamiento estable y seguro de Internet, teniendo en cuenta el plurilingüismo.
>
> La gestión de Internet abarca cuestiones técnicas y de política pública, y debe contar con la participación de todas las partes interesadas y de organizacio-

---

municaciones, incluido el de banda ancha e Internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios"; disponible en: *http://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013.*

[272] Esta cuarta generación de derechos, aparecería a finales del siglo XX, estaría representada por los que han de proteger a la persona frente a amenazas procedentes de las biotecnologías (prohibición de la clonación reproductiva humana, por ejemplo) y de las propias TICs (Internet, entre ellas).

[273] CMSI, disponible en: *http://www.itu.int/net/wsis/docs/geneva/official/dop-es.html*.

nes internacionales e intergubernamentales competentes. A este respecto se reconoce que:

a) *La autoridad* en materia de política pública relacionada con Internet es un derecho soberano de los Estados. Ellos tienen derechos y responsabilidades en tal cuestión;
b) *El sector privado* ha desempeñado, y debe seguir desempeñando, un importante papel en el desarrollo de Internet, en los campos técnico y económico;
c) *La sociedad civil* también ha desempeñado, y debe seguir realizando, un importante papel en asuntos relacionados con Internet, especialmente a nivel comunitario;
d) *Las organizaciones intergubernamentales* han efectuado, y deben continuar, un papel de facilitador en la coordinación de las cuestiones de política pública relacionadas con Internet;
e) *Las organizaciones internacionales* han llevado a cabo, y deben seguir haciéndolo, una importante función en la elaboración de normas técnicas y políticas pertinentes relativas a Internet.

De los principios señalados, surge el alcance de la "gobernanza de Internet", la participación de las "múltiples partes interesadas", la identificación de una alternativa para construir un Internet libre, estable, descentralizado, único y seguro que permita el desarrollo de la sociedad global.

Ahora bien, se esbozaron únicamente algunos principios sobre cómo es Internet, se reconoció a este como un recurso mundial, un bien público, aproximándose de tal forma a un nuevo esquema donde no solo los Estados decidían sobre los asuntos de Internet. A decir de Markus Kummer (Jefe de la Secretaría del Grupo de Trabajo de las Naciones Unidas sobre la gobernanza de Internet):

> … se trata de principios básicamente tradicionales de cooperación internacional, tales como la transparencia y la democracia. También introducen algunos aspectos específicos de Internet tales como el reconocimiento de que la red es ahora un recurso mundial. Además, dichos principios reconocen el carácter multifacético de Internet, ya que se insiste en que los gobiernos, el sector pri-

vado, la sociedad civil y las organizaciones internacionales deberían participar plenamente en su gestión (Kummer, 2005).

Así, el Grupo de Trabajo sobre la Gobernanza de Internet propuso la siguiente definición de gobernanza de Internet: "34. … es desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de Internet"[274].

De igual forma, la UNESCO "reconoce el potencial de internet para fomentar un desarrollo humano sostenible, construir unas sociedades del conocimiento inclusivas y mejorar la libre circulación de la información y las ideas en el mundo. Por consiguiente, defiende una visión abierta, transparente e incluyente de la gobernanza de Internet basada en el principio de apertura, que incluye la libertad de expresión, el respeto a la vida privada, el acceso universal y la interoperabilidad técnica. La ética y el respeto de la diversidad cultural y lingüística en el ciberespacio son otras de las principales preocupaciones de la Organización".

En ese sentido, muchos países reconocen a Internet como un tema de carácter prioritario para sus gobiernos y de vital importancia para la convivencia internacional. Esta misma causa, produjo que la gobernanza de Internet llamara cada vez más la atención de todos y por ello es de suma importancia conocer las bases sobre las cuales los diferentes ámbitos de la sociedad pueden participar con acciones pequeñas que lograrán impacto favorable en el orden global.

La Internet Society (ISOC), describe los principios de la gobernanza de Internet de la siguiente manera:

> Los principios rectores recomendados para la gobernanza de Internet son los siguientes:
>
> 1. Participación abierta, inclusiva y transparente. Para garantizar que los resultados de los procesos de gobernanza de Internet sean tanto eficaces como aceptados, es necesaria la participación de actores interesados e informados,

---

[274] *Agenda de Túnez para la Sociedad de la Información*, WSIS-05/TUNIS/DOC/6(Rev.1)-S, *https://www.itu.int/net/wsis/docs2/tunis/off/6rev1-es.html.*

cada uno con sus respectivas funciones y responsabilidades. Esta participación también asegura que las partes interesadas puedan participar directamente en el trabajo y tener acceso a sus resultados.

2. Toma de decisiones basada en el consenso. Los procesos de formulación de políticas deben tomar en cuenta tanto la experiencia práctica como la pericia individual y colectiva de una amplia gama de partes interesadas. Las decisiones se deben tomar mediante procesos responsables basados en el consenso.

3. Supervisión y empoderamiento colectivos. Para garantizar la seguridad, estabilidad y resiliencia de Internet es necesario desarrollar estructuras y principios de gobernanza en un entorno de fuerte cooperación entre todas las partes interesadas, donde cada una contribuya sus propias habilidades.

4. Enfoques pragmáticos y basados en la evidencia. Las discusiones, debates y decisiones relacionadas con la gobernanza de Internet deben tener en cuenta y basarse en información objetiva y empírica.

5. Voluntarismo. En el ámbito del desarrollo de políticas técnicas de Internet, significa que el éxito es determinado por los usuarios y por el público, no por una autoridad central.

6. Innovación sin permiso. El notable crecimiento de Internet y consiguiente explosión de la innovación y el uso de Internet es un resultado directo del modelo abierto de la conectividad y el desarrollo de estándares de Internet. Cualquier persona debe poder crear una nueva aplicación en Internet sin tener que obtener la aprobación de una autoridad central. La gobernanza de Internet no debe restringir ni regular la capacidad de los individuos y las organizaciones para crear y utilizar nuevos estándares, aplicaciones o servicios.

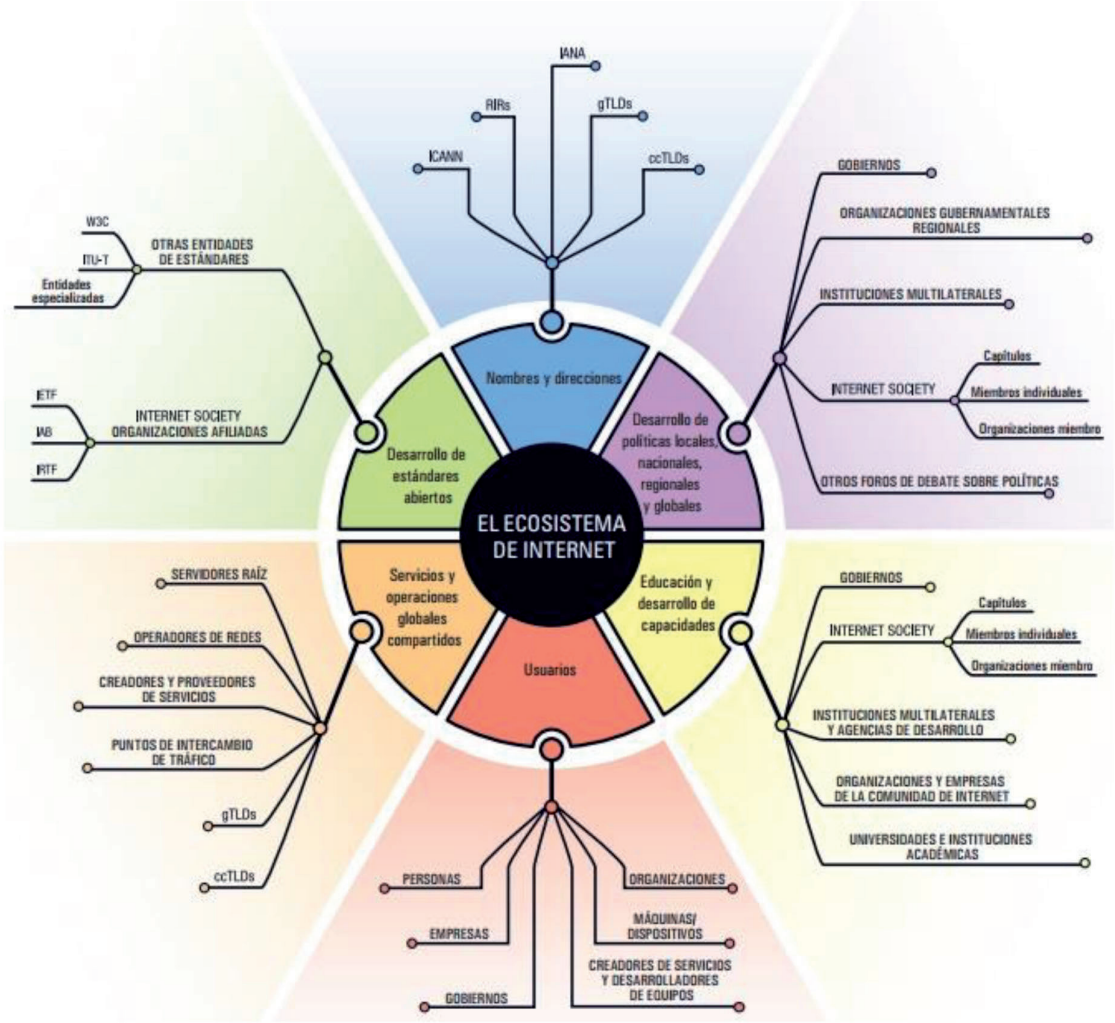
El ecosistema de Internet que existe hoy se basa en los principios fundamentales de la propia Internet y se fortalece con la participación de una amplia gama de actores que emplean procesos abiertos, transparentes y colaborativos. La cooperación y la colaboración siguen siendo esenciales para mantener la innovación y el crecimiento de la Red. Lo anterior es fundamental para el desarrollo de políticas públicas en materia de datos abiertos, así como de acciones desde el sector privado en el aprovechamiento de los datos públicos o privados para generar valor económico, social y seguir detonando la innovación.

4. *Ecosistemas de Internet*

Todos los días, cuando las personas se conectan, navegan y entretienen, gracias a Internet ocurren muchos actos técnicos, políticas, protocolos, grupos de trabajo y diversos actores interrelacionados para que ello suceda. Existe un conjunto de bases teóricas sobre las que se apoya, y que es vital para la vida digital que hoy día tiene casi la mitad del mundo gracias a Internet. A todo este conjunto tecnológico e innovador de interacción de personas, protocolos y servicios lo conocemos como ecosistema de Internet. Según la organización Internet Society (ISOC), líder global en este tema, el ecosistema se utiliza para describir las organizaciones y comunidades que ayudan a la evolución de Internet.

Internet es exitosa en gran parte gracias a su modelo único: la propiedad global compartida, el desarrollo basado en estándares abiertos y los procesos de acceso libre para el desarrollo de tecnologías y políticas. El éxito sin precedentes de Internet continúa su marcha porque su modelo es abierto, transparente y colaborativo. Se basa en procesos y productos que son locales, ascendentes y accesibles para usuarios de todo el mundo (Internet Society, 2010).

Podemos verlo como una nueva forma de participación en la que diferentes organizaciones buscan aportar a la creación de políticas públicas y procesos técnicos que puedan definir el funcionamiento de la Red. Dentro de este ecosistema se generan discusiones, foros y debates abiertos donde participan diferentes actores: la sociedad civil, entidades públicas y privadas, academia, sector privado, comunidad técnica; todos buscando contribuir, de una forma u otra, y así contar con un Internet libre, descentralizado y abierto.



