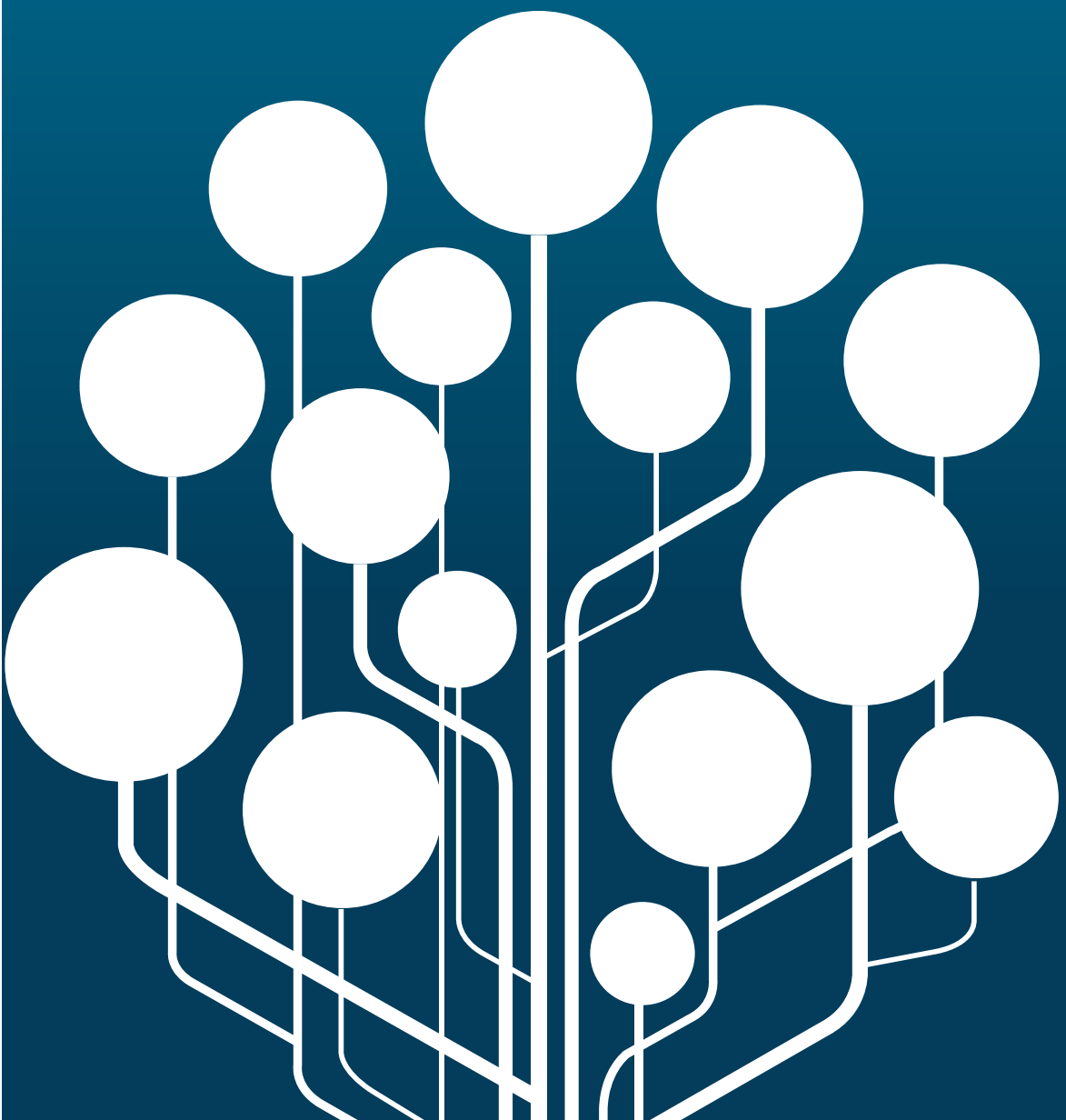
Gobierno abierto y privacidad: la problemática del Big data y el cómputo en la nube



Gobierno abierto y privacidad: la problemática del Big data y el cómputo en la nube

Dra. Wilma Arellano Toledo[1]

Gobierno electrónico y gobierno abierto son dos acepciones o fenómenos que se tornan cada vez más necesarios —y por tanto, van en ascenso— en las actuales sociedades en donde la información y las TIC tienen un papel central. El primero de ellos viene tomando forma desde hace décadas en diversos países yen el caso concreto de México en la última década. El segundo, de igual manera ha surgido y evolucionado en otras latitudes antes que en nuestro país, pero el presente gobierno le ha puesto especial atención y ha creado estrategias para su desarrollo e, incluso, copreside la Alianza para el Gobierno Abierto.