("El Ecosistema de Internet". Internet Society, 2009)

5. *Actores relacionados al ecosistema de Internet*

Respecto a la diversidad de actores en el ecosistema, ISOC señala: "el ecosistema de Internet es el término utilizado para describir a las organizaciones y comunidades que dirigen el funcionamiento y desarrollo de las tecnologías y la infraestructura que conforman la Internet global" (Internet Society, 2010).

Estas organizaciones comparten valores comunes para el desarrollo abierto de Internet. El término ecosistemas de Internet implica que la adopción y desarrollo rápidos y continuos de tecnologías sean atribuidos a la implicación de muy diversos actores; procesos abiertos, transparentes y colaborativos, así como el uso de productos e infraestructuras con un control y propiedad diversificados.

Entre las organizaciones que conforman el ecosistema de Internet se incluyen[275]:

- Organismos dedicados a la elaboración de estándares técnicos, tales como la Fuerza de Tareas de Ingeniería de Internet (IETF) y el Consorcio World Wide Web (W3C);
- Organizaciones que gestionan recursos para funciones de asignación de direcciones globales, tales como la Corporación de Internet para la Asignación de Nombres y Números (ICANN), incluida la Autoridad para la Asignación de Números de Internet (IANA), los Registros Regionales de Internet (RIR) y los Registradores y Registros de Nombres de Dominios;
- Empresas que ofrecen servicios de infraestructura de red, tales como proveedores de servicios de nombres de dominios (DNS), operadores de redes y puntos de intercambio de tráfico en Internet (IXP);
- Personas y organizaciones que utilizan Internet para comunicarse entre sí y ofrecer servicios; y
- Organizaciones que ofrecen formación y crean capacidad para desarrollar y utilizar tecnologías de Internet, tales como organismos multilaterales, instituciones educativas y agencias gubernamentales.

III. DATOS ABIERTOS

1. *Antecedentes*

Los datos abiertos son un elemento de una concepción filosófica de la era del conocimiento, la voluntad ciudadana de considerar la información pública como un bien común, colectivo y que debe servir a todos para generar mayor innovación, más progreso y desarrollo sostenible de nuestro planeta. Hay aproximaciones del término datos abiertos con el software abierto y la cultura de compartir conocimiento. Sin embargo, los datos abiertos tomaron un rumbo más en el sentido de las características técnicas que permiten su uso y reutilización como información pública.

---

[275] Ver ISOC, *https://www.internetsociety.org/es/resources/doc/2014/makes-internet-work-internet-ecosystem/*.

Este movimiento se origina en Estados Unidos. En 1966, la ley norteamericana sobre la libertad de información (*Freedom of Information Act*), permite el libre acceso a documentos administrativos. Esta medida, tomada durante la guerra de Vietnam, es objeto de restricciones en el curso de las décadas siguientes. Sin embargo, esta corriente encuentra una segunda oportunidad, en su vínculo con el Internet y la cantidad de datos generados, a través de una asociación norteamericana, en California, cuyo objetivo era reforzar, dinamizar el debate democrático y mejorar el servicio público (OpenDataSoft, 2017).

2. *Definiciones*

Más que una tendencia o moda, los datos abiertos son considerados como un rasgo distintivo de la transformación en la sociedad de la información y el conocimiento, es un vector fundamental para la economía digital, una herramienta para la transparencia, rendición de cuentas y participación ciudadana. Además de ser un factor de estímulo para la innovación social, la colaboración y el desarrollo sostenible.

Si bien la idea de lo abierto no es del todo nueva, ya que desde hace varias décadas se desarrolló la cultura de software abierto, conocimiento abierto; lo nuevo es el valor, para la implementación de políticas públicas, que generan los datos en razón del desarrollo sostenible.

De acuerdo al Open Data Handbook, los datos abiertos son: "datos que pueden ser utilizados, reutilizados y redistribuidos libremente por cualquier persona, y que se encuentran sujetos, cuando más, al requerimiento de atribución y de compartirse de la misma manera en que aparecen". De la anterior definición resalta el hecho de "compartirse de la misma manera en que aparecen", lo cual deja fuera oportunidades como la comercialización o explotación si su origen no permite esto.

La Carta Internacional de Datos Abiertos[276] señala como tales a los "datos digitales que son puestos a disposición con las características técnicas y jurídicas necesarias para que puedan ser usados, reutilizados y redistribuidos libremente por cualquier persona, en cualquier momento y en cualquier lugar".

[276] La Carta Internacional de Datos Abiertos es un ejercicio colaborativo entre autoridades gubernamentales y sociedad civil para la apertura de datos en formatos abiertos; disponibles en: *https://opendatacharter.net/principles-es/#* .

De la anterior definición destaca la referencia a *características jurídicas*, lo anterior muestra el reflejo del entrecruzamiento de varios derechos, como es el caso de los derechos de acceso a la información pública, el derecho a la privacidad y protección de datos personales, el derecho al secreto bancario y comercial, el derecho de las autoridades a clasificar la información pública como reservada o confidencial y la seguridad nacional. En esta definición, no repara en la obligación de compartir del mismo modo en que aparecen, aunque dependerá de la naturaleza jurídica de los mismos.

Es importante precisar que existen datos abiertos en el sector público (datos abiertos gubernamentales o datos abiertos de información pública), y en el sector privado y social. Los datos abiertos pueden ser de origen público o privado. Son públicos aquellos que emanan de la información que se genera de los servicios públicos que prestan las autoridades, a partir de que son generados por entes públicos, que trabajan con recursos del erario, en el marco del derecho de acceso a la información[277].

Los datos abiertos privados son provenientes de la información de los particulares (empresas o instituciones), cuyos datos son de información particular no sujeta a la coacción de la autoridad y por tanto gozan de la protección de la propiedad privada, el derecho a la vida privada, la protección de datos personales o secreto comercial o bancario, cuando sea el caso. En ambos supuestos existe una correlación entre oferta y demanda, y un sinnúmero de finalidades en las que se identifican grandes oportunidades.

3. *Principios de los datos abiertos*

Tim Berners-Lee establece una escala de calidad de los datos abiertos bajo estos principios:

a) Datos no filtrados "degradados" en cualquiera de sus formatos;
b) Datos disponibles en formatos estructurados (tabuladores en CSV, XML, Excel, RDF);

[277] En México sería susceptible de esta interpretación todos los sujetos obligados de conformidad con la Ley General de Transparencia y Acceso a la Información Pública.

c) Datos libres de explotación jurídica (licencias) y técnicamente bajo formatos carentes de propietario;
d) Datos accesibles vía URL, que puedan ser consultados haciendo un clic en ellos; y
e) Datos vinculados a otros datos para contextualizarlos y enriquecerlos; (Berners-Lee, 2010).

El Grupo de Trabajo de Datos Abiertos (*Open Government Working Group Meeting* in Sebastopol, CA) estableció como principios los siguientes[278]:

a) Completos;
b) Primarios;
c) Oportunos;
d) Accesibles;
e) Legibles por máquina;
f) No discriminatorios;
g) No propietarios; y
h) Libre de licencia (o no restrictivos en materia de propiedad intelectual).

---

[278] *December 7-8, 2007— this weekend, 30 open government advocates gathered to develop a set of principles of open government data. The meeting, held in Sebastopol, California, was designed to develop a more robust understanding of why open government data is essential to democracy. The group is offering a set of fundamental principles for open government data. By embracing the eight principles, governments of the world can become more effective, transparent, and relevant to our lives.* Disponible en: *https://public.resource.org/8_principles.html.* Traducción propia obtenida de:
1. Complete.- *All public data is made available. Public data is data that is not subject to valid privacy, security or privilege limitations.*
2. Primary.- *Data is as collected at the source, with the highest possible level of granularity, not in aggregate or modified forms.*
3. Timely.- *Data is made available as quickly as necessary to preserve the value of the data.*
4. Accessible.- *Data is available to the widest range of users for the widest range of purposes.*
5. Machine processable.- *Data is reasonably structured to allow automated processing.*
6. Non-discriminatory.- *Data is available to anyone, with no requirement of registration.*
7. Non-proprietary.- *Data is available in a format over which no entity has exclusive control.*
8. License-free.- *Data is not subject to any copyright, patent, trademark or trade secret regulation. Reasonable privacy, security and privilege restrictions may be allowed.*

La Carta Internacional de Datos Abiertos (CIDA) señala los siguientes principios:

a) Abiertos por defecto;
b) Oportunos y exhaustivos;
c) Accesibles y utilizables;
d) Comparables e interoperables;
e) Para mejorar la gobernanza y la participación ciudadana; y
f) Para el desarrollo incluyente y la innovación.

4. *Datos abiertos en el sector privado: ámbito bancario*

Debemos recordar que los datos abiertos son una herramienta que se pueden generar por diferentes sectores e igualmente se consumen y explotan desde diferentes ámbitos de la economía. Dentro de los rubros que cuentan con mayor potencial el sector financiero, con la gran generación de datos de clientes, productos financieros y un sector muy amplio diverso, representa una gran oportunidad para explotar los datos abiertos para que los bancos puedan ofrecer mejores experiencias y servicios a sus clientes.

Como caso representativo del sector público en el uso de datos abiertos en el sector bancario tenemos The Open Banking Standard[279], ya que el poder de los datos en el sector bancario impacta significativamente "cuando se comparten o publican datos bancarios en formatos abiertos utilizando API abiertas, se pueden usar para crear aplicaciones y recursos útiles para ayudar a las personas a encontrar lo que necesitan. Los clientes pueden buscar una hipoteca más fácilmente, los bancos ubicar clientes que coincidan con un nuevo producto y las empresas pueden compartir datos con sus contadores. Esto, a su vez, mejorará la eficiencia y estimulará la innovación"[280].

---

[279] Open Data Institute, Helping customers, banks and regulators take banking into a truly 21st-century, connected digital economy, 2016, disponible en: *https://theodi.org/open-banking-standard.*

[280] *Idem.*

En 2015, el Grupo de Trabajo de Banca (*Open Banking Working Group*) estableció el estándar de banca abierta. Este estándar es una guía para aprender, crear, compartir y usar los datos bancarios. Se desarrolla y mantiene de forma colaborativa y transparente, y cualquier persona puede acceder y utilizar dichos datos.

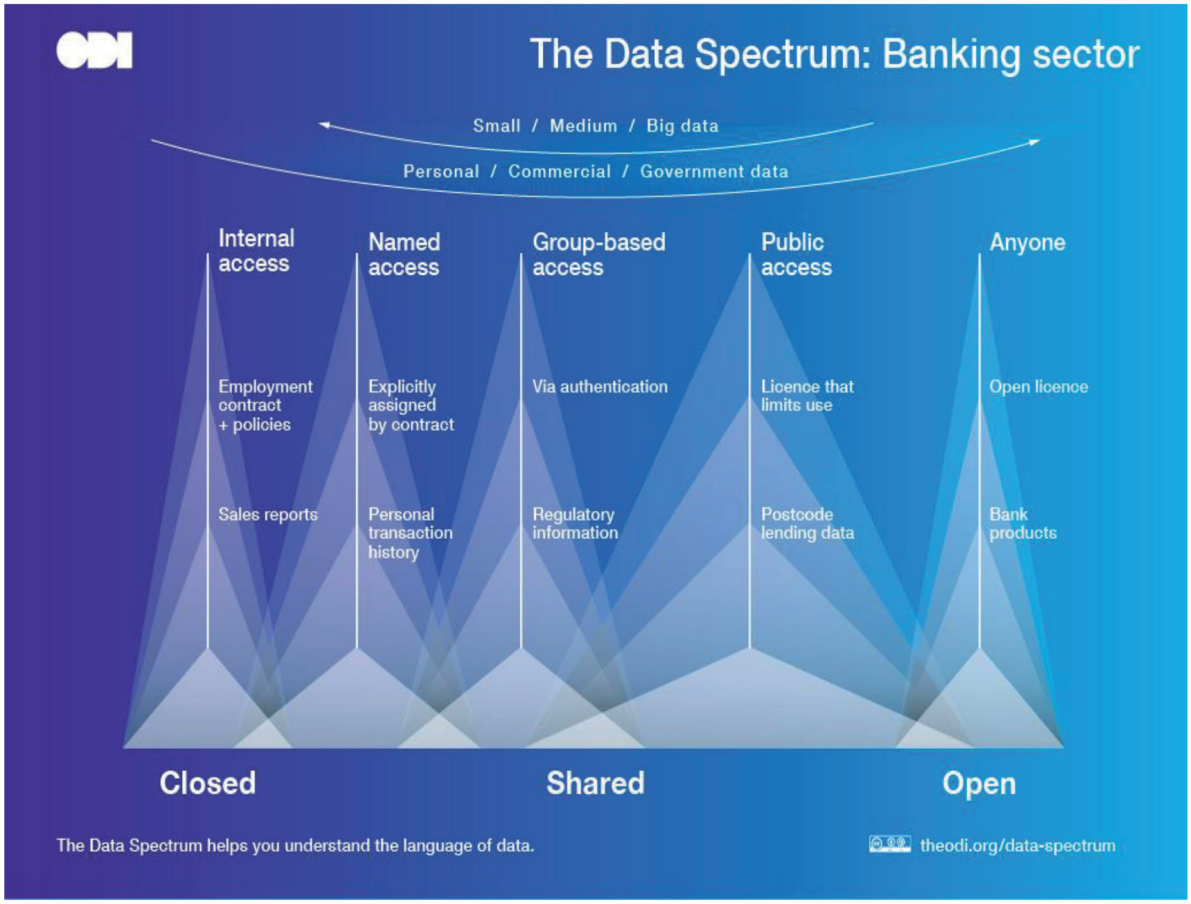
El marco del estándar de banca abierta ayudará a emprendedores, empresarios, sector financiero y usuarios de los servicios financieros de manera importante, ya que hoy día estos últimos buscan generar una experiencia muy personalizada a los clientes, por ello el sector FinTech tendrá una gran oportunidad que deberá acompañar la actualización del sector financiero tradicional.

Los usuarios de la banca podrán tener mayor gama de ofertas de productos y servicios financieros gracias a que los datos abiertos que genera el ecosistema financiero permiten que otros emprendan negocios para ofrecer servicios digitales de carácter financiero que cubran las necesidades de los clientes, de manera más ágil y particular que los servicios estandarizados que actualmente ofrecen los agentes financieros.

Para las instituciones financieras representan una gran oportunidad de generar alianzas con pequeños proveedores de servicios financieros –FinTech–. Estos servicios tienen potencial de fomentar el ahorro de usuarios de pequeños ingresos, hacerlo de forma más fácil, ágil y bajo el control del propio usuario. Además, los servicios financieros personalizados pueden significar ahorros de los clientes por reducir la labor de intermediación y altas comisiones que hoy deben costear las instituciones financieras.

Finalmente, este caso representativo es para dar evidencia de cómo los datos abiertos pueden detonar economía en diferentes actividades de la sociedad y lograr con la generación de datos abiertos del sector privado impulso al desarrollo sostenible.

Para ayudar a dimensionar el escenario y lenguaje en materia de datos abiertos del sector bancario, el ODI nos ofrece el espectro siguiente:



Aunado a los datos abiertos que pueden generar los diferentes ecosistemas de sectores privados, es necesario dimensionar el alcance del análisis de datos con datos abiertos de bases abiertas como las redes sociales.

Existen datos abiertos y/o desagregados en cada actividad digital que se realiza usando tecnologías digitales; cada like, cada clic, cada mensaje, cada acción deja rastro en datos digitales que puede generarse en formatos abiertos. Estos datos abiertos del sector privado guardan gran valor para la innovación, el desarrollo económico y también para complementar el análisis que puedan hacer las instituciones públicas en el diseño, implementación y seguimiento de las políticas públicas. Así, los conjuntos de datos abiertos públicos o gubernamentales y del sector privado son más valiosos cuando se pueden complementar, y así aumentar la capacidad de análisis y de interpretación para la comprensión más acertada de

algún fenómeno social y para ofrecer soluciones de diferentes índoles en favor del desarrollo económico, político y social.

El procesamiento de toda la masa de datos que esté a disposición para su análisis requerirá de grandes capacidades de cómputo, de cómputo en la nube, del denominado *Big Data, machine learning*, inteligencia artificial y una lista más de nuevas tecnologías, nuevas metodologías y nuevas formas de generar habilidades para la interpretación y uso, hacia el estudio y atención de fenómenos sociales.

El uso de los datos y las tecnologías como la Inteligencia Artificial también representará un reto a la multidisciplina, ya que los fenómenos son cada vez más complejos y el propio ciclo de la información, desde su generación hasta su interpretación para aplicarla a un fenómeno, exigirá valores éticos y garantizar que los datos cumplan con el enfoque de los derechos humanos; por ejemplo, la protección de la vida privada y la protección de los datos personales. También es clave, en la búsqueda de solucionar problemas a través de los datos, contemplar cuestiones éticas y morales, tal es el caso de la transparencia algorítmica para garantizar que los resultados que arrojen los procesos de análisis hechos por programas y máquinas no tenga por configuración algún sesgo hacia la discriminación o algún aspecto que vaya en contra del desarrollo sostenible y digno de las personas.

5. *Panorama internacional*

En Europa, desde el 2003, los datos abiertos se encuadran en reglamentaciones del Parlamento Europeo, a través de la Comunicación "*Datos abiertos. Un motor para la innovación, el crecimiento y la gobernanza transparente*[281]".

Desde el punto de vista legislativo, la Directiva de 2003, relativa a la reutilización de la información del sector público, estableció el marco legislativo general a nivel europeo. Esta Directiva establece un grado mínimo de armonización.

En el terreno de las políticas públicas, los antecedentes en sectores específicos fueron:

---

[281] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo, al Comité de las Regiones. *Datos abiertos: Un motor para la innovación, el crecimiento y la gobernanza transparente*, COM/2011/0882, que puede consultarse en: *http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52011DC0882*.

- La Directiva relativa al acceso a la información medioambiental[282] y la Directiva INSPIRE, destinadas a alcanzar la mayor difusión posible de la información en esa materia y a la armonización de los conjuntos de datos clave;
- La Comunicación de la Comisión sobre el conocimiento del medio marino 20209[283], destinada a facilitar el uso de los datos marinos y reducir su coste, entre otras cosas;
- Las iniciativas contenidas en el Plan de acción para el despliegue de sistemas de transporte inteligentes (STI) de 2008[284], centradas en el acceso de los proveedores de servicios privados a la información en tiempo real sobre tráfico y desplazamientos, entre otras cosas;
- La política de la Comisión en materia de acceso abierto a la información científica[285], en la que se incluye el proyecto piloto para las publicaciones

---

[282] Los objetivos de esta Directiva fueron: (1) Un mayor acceso del público a la información medioambiental y la difusión de tal información contribuye a una mayor concienciación en materia de medio ambiente, a un intercambio libre de puntos de vista, a una más efectiva participación del público en la toma de decisiones medioambientales y, en definitiva, a la mejora del medio ambiente. (2) La Directiva 90/313/CEE del Consejo, de 7 de junio de 1990, sobre libertad de acceso a la información en materia de medio ambiente inició un cambio en el modo en que las autoridades públicas abordan la cuestión de la apertura y de la transparencia, estableciendo medidas para el ejercicio del derecho de acceso del público a la información medioambiental que conviene desarrollar y proseguir. Directiva 2003/4/CE del Parlamento Europeo y del Consejo, de 28 de enero de 2003, relativa al acceso del público a la información medioambiental y por la que se deroga la Directiva 90/313/CEE del Consejo, puede consultarse en el sitio: *http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:32003L0004*

[283] Señala entre sus objetivos: 1. Simplificar la utilización de datos sobre el medio marino y reducir su coste; 2. Fomentar la competitividad y la innovación entre usuarios de estos datos; y 3. Reducir la incertidumbre de los datos para facilitar una base más sólida que permita gestionar futuros cambios. La Comunicación de la Comisión al Parlamento Europeo y al Consejo de 8 de septiembre de 2010 titulada "Conocimiento del medio marino 2020: observación y recogida de datos sobre el medio marino con miras a un crecimiento inteligente y sostenible", disponible en: *http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:ev0025&from=ES*.

[284] Este Plan de Acción tuvo por finalidad acelerar y coordinar el despliegue de los sistemas de transporte inteligentes (STI) en el transporte por carretera y de las correspondientes interfaces con otros modos de transporte. Disponible en: *http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52008DC0886R(01)&from=ES.*

[285] La iniciativa sobre bibliotecas digitales pretende conseguir que la información resulte más accesible y utilizable en el entorno digital sobre la información científica en la era digital: acceso,

que resultan de proyectos financiados por la Unión Europea y una participativa infraestructura electrónica de repositorios de libre acceso a escala paneuropea; el repositorio de publicaciones del JRC es también pertinente en este contexto; y

- Las políticas para la digitalización del patrimonio cultural y el desarrollo de Europeana (la biblioteca, archivo y museo digital de Europa), destinados a garantizar la mayor utilización posible del material cultural digitalizado y los metadatos correspondientes[286].

En Francia, la Comisión de Acceso a Documentos Administrativos (CADA, por sus siglas en francés: *Commission d'accès aux documents administratifs*), creada en 1978, asegura la buena aplicación de la apertura y la reutilización de datos. Más allá de una ley, CADA posee las premisas de los datos abiertos y concretiza el derecho de acceso a todos los documentos de una Administración en el marco de su misión de servicio público. Al respecto, Gilles J. Guglielmi señala que los datos abiertos en Francia se identifican como: "un sistema completo de gestión de datos públicos, que permite articular el acceso a los datos específicamente jurídicos y el derecho a la información administrativa para obtener una política de reutilización de las informaciones recolectadas en todo el sector público"[287]. Además, señala la presencia de tres etapas. Primera etapa: un servicio público de acceso a las informaciones jurídicas; a partir de 1998, el Gobierno francés había decidido poner en línea gratuitamente ciertos "datos públicos esenciales. Segunda etapa: la reutilización de informaciones del sector público. Se da entonces por sentada

---

difusión y preservación. COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO Y AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO, *http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0056&from=ES*.

[286] El objetivo político de la Comisión es que en 2010 se pueda acceder, a través de este sitio, a 10 millones de objetos. Dicho número debería multiplicarse en años posteriores. La alimentación de *Europeana* exige un esfuerzo continuado de digitalización en toda Europa, así como la adición a los objetos digitalizados de metadatos que respondan a las normas más estrictas. EUROPEANA: UNA ESTRATEGIA PARA OFRECER EN LÍNEA EL PATRIMONIO CULTURAL DE EUROPA, *http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52009DC0440&qid=1517223507617&from=EN*.