1 Este artículo fue realizado en el marco del proyecto *Régimen jurídico constitucional del Gobierno 2.0- Open government. Participación y transparencia electrónicas y uso de las redes sociales por los poderes públicos,* en donde la autora participa como investigadora internacional en el proyecto, cuyo Investigador Principal es el Dr. Lorenzo Cotino Hueso. Es financiado por el Ministerio de Economía y Competitividad de España mediante el Subprograma de Proyectos de Investigación Fundamental para el periodo 2013-2015. Referencia: DER2012-37844.

Todo esto, que es sin duda relevante para el impulso y perfeccionamiento de las relaciones entre gobernantes y gobernados, puede no obstante incidir en derechos fundamentales de estos últimos de manera positiva —por ejemplo, en relación con el derecho a la información—, pero también negativa —posibles vulneraciones al derecho a la privacidad—. Fenómenos recientes y que van de la mano del desarrollo tecnológico, tales como el Big Data y el Cómputo en la Nube (o *Cloud Computing*) acentúan la complejidad de esta dualidad, pero también aportan novedosos y útiles elementos al crecimiento y progreso del E-gov y el Open-Gov.

PALABRAS CLAVE: Gobierno abierto, privacidad, derecho a la información, cómputo en la nube, Big Data

Introducción

Los derechos a la privacidad y a la protección de datos personales están garantizados en distintos ordenamientos nacionales e internacionales, pero estos han ido evolucionando con la aparición de múltiples servicios y aplicaciones que traen consigo las Tecnologías de la Información y la Comunicación (TIC). Es por ello que en el caso de México, si bien en la Constitución existe un derecho fundamental a la protección de datos personales y, derivado de ello, se aprobó una Ley en la materia que aplica solamente al sector privado (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, LFPDPPP),aún hay muchos vacíos que se deben cubrir. Uno de ellos, muy importante, es el que tiene relación directa con dichas tecnologías, pero también con las obligaciones de los entes de las Administraciones Públicas (AAPP) en el manejo de la información personal de los ciudadanos.

Lo anterior se explica porque, a diferencia de lo que acontece en España en donde su Ley Orgánica de Protección de Datos (LOPD) es aplicable a los ficheros de titularidad pública y a los de titularidad privada, en nuestro caso la ley en la materia no establece obligaciones para el gobierno. Es en la Ley de Transparencia en donde aparece un apartado sobre privacidad. Entendiendo ese derecho como un límite al acceso a la información en poder de los sujetos obligados (entes públicos), es decir, como parte del régimen de excepciones y con exigencias muy exiguas en cuanto a medidas de seguridad y protección, a diferencia de las que se aplican al sector privado, en donde además el régimen de sanciones es sumamente riguroso.

En México se aprobó una reforma constitucional en materia de Telecomunicaciones, Radiodifusión y Competencia Económicay, en consecuencia, una nueva Ley de Telecomunicaciones y Radiodifusión que desarrolla lo dispuesto en aquella y que incluye algunos elementos sobre privacidad y protección de datos personales, pero que siguen siendo insuficientes. Es por ello y, en consonancia con lo anteriormente expuesto, que uno de los desafíos pendientes es que se modifique la LFPDPPP, para añadir supuestos concretos de las telecomunicaciones, como la geolocalización, las etiquetas RFID —que tienen estrecha relación con el denominado Internet de las cosas— o las aplicaciones móviles.

Asimismo, una vez reformado recientemente el marco sobre transparencia y acceso a la información, que da paso a una nueva era de su garantía en México y conectado con la Estrategia Digital Nacional —que incluye una política de datos abiertos u *Open Government*, en donde el Big Data tiene un papel central—, el respeto a la privacidad de las personas debe ser plenamente garantizado. Finalmente, es necesario considerar el rol que tiene el denominado cómputo en la nube o *cloud computing*, que se ha convertido en un desafío para la protección de los datos personales y la privacidad de los usuarios. Sin embargo, al ofrecer diversas ventajas a los sectores empresarial, gubernamental y social, es pertinente que se fomente su uso, pero siempre con un sentido de protección de los derechos fundamentales que pueden verse afectados.