[287] Guglielmi, Gilles J., *Open data y servicio público. Los datos públicos abiertos son un servicio público*, Madrid, INAP.

la existencia de un servicio público nacional cuya misión consiste en difundir todas las informaciones jurídicas normativas. Tercera etapa: los datos públicos abiertos como servicio público administrativo. Los temas del acceso de los ciudadanos a los documentos administrativos y de una puesta a disposición gratuita, y facilitada en Internet, de un gran número de datos públicos.

En Estados Unidos destacan dos documentos, ambos emitidos bajo la administración del expresidente Barack Obama: el primero, en el año 2009, denominado "*Memorandum for the Heads of Executive Departments and Agencies*"[288]; el segundo constituye la "*Executive Order. Making Open and Machine Readable the New Default for Government Information*", emitida en el año 2013.

En el primer instrumento se establecen los lineamientos para el gobierno abierto sobre la publicación de información en línea. Lo anterior de conformidad con los principios de transparencia, participación y colaboración. Para cumplir con la meta de crear un gobierno más abierto, el Memorándum señala que las agencias y departamentos realicen los pasos siguientes: *a)* publicar información pública gubernamental en línea; *b)* mejorar la calidad de la información pública gubernamental; *c)* constituir e institucionalizar una cultura de gobierno abierto; y *d)* crear una política marco que habilite el gobierno abierto. Mientras que las disposiciones de la "*Executive Order. Making Open and Machine Readable the New Default for Government Information*"[289] hacen referencia a la apertura de datos públicos bajo formatos utilizables para que puedan ser reutilizados, y dice lo siguiente:

---

[288] *Memorandum for the Heads of Executive Departments and Agencies,* Casa Blanca, *https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf.*

[289] Traducción propia de: "To promote continued job growth, Government efficiency, and the social good that can be gained from opening Government data to the public, the default state of new and modernized Government information resources shall be open and machine readable. Government information shall be managed as an asset throughout its life cycle to promote interoperability and openness, and, wherever possible and legally permissible, to ensure that data are released to the public in ways that make the data easy to find, accessible, and usable. In making this the new default state, executive departments and agencies (agencies) shall ensure that they safeguard individual privacy, confidentiality, and national security". *Executive Order. Making Open and Machine Readable the New Default for Government Information,* Casa Blanca, *https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government-*.

> Para promover el crecimiento continuo del empleo, la eficiencia en la gestión pública y el bien común se puede poner a disposición del público los datos de la información pública gubernamental, el estado por default de los recursos de información gubernamentales derivado de su modernización debe ser abierto y legible por máquina. La información gubernamental debe ser administrada como un activo a lo largo de su ciclo de vida para fomentar la interoperabilidad y la apertura, de manera que los datos sean fáciles de encontrar, accesibles y utilizables. Al hacer de este el nuevo estado por default, los departamentos ejecutivos y las agencias se asegurarán de que protejan la privacidad, la confidencialidad y la seguridad nacional.

Obama señala en dicha orden que: "La apertura en el gobierno fortalece la democracia, promueve la entrega de servicios eficientes y efectivos al público, y contribuye al crecimiento económico" (Obama, 2013).

En el plano internacional, resulta valioso observar cómo se ubican diversos países en el Índice Global de Datos Abiertos, realizado por Open Knowledge Foundation[290]. En su primer informe "GODI 2016/17: El estado de los datos abiertos gubernamentales en 2017", se describen los obstáculos para la publicación de datos abiertos gubernamentales, a lo que se sugieren pasos que permitirán el progreso en materia de datos abiertos: *a)* los datos son difíciles (si no es que imposibles de encontrar en línea; *b)* es muy común que no se pueden usar fácilmente; y *c)* las licencias abiertas son prácticas poco frecuentes. Se requiere apegarse a estándares. A continuación, se muestran las primeras 12 posiciones en el Índice[291]:

---

[290] Open Knowledge Foundation. Texto tradución propia de: The GODI 2016/17 Report: The State of Open Government Data in 2017 this is Open Knowledge International's first State of Open Government Data report. Based on key findings from our work on the Global Open Data Index (GODI) 2016/17 it outlines the obstacles to open government data publication, and suggests steps that will allow progress in the field of open data. The report identifies three problem areas: 1) data is hard (or even impossible) to find online, 2) data is often not readily usable, 3) open licensing is rare practice and jeopardised by a lack of standards. Disponible en: *https://index.okfn.org/insights/*.

[291] GODI 2016/17 Report, *https://index.okfn.org/insights/*.

De acuerdo al Barómetro de Datos Abiertos, en los rankings Latinoamérica y por región, respectivamente, las posiciones son las siguientes[292]:

[292] The Open Data Barometer, *http://opendatabarometer.org/?_year=2016&indicator=ODB&region=:LA*.

The Open Data Barometer

A global measure of how governments are publishing and using open data for accountability, innovation and social impact.

Country	Rank	Score (OUT OF 100)	Change	Score Trend (OVER PAST EDITIONS)	Readiness (OUT OF 100)	Implementation (OUT OF 100)	Emerging Impact (OUT OF 100)
Mexico See details	11	73	5 ▲		83	58	88
Uruguay See details	17	61	2 ▲		75	64	38
Brazil See details	18	59	-1 ▼		66	55	59
Colombia See details	24	52	4 ▲		72	42	46
Chile See details	26	47	4 ▲		62	56	16
Argentina See details	38	38	14 ▲		57	35	23
Jamaica See details	40	37	13 ▲		44	35	36
Peru See details	48	33	-4 ▼		47	38	14
Dominican Republic See details	50	32	NEW		45	32	22
Paraguay See details	53	28	9 ▲		35	33	16

6. *La OCDE y datos en México*

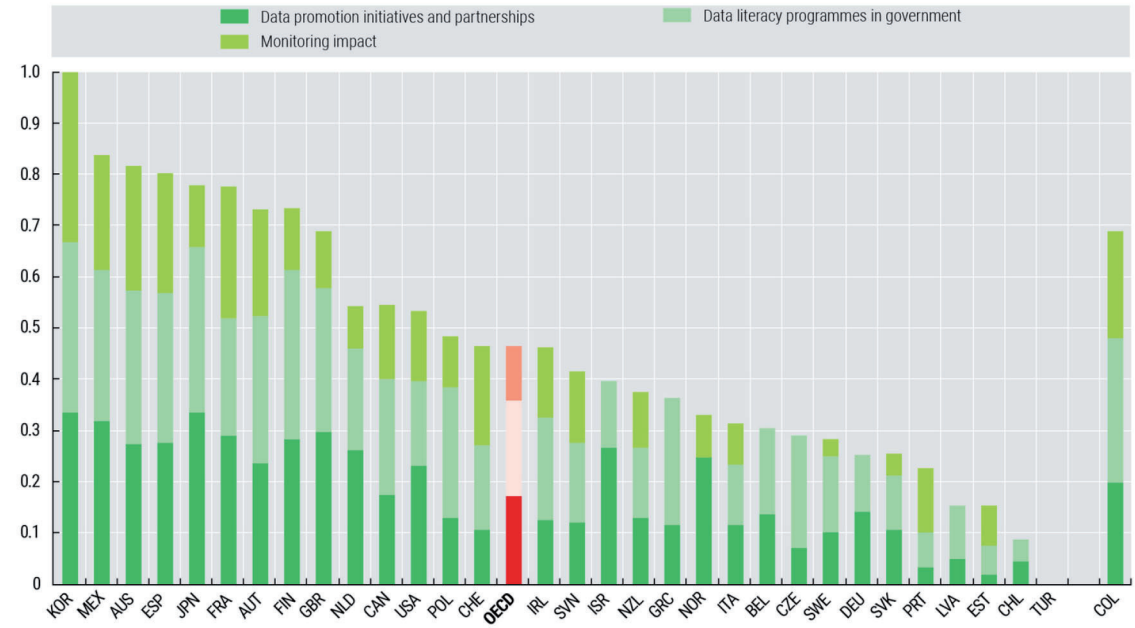
A partir de la publicación de la política de datos abiertos en México se desarrollaron acciones bajo un modelo de multiples actores, favoreciendo la interrelación entre oferta y demanda de los datos abiertos, identificando aliados estratégicos y obteniendo las experiencias de los países más desarrollados en el tema. Las cifras positivas de México en los rankings internacionales en materia de datos abiertos es gracias al liderazgo desde la Coordinación de Estrategia Digital Nacional y el trabajo conjunto de las dependencias y entidades de la Administración Pública Federal, y algunos aliados de la sociedad civil, la academia, los órganos autónomos y el esfuerzo destacado de las entidades federativas y algunos municipios.

La OCDE ha elaborado diversos estudios en los que refiere el avance de la política de datos abiertos de México[293]:

[293] *Government at a Glance 2017*, OurIndex Data, OCDE, p. 193, disponible en: *http://www.keepeek.com/Digital-Asset-Management/oecd/governance/government-at-a-glance-2017_gov_glance-2017-en#.WnKik4-cG3A#page194.*

El "Índice Nuestros Datos", ofrece información valiosa señalando que México se ubica en el segundo lugar en *reuso y creación de impacto con datos abiertos*, y el quinto lugar a nivel global, de lo que se observa un crecimiento de cinco lugares desde 2015"[294].

10.12. OURdata Index, government support for data re-use (pillar 3), 2017



Source: OECD Survey on Open Government DAta

Lo anterior, de acuerdo al Ejecutivo Federal, en voz de Alejandra Lagunes[295] y Enrique Zapata:

> Es resultado de las diversas iniciativas de uso de datos abiertos desarrolladas e implementadas en conjunto con aliados clave en todos los sectores de la sociedad, mediante las cuales se busca utilizar los datos abiertos como habilitadores del combate a la corrupción, servicios de salud personalizados, desarrollo económico, política pública basada en evidencia y desarrollo sostenible, entre muchos otros. Este es sin duda un gran logro, pero sabemos que pode-

[294] *México líder global de datos abiertos*, disponible en: *https://datos.gob.mx/blog/mexico-lider-global-de-datos-abiertos?category=noticias&tag=desarrollo-sostenible*.

[295] *Think Big, Data Innovation in Latin America and the Caribbean*, México Digital, *https://www.youtube.com/watch?v=jBfV34zhE24*.

mos hacer más. Por esta razón –y siguiendo las conclusiones del Reporte– el día de hoy se anunciaron algunos compromisos que serán trabajados como parte de la política de datos abiertos en México en los próximos meses:

- En conjunto con DEMOS, el Open Data Institute y la Embajada del Reino Unido en México, se dará inicio a la segunda fase de Labora –la iniciativa de desarrollo económico con datos abiertos. En esta ocasión, además de seguir creando capacidades de uso en PyMEs, se trabajará con incubadoras y aceleradores sectoriales–, comenzando por el sector de FinTech, para hacer de los datos abiertos un verdadero insumo productivo para la economía.
- Para avanzar hacia un modelo colaborativo de plataformas de datos abiertos, hoy se lanza una colaboración estratégica entre la plataforma datos.gob.mx y el sitio de Datos Abiertos de la Sociedad Civil Datamx.io, con el objetivo de fomentar la publicación de datos abiertos del sector privado y la sociedad civil, así como para aumentar la calidad de los datos existentes a través de estrategias de generación colaborativas.
- Para robustecer el marco de gobernanza para los datos abiertos a nivel internacional, trabajaremos con el Banco Interamericano de Desarrollo (BID) y la Carta Internacional de Datos Abiertos para que México sea el primer país del mundo en probar la implementación de la Guía de Datos Abiertos Anticorrupción.
- Por último, junto con la OCDE, se comenzará el desarrollo del reporte "Futuro de los Datos Abiertos MX", para establecer la visión, objetivos y acciones para fortalecer, acelerar y dar continuidad al uso de datos abiertos en México durante los próximos años.