Los artículos 6º, 7º y 16º de la Constitución Mexicana: derechos a la información, al acceso, a Internet y a la protección de datos

Es fundamental considerar que en los tiempos actuales, muchos países han puesto en marcha políticas y han consolidado marcos jurídicos para incentivar el uso de la tecnología en aras del desarrollo de un auténtico Estado de Derecho y en el ámbito de la participación y transparencia de un país, sin descuidar la esfera de la intimidad de los individuos. México no puede quedarse a la zaga de la tendencia mundial en la conformación de un sistema y de una normativa moderna, eficiente y que integre todos los factores esenciales para garantizar una auténtica democracia.

Con el uso de las TIC, entre las que destacan la telefonía móvil y otros sistemas, redes y servicios asociados a las telecomunicaciones, se puede potenciar el ejercicio de derechos de participación y transparencia, pero los riesgos que se corren, tanto de seguridad como de una posible vigilancia por parte de las autoridades, también son muchos. Sobre todo teniendo en cuenta la utilización de etiquetas RFID y las aplicaciones de geolocalización que muchos teléfonos inteligentes tienen.

Asimismo, la aparición de una Cédula de Identidad Ciudadana en México incluirá más datos personales y su tratamiento deberá ser más cuidadoso y delicado. La razón principal es que esa cédula contará con la identidad biométrica de cada mexicano. Si bien esto puede traer consigo muchas ventajas, porque se evita que se entreguen distintas identificaciones en diferentes instancias, también puede conllevar riesgos que es necesario evitar con una adecuada regulación de protección de datos personales en general, para todas las empresas públicas y privadas pero, en especial, para las instituciones y autoridades electorales encargadas del manejo de esa información.

Dicha cédula ha sido implementada en otros países en forma de Documento Nacional de Identidad o DNI en versión electrónica. Las medidas de seguridad son múltiples para proteger a todos los actores involucrados y ese debe ser el caso en este país, en donde de inicio puede utilizarse la Firma Electrónica Avanzada (o FIEL) que ahora sólo se aplica con fines fiscales (SAT) y financieros (Banxico).Ahora bien, como adelantamos en la introducción, la protección de datos personales aparece en la legislación mexicana, primeramente, como parte del régimen de excepciones de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) de 2002. Esto es, se manifiesta como uno de los límites del derecho de acceso de los ciudadanos a la información que poseen las entidades de la Administración.

Posteriormente, el derecho fundamental a la protección de datos de carácter personal se reconoce en la Constitución mexicana, a través de su artículo 16º, y se crea la ley que lo desarrolla y que, como mencionamos antes, sólo aplica al sector privado. En este ordenamiento, la garantía de protección a la información personal reaparece con otro cariz, de manera que son los entes privados los que están obligados a respetar ciertos principios en cuanto al tratamiento y, sobre todo, a obtener el consentimiento de los titulares para ese objetivo.

Por tanto, las dos manifestaciones de este derecho —ligado notablemente al de la intimidad, pero perfectamente distinguible del mismo—, suponen retos y desafíos que, aunados a la evolución acelerada de las TIC y el tránsito de muchos países a la denominada Sociedad de la Información y el Conocimiento (SIC), implican una problemática que adquiere un sentido más complejo, para lo cual hay distintas respuestas. Una de las que sobresalen es la adopción de códigos éticos y otras medidas de autorregulación, formando parte de un esquema que, complementando las disposiciones del Derecho positivo, podría constituirse como heterorregulación.

Como se esbozó anteriormente, otro derecho que ya es fundamental en México tras la reforma del artículo 6º constitucional es el del acceso a la información pública gubernamental, relacionado estrechamente con la transparencia y la rendición de cuentas. Aparece primero una legislación que lo desarrolla, a partir de una sola afirmación que se había incluido en la Ley fundamental desde 1977: "el derecho a la información será garantizado por el Estado". Con fundamento en ello, en 2003 se publica la Ley de Transparencia, su Reglamento y se crea el Instituto Federal de Acceso a la Información (IFAI)[2].