En la elaboración del estudio OCDE, "Futuro de los datos abiertos en México[296], se pretende identificar oportunidades para fortalecer y dar continuidad a la polí-

[296] *El futuro de los datos abiertos en México: retos y experiencias en países de la OCDE*, disponible en el canal de YouTube, DatosGobMx, octubre 2017. Este webinar es un ejercicio de interacción con diferentes actores expertos en datos abiertos, de diferentes países de la OCDE, en el que intercambian opiniones, experiencias sobre datos abiertos y cómo estos constituyen un catalizador para el desarrollo económico, político y social. Estos ejercicios son sumamente valiosos porque con

tica de datos abiertos en México en los próximos años. El estudio se realizó en las siguientes etapas[297]:

1. Webinario para intercambiar experiencias entre países de la OCDE. En la primera fase se llevó a cabo un webinario sobre experiencias y retos en políticas de datos abiertos en otros países miembros de la OCDE, así como sobre el desarrollo de capacidades digitales al interior de las instituciones y la gobernanza de estas iniciativas. En la conversación participaron representantes de Argentina, Francia, Reino Unido, Corea y España[298].
2. Cuestionarios en línea a generadores y usuarios de datos de gobierno, sociedad civil e iniciativa privada. La OCDE envió un cuestionario en línea a enlaces de las dependencias y entidades de la Administración Pública Federal, así como representantes de organizaciones de la sociedad civil y empresas, para obtener insumos sobre las fortalezas, debilidades, oportunidades y amenazas a la política de datos abiertos en los próximos años.
3. Entrevistas técnicas a actores clave. Expertos de la OCDE realizaron entrevistas a 35 actores clave de los ámbitos privado, de la sociedad civil y gubernamental, que publican datos abiertos en "datos.gob.mx", o que utilizan los mismos para crear oportunidades de negocio o mejorar la rendición de cuentas. Durante las entrevistas se obtuvieron perspectivas y recomendaciones de expertos y usuarios para visualizar el futuro de los datos abiertos en México.

Aunado a lo anterior, algunos expertos expresan su visión sobre datos abiertos de la siguiente manera.

"Estamos haciendo una cultura del manejo de los datos abiertos. En Conagua creemos que el existir una plataforma específica para encontrar información es muy positivo, pues socializa la información y permite una corresponsabilidad del usuario con las acciones del gobierno": Alfonso Camarena, Conagua.

---

el uso de la tecnología se pueden conocer los retos y experiencias de los diferentes países de manera muy ágil, y con ello contribuir a fortalecer las acciones que se realizan en México y otros países. Disponible en: *https://www.youtube.com/watch?v=GSBjXM4cAPc.*

[297] *El futuro de los datos abiertos en México*, *op. cit.*

[298] Webinario *El futuro de los datos abiertos en México*, *https://datos.gob.mx/blog/webinario-el-futuro-de-los-datos-abiertos-en-mexico?category=aprende&tag=economia.*

Algunas de las personas entrevistadas provinieron de instituciones como Segob, RAN, SAT, Conagua, Cenapred, SHCP, IMSS, INEGI; así como de sociedad civil e iniciativa privada, como DEMOS, Transparencia Mexicana, Google México, OPI Analytics, PODER, SocialTIC y Data-Pop Alliance, entre otros. "El campo de los datos abiertos no se ha terminado de explorar, en un futuro vamos a encontrar más objetos accionables, más inteligencia, pero sobre todo vamos empezar a ver más exigencia, nuevos temas y mayor calidad de la información que nos va a llevar a una mayor innovación": Sergio Araiza, SocialTIC.

Los participantes aportaron ideas y propuestas para la sostenibilidad de la política, el fortalecimiento de la comunidad de usuarios de datos abiertos en México, formas de financiamiento de proyectos para la innovación y las áreas de oportunidad en el gobierno para convertir a los datos abiertos en un insumo para las actividades y toma de decisiones de distintos actores.

> Los datos abiertos tienen un valor democrático, los ciudadanos tenemos derecho a saber qué pasa en nuestras instituciones. Los datos abiertos los podemos usar para la rendición de cuentas, pero también para la interoperabilidad, generación de valor en las empresas y para la participación ciudadana. Creo que en el futuro los datos abiertos van a ser más utilizados y formarán parte de una infraestructura básica del gobierno: Eduard Martín-Borregón, Poder.

Los beneficios en la publicación y uso de datos abiertos en México son cada vez más visibles y reconocidos en el ámbito nacional e internacional. Sin embargo, existen retos en términos de gobernanza y sostenibilidad de las iniciativas, que requiere de la participación y colaboración de todos los sectores. El futuro de los datos abiertos se construye entre todos.

> El valor de los datos abiertos en México va más allá de transparencia y rendición de cuentas, y se ha convertido poco a poco en una infraestructura nacional de información que permite hacer a las empresas más productivas y el trabajo de gobierno más efectivo en términos de la distribución de recursos y medición de resultados. Hay una tendencia muy clara en usar los datos abiertos para mejorar los procesos y medir el impacto que pueden tener estos para mejorar y conocer mejor a relación con los clientes y los ciudadanos: Alejandro Maza, OPI Analytics.

Por último, cabe mencionar: "Los datos abiertos son y serán la unidad de lenguaje más importante para el futuro": Enrique Zapata, Datos abiertos, Estrategia Digital Nacional.

7. *Panorama de organizaciones e iniciativa de datos abiertos y periodismo de datos en América Latina 2016-2017*[299]

Esta obra refleja de manera interesante el uso de los datos abiertos en labores periodísticas. Respecto del panorama en México señala lo siguiente.

> En el lado positivo, México es el país mejor posicionado de América Latina en datos abiertos, de acuerdo con el barómetro. Según Ricardo Alanís, de las organizaciones dateras Codeando México y Cívica Digital, el país está muy adelantado en legislación y compromisos públicos.
>
> "México tiene una ventaja en dos de las áreas más relevantes en el Barómetro para evaluar la capacidad de datos abiertos, que es readiness e impact. En readiness estamos muy adelantados. Esta clasificación evalúa el entorno de la legislación y las características del país para poder generar datos abiertos. En impacto estamos también en los percentiles más altos de la región, superando a Uruguay y Brasil, y el impacto significa qué se está haciendo con los datos abiertos"; dijo Alanís a Distintas Latitudes.
>
> En la legislación, el entorno regulatorio nos ha puesto a la vanguardia. Pero hay muchos aspectos pendientes de aplicación. Los *datasets* todavía no están en el nivel, o estamos en el proceso de mejorar la calidad de los *datasets;* agregó.
>
> Para Alanís, los retos más grandes están en implementación, que implica una formalización de las estrategias de uso de datos contra la corrupción, para el desarrollo económico y la seguridad social. También, es importante analizar cómo se está dando seguimiento a los indicadores del país, si los periodistas están usando los *datasets* y sacando notas, para que se aumente la calidad de vida, la eficiencia gubernamental y el desarrollo del país.
>
> "En ese sentido, creo que los datos que estamos generando ya están cubriendo las áreas funcionales del país, pero nos falta muchísimo para mejorar su

[299] Pérez Damasco, Diego, *Datos, dateros y debates: Panorama de organizaciones e iniciativa de datos abiertos y periodismo de datos en América Latina 2016-2017,* Factual/Distintas latitudes, 2017, *https://distintaslatitudes.net/wp-content/uploads/2018/01/Datos_Ebook.pdf.*

uso. De ahí, esfuerzos como el *Open Data Charter,* están empujando mucho la profundización temática de los datos"; dijo Alanís.

Por otro lado, todavía se debe impulsar mucho el desarrollo local y el uso local de datos abiertos. Estados como Puebla, Jalisco, Nuevo León y Guadalajara están haciendo esfuerzos interesantes, los cuales necesitan una mayor integración y un salto, porque justamente es en lo local donde se pueden hacer grandes cambios.

8. *Datos abiertos para el desarrollo sostenible*

Para entender a qué se refiere el desarrollo sostenible, la Asamblea General de las Naciones Unidas lo define como: "la satisfacción de las necesidades de la generación presente sin comprender la capacidad de las generaciones futuras para satisfacer sus propias necesidades" (AGNU, 1987).

El desarrollo sostenible ha emergido como el principio rector para el desarrollo mundial a largo plazo. Consta de tres pilares que el desarrollo sostenible trata de lograr de manera equilibrada: el desarrollo económico, el desarrollo social y la protección del medio ambiente.

El gobierno mexicano, como parte de su política pública, ha desarrollado una herramienta para abordar el avance de los ODS a partir del uso de los datos abiertos. La herramienta es *www.agenda2030.mx.* En dicho sitio, el gobierno mexicano señala:

> Durante la 70° sesión de la Asamblea General de las Naciones Unidas en Nueva York, los 193 Estados miembros se reunieron en la Cumbre Global de Desarrollo Sostenible para adoptar la Agenda 2030. Esta marca un ambicioso plan de acción internacional con 17 nuevos objetivos de desarrollo, llamados los Objetivos de Desarrollo Sostenible (ODS), que buscan ampliar los Objetivos de Desarrollo del Milenio (ODM), acordados en el marco de la Cumbre del Milenio de las Naciones Unidas en el año 2000[300].

[300] *Se lanza herramienta de datos para los objetivos de desarrollo sostenible*, Plataforma Nacional Digital, *https://datos.gob.mx/blog/se-lanza-herramienta-de-datos-para-los-objetivos-de-desarrollo-sostenible?category=casos-de-uso&tag=geoespacial.*

> En esta se pretenden alcanzar los retos globales en todos los ámbitos, se debe reconocer que existe una crisis en el centro de estos esfuerzos, una crisis de escasez de datos. A la vez nos enfrentamos a una transformación global que busca aprovechar el potencial de las nuevas tecnologías, impulsadas por la revolución de datos, para impactar positivamente en el desarrollo económico y social del mundo.
>
> México junto con Colombia, Kenia y Estados Unidos, anunciaron la Alianza Global de Datos para el Desarrollo Sostenible en respuesta a esta crisis[301].
>
> Esta alianza busca apoyar la toma de decisiones basadas en datos, promoviendo los datos abiertos y la generación de nuevos datos de múltiples fuentes para ayudar a hacer frente a los desafíos que los Objetivos de Desarrollo Sostenible presentan: acabar con la pobreza extrema, luchar contra el cambio climático y garantizar una vida saludable para todos. Al asegurar nuevas inversiones en datos de calidad y oportunos, promover la adopción de principios comunes para abrir y compartir datos y conectar datos con acciones.

Al respecto, es de resaltar el esfuerzo de México en la medición de los trabajos en materia de la Agenda 2030[302].

9. *Datos abiertos en México*

El Plan Nacional de Desarrollo 2013-2018 tiene como una de sus estrategias transversales la de "Gobierno cercano y moderno", la cual señala como una de sus líneas de acción el Objetivo 5: "Establecer una Estrategia Digital Nacional para fomentar la adopción y el desarrollo de las TICs, e impulsar un gobierno eficaz que inserte a México en la Sociedad del Conocimiento". Dicho Objetivo incluye el de Transformación Gubernamental, que pretende construir un gobierno innovador, transparente, eficiente, abierto, centrado en las necesidades de la sociedad, y que utiliza la tecnología para mejorar la relación con los ciudadanos, así como un habilitador de datos abiertos, el cual considera:

---

[301] *Cfr. https://www.gob.mx/cidge/articulos/alianza-global-de-datos-para-el-desarrollo-sustentable?idiom=es.*
[302] Disponible en: *http://www.onu.org.mx/agenda-2030/*.

- Generar y coordinar acciones orientadas hacia el logro de un gobierno abierto;
- La estrategia digital nacional utiliza la política de datos abiertos como habilitador para el fomento de la transparencia, innovación y la participación ciudadana; e
- Impulsa la publicación de datos abiertos para crear un ecosistema de cocreación de servicios públicos, detonar la innovación y el emprendimiento, al convertir la información en manos del gobierno en un activo de valor social (México Digital, 2017).

Todo gobierno que se quiera considerar abierto tendrá que establecer bases para la acción conjunta de políticas, estrategias, compromisos y diversas formas de actuación colaborativa. De esta forma se puede perfilar que el gobierno abierto es un modo de gobernar y gestionar lo público en una democracia, que se caracteriza por proveer información pública a la ciudadanía, en su forma más pura y fácil de acceso, como son los datos abiertos. Si bien estos por sí solos no representan la nueva transparencia, están acompañados de atributos de calidad que otorgan valor a la información pública.

Desde el año 2013, el Gobierno de la Republica comenzó a trabajar con representantes del sector público, social y privado para implementar su política de datos abiertos, y a dos años de la publicación del Decreto por el que se establece la regulación en materia de datos abiertos, México es líder en América Latina y el Caribe, y su política es una de las más reconocidas a nivel global.

Esto es resultado de las diversas iniciativas de uso de datos abiertos, desarrolladas e implementadas en conjunto con aliados clave en todos los sectores de la sociedad, mediante las cuales se busca utilizar los datos abiertos como habilitadores del combate a la corrupción, servicios de salud personalizados, desarrollo económico, política pública basada en evidencia y desarrollo sostenible, entre muchos otros (Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (2015).

A. *Política de datos abiertos*

México dio sus primeros pasos en materia de datos abiertos a través de la publicación del Esquema de Interoperabilidad y Datos Abiertos (EIDA)[303], el cual señala como objetivo: "… la integración de los procesos relacionados con servicios digitales, así como para compartir y reutilizar plataformas y sistemas de información, a fin de incrementar la eficiencia operativa de la Administración Pública Federal y su relación con la sociedad". Y define a los datos abiertos como: "los datos digitales de carácter público que administra la APF y que en términos de las disposiciones aplicables no tienen naturaleza reservada o confidencial y que son accesibles de modo que los particulares pueden reutilizarlos según convenga a sus intereses".

Como puede observarse la definición está enmarcada en el contexto de la Administración Pública Federal, lo cual parece un error importante, aunque es válido por el ámbito de aplicación y dado que los destinatarios de la norma administrativa son las dependencias y entidades de la Administración Pública Federal, mismas que conforme este Acuerdo (EIDA) están obligadas a: "Poner a disposición de la sociedad, cuando la información digital sea pública y en términos de las disposiciones aplicables no tenga naturaleza reservada o confidencial, *como datos abiertos*, de modo tal que sea *técnicamente posible localizarla, recuperarla, indizarla y reutilizarla* a través de aplicaciones Web".

Para inicios de la Administración 2013-2018, el Gobierno Federal, bajo el liderazgo de la Coordinación de Estrategia Digital Nacional, realizó un estudio de preparación de la política de datos abiertos, a saber: "Diagnóstico sobre el Estado de Preparación de Datos Abiertos preparado para el Gobierno de los Estados Unidos Mexicanos"[304]. En el referido documento se observa que:

---

[303] Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal, publicado en el Diario Oficial de la Federación el 6 de septiembre de 2011, disponible en: *http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011.*

[304] El "Estudio de Preparación para la Apertura de Datos del Gobierno de los Estados Unidos Mexicanos", ha sido elaborado por dos consultores internacionales: Jeff Kaplan y Nagore de los Ríos, como producto final de un trabajo de campo en el que ha participado de forma muy activa el Gobierno de México y que ha contado también con la voz de representantes de distintos sectores de la sociedad civil. Disponible en: *http://opendatatoolkit.worldbank.org/docs/odra/odra_mexico_complete.pdf.*

La evaluación utiliza un enfoque ecosistémico para abrir los datos, lo que significa que está diseñado para observar el entorno más amplio de Datos Abiertos. En el lado de la "oferta", incluye asuntos como el marco de políticas y normas, los datos ya existentes en el gobierno, la infraestructura tecnológica y los estándares; mientras que del lado de la "demanda" surgen temas como los mecanismos de participación ciudadana, la demanda existente de datos del gobierno, y la existencia de comunidades de posibles usuarios. Esta evaluación establece medidas sobre ocho dimensiones que se consideran esenciales para una iniciativa sostenible de Datos Abiertos: 1. Liderazgo; 2. Legislación y Políticas; 3. Organización; 4. Datos públicos; 5. Demanda; 6. Ecosistema y comunidades de usuarios; 7. Financiamiento; 8. Tecnología.

Primera conclusión. Potencial líder. A la hora de centrar sus esfuerzos en abrir datos, el Gobierno Federal de México inicia con una serie de ventajas comparativas, tales como: casi todos los datos importantes son digitales; poseen una gran cantidad de talento técnico y parte de la sociedad civil capacitada; existen casos de Datos Abiertos bajo algunas iniciativas a nivel sub-nacional; hay una clara vinculación de Datos Abiertos con los principios y objetivos de las iniciativas del Presidente, y ya existe un equipo designado y trabajado en implementar la apertura de datos. Esto puede posicionar a México dentro de los líderes de los Datos Abiertos si se consiguen superar algunos obstáculos importantes y mantener la voluntad política detectada, dando un gran salto cualitativo.

Segunda conclusión. Los Datos Abiertos suponen grandes oportunidades para México. Pueden ayudar a transformar el "sistema operativo" del gobierno a la hora de realizar inversiones públicas, mejorar los servicios públicos, formular políticas basadas en evidencias y gobernar de forma transparente. También supone una enorme oportunidad para incrementar la economía del país a través de la reutilización de los datos por parte de empresas, desarrolladores y emprendedores. Así mismo, pueden servir de ejemplo y ayudar a los Estados a mejorar su forma de gestionar. Y pueden situar a México entre los principales países en esta tendencia emergente.

Tercera conclusión. Los mayores obstáculos para la puesta en marcha y el mantenimiento de la iniciativa de datos abiertos son:

- Falta de comprensión en algunas áreas legales del gobierno sobre la importancia de la iniciativa de Datos Abiertos; y sobre las licencias abiertas que requieren los datos para ser catalogados como "Datos Abiertos".
- Establecer mecanismos de coordinación internos que garanticen una eficaz implementación de una política de Datos Abiertos, que ayuden a promover el uso de los datos y ofrezcan soluciones adecuadas para poder hacer frente a la demanda.
- La falta de capacidad de las entidades federales para acceder a algunos de los tipos de datos más importantes (ejemplos: datos catastrales, el gasto sanitario por ubicación, los gastos menores al 30% del Seguro Popular), debido a la autonomía de los gobiernos estatales y locales bajo la estructura de política descentralizada de México.
- Algunos altos cargos de Secretarías y entidades clave han expresado su interés en generar Datos Abiertos, sin embargo, todavía no son visibles de cara al público porque sus acciones no han trascendido fuera ni dentro del gobierno.

Cuarta conclusión. La situación de los datos geoespaciales en México es problemática. Esto supone un problema a resolver, ya que se ha comprobado que los datos de GIS (Sistemas de Información Geográfica) son los más depurados y reutilizados por otros gobiernos del mundo que han implementado iniciativas de Datos Abiertos, y además porque se ha demostrado que son claves para generar un sustancial valor económico. Los datos del GIS no están fácilmente accesibles, lo que perjudica la innovación, especialmente para las pequeñas y medianas empresas.

Quinta conclusión. Una iniciativa Federal de Datos Abiertos puede ser diseñada para fortalecer y apoyar directamente las prioridades del Plan Nacional de Desarrollo.

De manera general, esta es la evaluación:

Áreas de evaluación	Importancia	Evaluación
1. Liderazgo	Muy alta	
2. Legislación / políticas	Alta	
3. Organización	Medio-alta	
4. Datos públicos	Alta	
5. Demanda	Alta	
6. Reutilización y comunidades	Medio-alta	
7. Financiamiento	Alta	
8. Tecnología	Alta	

El análisis concluye en general que: "Basándonos en las dimensiones estudiadas, la conclusión general es que el Gobierno de México presenta bases sólidas sobre las que llevar a cabo una iniciativa de Datos Abiertos exitosa para ayudar a impulsar los objetivos prioritarios del Plan Nacional de Desarrollo y que le posicione entre los mejores de su ámbito".

La política de datos abiertos orienta la relación de la oferta y la demanda, en las necesidades tanto de instituciones como de los usuarios que precisan datos. Las instituciones públicas del Gobierno Federal en México son parte de una consulta en la que la ciudadanía y todos los sectores colaboran en la priorización de los datos que se quieren abrir, vinculando así la oferta y la demanda y elevando el nivel de eficiencia de la política de datos abiertos. Se busca publicar de aquellos que pueden ser de mayor utilidad para crear nuevos servicios, hacer política pública basada en evidencia, fomentar el crecimiento económico y combatir la corrupción, entre otros objetivos prioritarios.

Dado que los datos son activos de información pública, producto del ejercicio de los recursos públicos, se entiende que los datos son de esta última naturaleza cuando son publicados en formatos abiertos, pueden ser reutilizados y redistribuidos en beneficio de la sociedad en general, no solo en materia de transparencia,

sino también para mejorar servicios como el agua, transporte, educación, salud; así como para detonar actividades económicas en diversos sectores.

El objetivo de la política de datos abiertos es sentar las bases para que los mismos se conviertan en una herramienta para facilitar el *crecimiento económico, fortalecer la competitividad y promover la innovación; al tiempo que permiten mejorar la prestación de servicios gubernamentales, incrementar la transparencia y rendición de cuentas, y conducir a una mayor eficiencia gubernamental*; logrando así una mejor gobernanza para el país (México Digital, 2014).

A finales de 2017, la página oficial del Gobierno Federal en materia de datos abiertos, *www.datos.gob.mx,* señala que contiene más de 25,590 datos de 245 instituciones. Los cuales han sido publicados por diferentes organismos. Con este portal se pretende atender el reto de que los datos abiertos lleguen a cualquier tipo de usuarios, no solo a técnicos y desarrolladores, sino también a analistas, periodistas, académicos y, en general, a cualquier persona que esté interesada en aprender a utilizar y aprovechar los datos con fines lícitos.

B. *Marco jurídico y modelo institucional de los datos abiertos*

La política de datos abiertos en México es un conjunto de ordenamientos jurídicos, modelo de gobernanza dentro de la Administración Pública Federal, que incluye una coordinación, un líder del tema y todas las dependencias y entidades como entes que colaboración en la implementación de la misma; aunado a la participación de la sociedad civil, individuos y empresas, que contribuyen en la selección de datos prioritarios a abrir y en la retroalimentación a partir de la demanda y consumo de los conjuntos de datos.