Posteriormente, en 2007 se reforma la Constitución mexicana para incluir el derecho de acceso a la información con mayor amplitud. Recientemente, como parte de la Reforma Constitucional en materia de Telecomunicaciones, Radiodifusión y Competencia Económica, se modifica nuevamente en abril de 2013 la Norma fundamental para que sean protegidos derechos conexos a la información y queda así:

> Artículo 6º. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el

2 El IFAI es el órgano regulador en materia de derecho de acceso a la información y, después de la aparición de la LFPDPPP, también en materia de protección de datos personales en posesión de particulares. La LFTAIPG lo define como: "un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho a la información, resolver sobre la negativa a las solicitudes de acceso a la información y proteger los Apor 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 38º) (las negritas son nuestras).

derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.

El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios...

A. Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. La información que se refiere a la 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 utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de estos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

Como puede observarse, se garantiza el derecho de acceso y —ligado a éste, diferenciado de él, pero como una dimensión distinta a la que veremos después—aparece el de protección de datos personales. Asimismo, se menciona un derecho a la información y un derecho de acceso a las tecnologías de la información y a la banda ancha; los cuales analizaremos por separado en lo sucesivo.

El derecho de acceso a la información pública se garantizaconsiderando las facultades que tienen los distintos niveles de la Administración pública —y los denominados OSO's[3] — y con sujeción a los criterios establecidos por las normas correspondientes. De ese modo, la información en poder de las autoridades es pública y sólo podrá reservarse por fines que tengan que ver con la seguridad o el interés público y según lo dicten las leyes correspondientes[4]. Sin embargo, como bien se indica, en la interpretación de estos casos debe predominar el interés de máxima publicidad.

En la otra parte del artículo se garantiza un derecho de acceso a la información personal que conste en archivos públicos y se determina la gratuidad en este trámite, aun cuando no se establecen otros elementos de los derechos ARCO[5] que sí se contemplan en relación a los datos de carácter personal en poder de los particulares, como ya veremos después. Asimismo, es importante la mención de este literal con respecto a garantizar la libertad de expresión, toda vez que en ocasiones, su ejercicio supone que se enfrente al de la intimidad e, incluso, puede tener lugar una colisión de ambos.

3 Se refiere la norma a los otros Otros Sujetos Obligados que surgen cuando "se determinó ampliar su ámbito de aplicación (el de la Ley de Transparencia) no sólo a la administración pública federal, sino también a los Poderes Legislativo, Judicial, los organismos constitucionales autónomos, los tribunales administrativos federales y cualquier otro órgano federal" (López y Arellano, 2008, p. 8).

4 De acuerdo con la Ley de Transparencia, artículo 13º, se considera información reservada y confidencial, aquella que pueda comprometer la seguridad y defensa nacionales y/o la seguridad pública, o que pueda "menoscabar la conducción en las negociaciones o bien, las relaciones internacionales", o dañar la estabilidad monetaria de México, poner en riesgo la vida o seguridad de cualquier persona y/ o causar prejuicio a las actividades de verificación de cumplimiento de las normas. Asimismo, entran en la categoría de reservadas, las informaciones que lo sean previamente por disposición oficial, el secreto industrial, comercial, bancario, etcétera; las averiguaciones previas, los expedientes judiciales y los procedimientos de responsabilidad de los servidores públicos (artículo 14).

5 Derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos personales, para ser ejercido por su titular ante particulares, ya que no se mencionan todos estos elementos en el ámbito de las bases de datos en poder de la Administración o ficheros de titularidad pública, como se les conoce en España a través de la LOPD.

En lo que respecta al derecho a la información que "será garantizado por el Estado", como se establece en el mencionado artículo, hay que decir que esta frase aparece en el apartado constitucional desde el 6 de diciembre 1977, ya que en aquel momento se vio la necesidad de legislar un derecho que, por el contexto político del país, se hacía evidente en su importancia y dimensiones. En el Plan Básico de Gobierno 1976-1982 se estipulaba que "el Derecho a la Información constituye una nueva dimensión de la democracia: es la fórmula eficaz para respetar el pluralismo ideológico, esto es, la diversidad y riqueza en la expresión de ideas, opiniones y convicciones" (López, 1978, p. 74).

Con respecto a la polémica inclusión[6] del derecho de acceso a las TIC, incluido Internet de banda ancha, por un lado está la situación en que se coloca a este derecho en el ámbito constitucional y lo avanzado de esta disposición en el plano internacional[7] y, por el otro, la preocupación de que el Estado verdaderamente garantice ese derecho y el mismo no quede en letra muerta. Para esto, será necesario dotarlo de un auténtico contenido con fundamento en el servicio universal de telecomunicaciones[8] reconocido en otros países.

Por otro lado, el artículo 7º guarda igualmente relación con el tema que nos ocupa, puesto que dispone que "es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. No se puede restringir este derecho por vías o medios indirectos…" (las negritas son nuestras). La redacción actual de este literal constitucional es un gran avance, puesto que también, como resultado de la reforma de 2013, se establece que la libertad de expresión debe ser garantizada por todos los medios, incluyendo los electrónicos y de telecomunicaciones. El artículo había sido escrito en la Constitución original (1917), con lo que, añejo y obsoleto, sólo se refería a la libertad de expresión a través de medios impresos.

Teniendo en consideración que la libertad de expresión —que en la forma de 1917 era una estricta libertad de imprenta, pero que se amplía con la mención de los nuevos medios— es una de las aristas del derecho a la información e incluso lo complementa en un fortalecimiento de la facultad de divulgar o difundir información, su mención

6 Algunos sectores de la doctrina opinaron, en el contexto de los debates sobre la Reforma Constitucional en Materia de Telecomunicaciones que ese derecho de acceso a las TIC no debería aparecer en la Constitución.

7 Pocos textos constitucionales incluyen esta disposición, ya que los países que lo han reflejado, lo han hecho en sus legislaciones de telecomunicaciones. Un ejemplo de ello es Finlandia, ya que en julio de 2010 se aprobó su nueva Ley de Mercado de las Comunicaciones y se garantizó el acceso a Internet de banda ancha en su seno.

8 Una definición que puede ser muy útil es la siguiente: "El servicio universal de telecomunicaciones debe tener un contenido mínimo, compuesto por tres elementos esenciales: acceso, calidad y precio. Esto es, acceso a los servicios de telecomunicaciones (originalmente sólo se trataba de acceso telefónico, pero con el paso del tiempo se han incluido el acceso a Internet, a otros servicios avanzados y otras prerrogativas), con una calidad mínima que permita un consumo adecuado y pertinente, con la característica de la asequibilidad. No es muy funcional un acceso que es caro o que no tiene la calidad suficiente para que realmente, con el uso de las telecomunicaciones y las TIC, se vaya minimizando la brecha digital" (Arellano, 2012).

en este trabajo era de evidente interés. En especial porque la libertad de expresión es fundamental, ya que "es una de las condiciones esenciales de cualquier régimen democrático; en otras palabras, la libertad de expresión es condición necesaria —aunque no suficiente, desde luego— para que se pueda considerar que en un determinado país hay democracia" (Carbonell, 2011, p. 367).

La relación entre dicho derecho y libertad es visto de la siguiente manera por López Ayllón (2009, p. 13): "el derecho a la información —contenido en la libertad de expresión— es la garantía que tienen las personas de conocer de manera activa —es decir, investigando— o activa —recibiendo—, las ideas, opiniones, hechos o datos que se producen en la sociedad" con lo que pueden conformar una opinión y así participar, entre otras cosas, de la vida democrática de su país". En este sentido, la libertad de expresión encuentra una liga perfecta con el régimen democrático en su conjunto, con el recién mencionado derecho a la información y con la transparencia —vinculada al derecho de acceso, pero no como sinónimo—.

La transparencia aparece más en la lógica de la rendición de cuentas[9], aunque no son lo mismo, lo cual se explica mejor de la siguiente manera: la rendición de cuentas no se limita "a la comunicación de información contable de un agente a un principal", sino que va más allá y se constituye como un "proceso dinámico" que revoluciona y perfecciona las relaciones entre el Estado y la sociedad "reconfigurando así la naturaleza misma de la democracia y la participación ciudadana" (Ackerman, 2008, p. 18). Por su parte, la transparencia supone una acción de apertura y de limpieza, de no poner velos a la actuación gubernamental, lo contrario a la opacidad. Mejor definida en la Ley de Transparencia, en su artículo 4º, como: la "acción de transparentar la gestión pública mediante la difusión de información que generan los sujetos obligados". En todo caso, los tres conceptos —derecho de acceso, transparencia y rendición— están relacionados y se impactan recíprocamente entre ellos[10].