Los datos abiertos requerían, al inicio de 2013, un marco normativo que diera forma a la política de datos abiertos, para ello el gobierno federal publicó el Decreto por el que se establece la regulación en materia de Datos Abiertos[305]. Con este, se ordenó que los datos de la información pública de las dependencias y entidades de

[305] El 20 de febrero de 2012 se publicó en el Diario Oficial de la Federación el Decreto que establece la regulación en materia de Datos Abiertos, disponible en: *http://www.dof.gob.mx/nota_detalle.php?codigo=5382838&fecha=20/02/2015.*

la Administración Pública Federal se pondrán a disposición de la población como datos abiertos precisamente, con el objetivo de facilitar su acceso, uso, reutilización y redistribución para cualquier fin lícito. Los datos abiertos se institucionalizan en México bajo la política de datos abiertos como una herramienta clave para impulsar el crecimiento económico, fomentar la innovación y mejorar la eficiencia gubernamental; además de apoyar la lucha contra la corrupción e incrementar la transparencia y rendición de cuentas.

En el portal de Internet *www.datos.gob.mx*[306] se conformó un catálogo de datos descargables en formatos abiertos, integrado por los conjuntos de datos de las dependencias y entidades.

El Decreto fijó las características mínimas para que tales conjuntos sean considerados datos abiertos: que sean gratuitos, no discriminatorios, de libre uso, legibles por máquinas, integrales, primarios, oportunos y permanentes. En su Artículo Primero precisa el objeto que tiene y este es:

> Regular la forma mediante la cual, *los datos de carácter público*, son *generados por las dependencias y entidades* de la Administración Pública Federal y por las empresas productivas del Estado, se pondrán a disposición de la población como datos abiertos, con el propósito de facilitar su acceso, uso, reutilización y redistribución para cualquier fin, conforme a los ordenamientos jurídicos aplicables.
>
> Retomando la precisión de lo público, esto trae consigo la obligación de analizar:
>
> - La Ley General de Transparencia y Acceso a la Información Pública;
> - Ley Federal de Transparencia y Acceso a la Información Pública;
> - La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados;
> - La Ley de Seguridad Nacional;
> - Y otras disposiciones complementarias.

Después de este análisis podremos identificar si se trata de información pública. Si lo es, se presume que los datos son públicos y por lo tanto deberán publicarse, o ponerse a disposición, a través del sitio para su uso por cualquier persona.

---

[306] *www.datos.gob.mx.*

El proceso antes descrito puede presentar casos de interpretación que tendrán que transcurrir por el proceso establecido en materia de transparencia y acceso a la información pública.

> En complemento, el Decreto de referencia establece:
> ARTÍCULO QUINTO.- Para ser considerados como datos abiertos, los conjuntos de datos deberán contar con las características mínimas siguientes:
> I. Gratuitos: Se obtendrán sin entregar a cambio contraprestación alguna;
> II. No discriminatorios: Serán accesibles sin restricciones de acceso para los usuarios;
> III. De libre uso: Citarán la *fuente* de origen como único requerimiento para ser utilizados libremente;
> IV. Legibles por máquinas: Deberán estar estructurados, total o parcialmente, para ser *procesados* e interpretados por equipos electrónicos de manera automática;
> V. Integrales: Deberán contener, en la medida de lo posible, el tema que describen a detalle y con los metadatos necesarios;
> VI. Primarios: Provendrán de la fuente de origen con el máximo nivel de desagregación posible;
> VII. Oportunos: Serán actualizados periódicamente, conforme se generen; y
> VIII. Permanentes: Se deberán conservar en el tiempo, para lo cual, las versiones históricas relevantes para uso público, se mantendrán disponibles a través de identificadores adecuados para tal efecto.

Como se puede observar, de las características anteriores no se advierte alguna que tenga conflicto con el derecho a la protección de datos personales.

C. *Guía de implementación*

Esta Guía tiene como propósito presentar, de manera general, los procesos que serán necesarios para la publicación de la información pública del gobierno en formatos abiertos y menciona las directrices generales que deberán seguirse. En específico está centrado en los dos primeros pasos de la etapa de preparación de datos con los cuales las entidades y dependencias podrán avanzar en el proceso de publicación de datos.

Es importante señalar que esta Guía de implementación menciona las características que deberán cumplir los datos para poder ser considerados abiertos y son las siguientes:

- Completos: que reflejen la totalidad del tema y descritos con detalle;
- Públicos: de interés general y carácter público, protegiendo la privacidad;
- Primarios: que provienen de la fuente original y tienen el máximo nivel de desagregación posible
- En tiempo: siendo oportunos y actualizados tan pronto sea posible;
- De libre acceso: disponibles de manera conveniente, sin restricciones de acceso ni discriminación;
- Procesable por máquina: estructurados de tal forma que permita el procesamiento automático;
- En formatos abiertos: que utilicen estándares abiertos, procesables por máquinas, y pueden ser descargables y operados con los requerimientos tecnológicos mínimos;
- Con licencia de libre uso: que define claramente la libertad y certeza de ser utilizados como insumo para cualquier fin, requiriendo, a lo mucho, atribución;
- Permanentes: para habilitar la capacidad de encontrar la información publicada a perpetuidad; y para que toda información hecha pública, permanezcan así, siempre con identificadores adecuados respecto a versiones y archivada en el tiempo;
- Costos de utilización: que deberán ser justos, preferentemente nulos, para evitar barreras al uso por parte de los ciudadanos.
  (Énfasis añadido)

Como se puede observar, en la cualidad de "público" se señala que no podrá afectar la privacidad, es decir, uno de los filtros previos a publicar es el análisis de lo público, la privacidad, lo confidencial.

Entiéndase el documento integrado por directrices técnicas que están pensadas para apoyar las políticas públicas que ponga en marcha el Gobierno de la Republica en materia de datos abiertos.

Los pasos que describe la Guía para la instrumentación de la política de datos abiertos son:

1) Paso 1 | Planea
   1.1. Formar un grupo de trabajo y designar un Enlace y Administrador de Datos Abiertos.
   1.2. Priorizar los datos de valor.
   1.3. Generar, publicar y actualizar el Plan Institucional de Publicación de Datos Abiertos.
2) Paso 2 | Publica
   2.1. Convertir los datos a formatos abiertos.
   2.2. Incrementar la interoperabilidad y usabilidad de los Datos Abiertos.
   2.3. Mejorar la disponibilidad y medios de distribución de los Datos Abiertos.
   2.4. Documentar de acuerdo al estándar DCAT y publicar el Catálogo Institucional de Datos Abiertos.
3) Paso 3 | Perfecciona
   3.1. Asegurar la disponibilidad de las URL utilizadas para publicar los Datos Abiertos.
   3.2. Fomentar la calidad de los Datos Abiertos publicados.
   3.3. Responder a los reportes ciudadanos de Datos Abiertos realizados mediante *datos.gob.mx.*
   3.4. Asegurar el cumplimiento con la Política de Datos Abiertos.
4) Paso 4 | Promueve
   4.1. Asegurar la generación, publicación y uso de Datos Abiertos en las herramientas y aplicativos digitales del gobierno.
   4.2. Impulsar el uso de Datos Abiertos en la ciudadanía.
   4.3. Establecer estrategias de comunicación digital.

De lo anterior destaca la priorización en razón de la participación de los generadores y de la sociedad en su conjunto, además el que se autocorrija derivado de la etapa de madurez donde se toman consideraciones de externos.

D. *Datos abiertos en la Ley General y Federal de Transparencia*

El derecho a la información es un derecho fundamental de toda persona, que consiste en solicitar, investigar, difundir, buscar y recibir información y documentos, en manos del gobierno. Para tener un marco común que garantizará el ejercicio y protección de este derecho en el país, se implementó la Ley General de Transparencia y Acceso a la Información Pública.

Esta Ley es reglamentaria del Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia y acceso a la información. Tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios.

En cuanto a la reglamentación de datos abiertos, en su Artículo 3o., fracción VI, describe qué son y cuáles son las características de los datos abiertos. Refiere así:

> Los datos abiertos son los datos digitales de carácter público que son accesibles en línea que pueden ser usados, reutilizados y redistribuidos por cualquier interesado y que tienen las siguientes características:
> a) Accesibles: Los datos están disponibles para la gama más amplia de usuarios, para cualquier propósito;
> b) Integrales: Contienen el tema que describen a detalle y con los metadatos necesarios;
> c) Gratuitos: Se obtienen sin entregar a cambio contraprestación alguna;
> d) No discriminatorios: Los datos están disponibles para cualquier persona, sin necesidad de registro;
> e) Oportunos: Son actualizados, periódicamente, conforme se generen;
> f) Permanentes: Se conservan en el tiempo, para lo cual, las versiones históricas relevantes para uso público se mantendrán disponibles con identificadores adecuados al efecto;

g) Primarios: Provienen de la fuente de origen con el máximo nivel de desagregación posible;
h) Legibles por máquinas: Deberán estar estructurados, total o parcialmente, para ser procesados e interpretados por equipos electrónicos de manera automática;
i) En formatos abiertos: Los datos estarán disponibles con el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no suponen una dificultad de acceso y que su aplicación y reproducción no estén condicionadas a contraprestación alguna;
j) De libre uso: Citan la fuente de origen como único requerimiento para ser utilizados libremente.

En cuanto a la Ley Federal de Transparencia y Acceso a la Información Pública, únicamente se refiere a los datos abiertos para la integración de un consejo consultivo, el cual estará integrado por diez consejeros honoríficos que serán propuestos por la Cámara de Senadores y durarán en su encargo siete años. Estos tienen la facultad –mejor dicho, el deber– de proponer mejores prácticas de participación ciudadana y colaboración en la implementación y evaluación de la regulación en materia de datos abiertos.

E. *Otros ordenamientos jurídicos en los que se refiere a los datos abiertos*

- Lineamientos y metodología para la liberación de grupos de Datos Abiertos. Cuyo objetivo es presentar a las dependencias y entidades de la Administración Pública Federal, que han suscrito bases de colaboración, conforme a lo que se establece en el Artículo Sexto del Decreto, los lineamientos que permitan a estas contar con herramientas de apoyo, a fin de que establezcan planes con acciones precisas para el cumplimiento de las metas que derivan de las medidas e indicadores que comprometieron en dichas bases, en lo que a materia de Tecnologías de la Información y Comunicaciones (TICs), en Datos Abiertos se refiere[307] (México Digital, 2015).

[307] *Cfr.http://www.funcionpublica.gob.mx/web/doctos/ua/ssfp/uegdg/pgcm/material/documentos/ti_3_pgcm_bases_lineam_datosabiertos.pdf.*

- Norma técnica para el acceso y publicación de Datos Abiertos de la Información Estadística y Geográfica de Interés Nacional. Esta norma tiene por objeto establecer las disposiciones para que los conjuntos de datos en el marco del servicio público de información estadística y geográfica, generados y administrados por las unidades del Estado, se pongan a disposición como datos abiertos, con el propósito de facilitar su acceso, uso, consulta, reutilización y redistribución para cualquier fin[308].
- Manual de implementación para el acceso y publicación de Datos Abiertos de la Información Estadística y Geográfica de Interés Nacional. Este Manual es una herramienta que regula, bajo parámetros tecnológicos homogéneos y de acuerdo a las mejores prácticas nacionales e internacionales, la puesta a disposición de la Información de interés nacional en materia de datos abiertos. Su elaboración obedece a la necesidad de promover la disponibilidad, difusión, uso, reutilización e intercambio de datos abiertos de la información estadística y geográfica de interés nacional al servicio de la sociedad[309].