Por otra parte, y aún analizando el texto constitucional mexicano, aparece el derecho a la protección de datos personales, considerado completamente autónomo por la

9 Para clarificar este término, podemos apoyarnos en Carbajal (2011, p. 5), cuando apunta que a la rendición de cuentas se le puede definir como: "'la obligación permanente de los mandatarios o agentes para informar a sus mandantes o principales de los actos que llevan a cabo como resultado de una delegación de autoridad que se realiza mediante un contrato formal o informal y que implica sanciones en caso de incumplimiento'. Su origen próximo proviene del inglésaccountability, un término que no posee un equivalente en español, al menos en forma precisa, ya que suele traducirse como control o como fiscalización y, en ocasiones, como responsabilidad. Para este caso, la interpretación más idónea es rendición de cuentas. La distinción lamentable es que el término accountabilityposee un carácter obligatorio, mientras que la rendición de cuentas parece tener un tinte voluntario".

10 En este sentido, Carbajal (2011) apunta que "es importante no equiparar el término en cuestión [el de transparencia] con 'derecho de acceso a la información' o 'rendición de cuentas', pues el primero de estos es un instrumento de la transparencia, mientras que la última es un instrumento de un sistema de rendición de cuentas. Ahora bien, la transparencia no es sólo el publicar documentos y datos, sino que implica una información clara, veraz, congruente, accesible, comprensiva, relevante y confiable".

doctrina del de la intimidad o el de la privacidad —según el país de que se trate— y que ha sido reconocido en la mayoría de los países del mundo;México, aunque de manera tardía, no ha sido la excepción. La diferencia entre el derecho a la protección de datos personales en México con respecto a otros países, como España por ejemplo, es que está delimitado de manera concreta y, sin embargo, no se hace alusión en el texto fundamental al derecho a la intimidad. En el artículo 16º de la Constitución mexicana se acercan, sin embargo, dos elementos que tienen relación con éste pero que, como decimos, son independientes. Así, ese artículo dispone que:

> Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
>
> 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.

Es evidente que el contexto de este artículo que luego hace alusión a la garantía de un debido proceso y a las condiciones de las órdenes de aprehensión, no era el más idóneo. Sin embargo, quedan establecidos dos elementos de protección a la privacidad de las personas: la inviolabilidad del domicilio y el reconocido específicamente derecho a la protección de datos personales, con las consecuentes posibilidades de ejercicio de los derechos ARCO: acceso, rectificación, cancelación y oposición.Aun cuando el derecho a la protección de datos personales aparece esbozado en el contexto de un derecho de acceso a la información pública y que este artículo 16º aparece para dar paso a la LFPDPPP, puede interpretarse, sin problema alguno, que lo establecido es aplicable a todos los ámbitos, tanto el público como privado, ya que el contenido del mismo no hace ninguna restricción al respecto.

Es importante mencionar, ya que estamos hablando de transparencia y derecho de acceso a la información, del artículo 7º constitucional que versa sobre la libertad de expresión, ya que se liga con lo anterior formando parte de un derecho a la información en términos más amplios, como los establecidos por la Declaración Universal de los Derechos Humanos de 1948, en cuyo literal 19 se contemplan las facultades de recibir, de difundir y de investigar información. Aunque, claro está, se refiere a toda la información, no solamente a la que tienen en su poder las autoridades de un país.

Transparencia, estado de Derecho y gobierno abierto

El estado de Derecho ha sido definido primariamente como aquel en donde no hay caos y la sociedad obedece a sus gobernantes y se cumple lo que dice la norma. Sin embargo, hoy en día, de acuerdo con algunos sectores de la doctrina, debemos aspirar a un Estado Democrático de Derecho que "defiende y fomenta los derechos de los ciudadanos a la información, la participación y la justicia social" (Ackerman, 2008, p. 19).Esto es, debe migrarse del concepto centrado en la cultura de la obediencia y de la legalidad a uno más maduro y concientizado de que existen las TIC que potencian la participación ciudadana y también el control hacia y desde sus gobernantes. Sin embargo, esa esfera de cumplimiento en donde los derechos y libertades que tratamos en la primera parte desempeñan un rol central, no debe traspasar los límites con respecto a los derechos fundamentales de los gobernados y, muy especialmente el que nos ocupa, el de la privacidad.