F. *Protección de datos personales como componente de la política de datos abiertos*

Un dato personal es aquella información concerniente a una persona física identificada o identificable, la cual solo debe usarse para los propósitos que fue entregada. Toda persona tiene derecho a la protección, acceso, supresión o corrección de sus datos personales, que obran en los archivos de gobierno.

La Constitución considera la protección de datos personales como derecho fundamental. Su salvaguarda se divide en dos ámbitos: Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados y Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

La primera Ley en cita tiene el objeto de establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados. Son sujetos obligados por esta Ley, 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.

---

[308] *Cfr. http://www.dof.gob.mx/nota_detalle.php?codigo=5374183&fecha=04/12/2014.*

[309] *Cfr.http://www.snieg.mx/contenidos/espanol/Normatividad/Normatividad_Vigente/Archivos_NV/Manual_de_Implementacion_DA_02062015.pdf.*

Por su parte, la Ley Federal del Protección de Datos Personales en Posesión de los Particulares tiene como objeto proteger los datos personales en posesión de las empresas, así como regular que dichos datos sean usados únicamente para la finalidad que fueron entregados, que se tenga un control de quién y para qué los tiene y que el titular o dueño de los datos siempre esté informado del trato dado a los mismos, buscando con lo anterior garantizar la privacidad y el derecho a la autodeterminación informativa de los individuos. Esta Ley será la aplicable para cuando se trate de datos abiertos de la información que posea un particular, el cual deberá garantizar el debido cumplimiento del derecho del titular de la información que almacena o está tratando.

Es importante recordar que cuando se lleva a cabo el tratamiento de datos se puede reducir el riesgo mediante acciones técnicas de disociación de datos y acciones de cifrado, para evitar su divulgación con cruce de datos abiertos o bases que se consiguen a través de Internet. Más aún, si consideramos que hoy día el poder del Big Data es enorme y que desafortunadamente no estamos exentos de la venta de bases de datos en el mercado negro. Por ello es vital reforzar el trabajo en materia de privacidad y seguridad de la información en los proyectos de datos abiertos.

A manera de revisión, la política de datos abiertos en México ha sido un referente en la región e incluso a nivel internacional, con tan solo cuatro años de trabajo desde que se lanzó la Estrategia Digital Nacional; dichos logros han sido posible por el trabajo colaborativo, a una visión estratégica y un equipo multidisciplinario, con la colaboración de organismos internacionales, de instituciones académicas, de la sociedad civil y del sector privado.

G. *Datos abiertos de la* UNAM

La finalidad del sitio *www.datos.unam.mx* es integrar y publicar como datos abiertos las colecciones universitarias digitales, a efecto de optimizar su uso para generar nuevo conocimiento y que la investigación de la UNAM tenga un mayor impacto para el análisis y solución de los principales problemas de nuestro país.

La UNAM publica como datos abiertos aquellos que provienen de las colecciones universitarias, las cuales concentran y generan un vasto acervo de informa-

ción científica, artística y cultural. Al difundirla bajo este esquema, el conocimiento acumulado incrementa sus posibilidades de utilización por nuevos usuarios para generar nuevo conocimiento. De esta manera, la UNAM retribuye y beneficia a los distintos sectores de la sociedad con la difusión del conocimiento y la investigación multidisciplinaria[310].

H. *Colaboración con Banco Mundial y Alianza para las Contrataciones Abiertas para implementar el Estándar de Datos de Contrataciones Abiertas en México*

Esta Alianza está conformada por representantes gubernamentales, sociedad civil, particulares, la cual busca colaborar para la implementación efectiva de datos de contrataciones abiertas; este modelo busca fomentar la integridad de gobierno y aumentar la trasparencia en las compras públicas del país.

Este grupo está conformado por el Gobierno de la República, INAI, Transparencia Mexicana, la Alianza para las Contrataciones Abiertas y el Banco Mundial, todos colaborando en el ciclo de contratación:

- Planeación;
- Concurso;
- Adjudicación;
- Contratación; e
- Implementación.

Un claro ejemplo lo podemos encontrar en el Nuevo Aeropuerto de la Ciudad de México (NAICM)[311]; aquí se implementó el estándar en la red compartida, haciendo de esta la primera asociación público-privada en el mundo por adoptar este modelo.

Adicionalmente México cuenta con un sitio de visualización de contrataciones abiertas a disposición de todos los ciudadanos, buscando llevar la transparencia a un mejor nivel.

---

[310] Véase el sitio de datos abiertos de la UNAM, disponible en: *https://datosabiertos.unam.mx/*.
[311] Datos del nuevo aeropuerto de la CDMX, disponible en: *https://datos.gob.mx/nuevoaeropuerto/*.

IV. CONSIDERACIONES FINALES

Los datos abiertos son un recurso muy valioso para la toma de decisiones del sector público, privado y social. Con datos abiertos podemos desarrollar innovación y detonar nuevos modelos de negocio, atender mejor a la población a partir de mejorar la gestión administrativa.

Los datos abiertos representan un componente de la revolución industrial, en conjunto con los dispositivos y hardware y software, debemos mantener el enfoque de derechos humanos en todo proyecto de datos abiertos en los que esté vinculada la información de las personas, y los datos abiertos o conjuntos de datos. En lo posible se recomienda agotar las medidas de seguridad de la información y la disociación de los datos para evitar la identificación de las personas.

El ecosistema digital y la gobernanza son fundamental para el éxito de los datos abiertos, ya sea en el sector público (datos abiertos gubernamentales) o datos abiertos en el sector privado; se requiere la colaboración para que:

a) Internet es el escenario principal sobre el cual hoy día se tratan los datos, por ello debemos protegerlo y contribuir a que siga siendo un motor para la innovación y una Red de redes que permita un trabajo colaborativo y horizontal;
b) La participación de los diferentes actores es sustancial ya que el diálogo y la participación de diversos sujetos y diferentes disciplinas permitirá que la oferta y la demanda se complementen y la generación de datos por parte del sector público esté acorde a la demanda;
c) El marco institucional y jurídico sobre el cual se desarrolla el ecosistema digital y la política de datos abiertos es también de suma importancia, pues se requiere mantener una constancia en la coordinación y seguimiento de las acciones de generación, publicación y mejora continua en materia de datos abiertos;
d) El fomento de los datos abiertos y el gobierno abierto, sobre un enfoque de derechos humanos, permitirá a las sociedades reforzar los valores democráticos y aspirar a una sociedad más informada, más crítica y

comprometida con los asuntos públicos. Los datos abiertos contribuyen de manera importante a la ciudadanía digital y la consolidación de una sociedad más transparente, más innovadora y próspera;

e) La revolución de los datos requiere desarrollar un enfoque multidisciplinario, en que varios profesionales cuenten con habilidades para comprender mejor y así aplicar la interpretación de los datos. Aunado a ello, se debe mantener presente el enfoque de derechos humanos en el desarrollo de tecnología, de la programación, de la interpretación y de la aplicación de los datos en la toma de decisiones.

V. FUENTES DE INFORMACIÓN

BERNERS-LEE, Tim, *Las cinco estrellas en datos abiertos*, Aragón Open Data, *http://opendata.aragon.es/portal/campus/static/html/2_las_5_estrellas_en_datos_abiertos.html.*

CARRILLO D'HERRERA, Juan Carlos, "Ley Federal de Datos Personales en Posesión de los Particulares", *Revista Seguridad*, México, número 10, mayo de 2011, *https://revista.seguridad.unam.mx/numero-10/ley-federal-de-protecci%C3%B3n-de-datos-personales-en-posesi%C3%B3n-de-particulares.*

Cumbre Mundial sobre la Sociedad de la Información, UNESCO, *http://www.unesco.org/new/es/communication-and-information/resources/multimedia/photo-galleries/world-summit-on-the-information-society-wsis/*.

Datos abiertos, México Digital, *https://www.gob.mx/mexicodigital/articulos/datos-abiertos-95287*.

Datos abiertos, Open Data Handbook, *http://opendatahandbook.org/guide/es/what-is-open-data/*.

Decreto por el cual se establece la regulación en materia de Datos Abiertos, *http://www.dof.gob.mx/nota_detalle.php?codigo=5382838&fecha=20/02/2015.*

El Ecosistema de Internet, Internet Society, *http://www.Internetsociety.org/sites/default/files/El_Ecosistema_de_Internet.pdf.*

Esquema del Plan de Desarrollo 2013-2018, *http://itcampeche.edu.mx/wp-content/uploads/2016/06/Plan-Nacional-de-Desarrollo-PND-2013-2018-PDF.pdf.*

Foro de Gobernanza en Internet, Cumbre Mundial de la Sociedad de la Información y del Conocimiento, *http://www.unesco.org/new/es/communication-and-information/resources/multimedia/photo-galleries/world-summit-on-the-information-society-wsis/*.

KUMMER, Marcus, *La gobernanza en Internet: Vayamos al grano,* Unión Internacional de Telecomunicaciones, *http://www.itu.int/itunews/manager/display.asp?lang=es&year=2004&issue=06&ipage=governance.*

KURBALIJA, Jovan, *Gobernanza en Internet: Asuntos, actores y brechas*, *https://www.diplomacy.edu/sites/default/files/IG-Spanish-1st.pdf*.

LEINER, Barry M., *Breve historia de Internet*. Internet Society, *https://www.Internetsociety.org/es/breve-historia-de-Internet/*.

Lineamientos para políticas de datos abiertos, SunLigth Foundation, *https://sunlightfoundation.com/opendataguidelines/es/*.

Los datos abiertos de México, Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico, *https://datos.gob.mx/*.

Nuestro Futuro Común, Comisión Mundial sobre el Medio Ambiente y el Desarrollo-Asamblea General de las Naciones Unidas, *http://www.un.org/es/ga/president/65/issues/sustdev.shtml*.

OBAMA, Barack, *Decreto Ejecutivo 13642: Haciendo el nuevo valor predeterminado de la información gubernamental de información abierta y legible, https://www.data.gov/*.

OSTROM, Elinor, *Gobernanza de recursos comunes*, Conferencia Magistral UNAM, *http://www.dgcs.unam.mx/boletin/bdboletin/2012_295.html.*

PÉREZ DAMASCO, Diego, *Datos, dateros y debates: Panorama de organizaciones e iniciativas de datos abiertos y periodismo de datos en América Latina*, *https://distintaslatitudes.net/wp-content/uploads/2018/01/Datos_Ebook.pdf.*

Política de datos abiertos, México Digital, *https://www.gob.mx/mexicodigital/articulos/politica-de-datos-abiertos?idiom=es*.

Programa para un gobierno cercano y moderno, Secretaría de la Función Pública, *https://www.gob.mx/sfp/acciones-y-programas/programa-para-un-gobierno-cercano-y-moderno-pgcm*.

"Significado de 'Gobernar'", *Diccionario de la Real Academia Española*, *http://dle.rae.es/?id=JHWWluC*.

"Significado de 'Gobierno'", *Diccionario de la Real Academia Española*, *http://dle.rae.es/?id=JHSRe0Y*.

Todo sobre los datos abiertos, OpenDataSoft, *https://www.opendatasoft.es/2017/01/04/todo-sobres-datos-abiertos/*.

TFJA

TRIBUNAL FEDERAL
DE JUSTICIA ADMINISTRATIVA