Coherente con lo que apuntamos antes, un Estado Democrático de Derecho sobrepasa al Estado represor y controlador que, por cierto, se puede ver fortalecido con el uso de las TIC. Va más allá: permitiendo también fomentar y potenciar los derechos y libertades. En resumen:

> Los avances de la tecnología aunada a las demandas de una sociedad cada vez menos tolerante y pasiva ante la opacidad de las instituciones gubernamentales y sus representantes, exigen transparencia por parte de estos, sobre todo concretizado en una real y objetiva rendición de cuentas con el fin de lograr cada vez más una consolidación del Estado de Derecho (Carbajal, 2011, p. 1).

La idea central que queremos destacar es que sólo mediante el respeto a un Estado de Derecho —en el sentido conceptual moderno del término— puede darse una auténtica transparencia y el gobierno conseguirá estar "abierto", en el sentido también más moderno del término.Así, tenemos que muchos países han ido implementando políticas de Open Gov que intentan responder a las nuevas exigencias de una sociedad cada vez más conectada y que utilizan las TIC para hacer valer sus derechos —no sólo los que enlistamos antes, sino todos aquellos que se potencian con el uso de la tecnología, como los relacionados con la participación política y ciudadana y que se enlazan, asimismo, con la concepción primaria del derecho a la información—.

En el caso de México, con la Presidencia de Enrique Peña Nieto comenzaron a impulsarse no solamente las reformas constitucionales hasta aquí mencionadas —de Derechos Humanos, de Telecomunicaciones, de Transparencia—, sino también una Estrategia Digital Nacional (EDN)y una Política de Datos Abiertos, consistentes en una

serie de acciones específicas para conseguir los propósitos que persiguen.La EDN es el plan de acción que configuró el gobierno mexicano para potenciar la adopción y uso cada vez más generalizado de las TIC. Su objetivo central es lograr un "México digital". Se compone de cincoobjetivos: Transformación Gubernamental, Economía Digital, Educación de Calidad, Salud Universal y Seguridad Ciudadana. Así como cinco habilitadores: Conectividad, Inclusión y Habilidades Digitales, Interoperabilidad, Marco Jurídico y Datos Abiertos. Varios de ellos tienen relación con el tema que nos ocupa, como puede observarse.

Es por ello que destacaremos el objetivo de Transformación Gubernamental[11] que se define como la "construcción de una nueva relación entre la sociedad y el gobierno, basada en la experiencia de los ciudadanos como usuarios de los servicios públicos" (Presidencia de la República, 2014) y cuyo eje para potenciarla serán las TIC. Asimismo, es de hacer notar el habilitador de Interoperabilidad que pretende que se fomente "la capacidad de los sistemas para intercambiar información del gobierno" y que se refiere tanto al aspecto técnico como semántico y organizacional(Presidencia de la República, 2014); y el habilitador de Datos Abiertos, que es el que más relación tiene con lo que nos ocupa y que potencia diversos derechos fundamentales tratados en la primera parte de este texto. Este habilitador alude al uso de información gubernamental en formatos abiertos que a su vez será "infraestructura base para establecer mecanismos de co-creación de servicios públicos"(Presidencia de la República, 2014).

Por su parte, la estrategia relacionada con el *Open Gov* se presentó a través de un Plan de Acción 2013-2015 de la Alianza para el Gobierno Abierto[12], de la cual México tiene ahora la Co-Presidencia con Indonesia. En ese Plan el Gobierno mexicano asume una serie de compromisos para lograr un "México abierto", centrado en la ciudadanía, con un presupuesto "abierto y participativo" y persiguiendo el empoderamiento de la sociedad y su participación.

11 Los seis objetivos secundarios del de Transformación Gubernamental son: Generar y coordinar acciones orientadas hacia el logro de un gobierno abierto; Instrumentar la Ventanilla Única Nacional para trámites y servicios; Instrumentar una política digital de gestión del territorio nacional; Crear una política de TIC sustentable para la Administración Pública Federal; Usar datos para el desarrollo y mejoramiento de políticas públicas; y Adoptar una comunicación digital centrada en el ciudadano.

12 La Alianza para el Gobierno Abierto está integrada por 60 países, pero fueron ocho los que la fundaron: México, Brasil, Estados Unidos, Filipinas, Indonesia, Noruega, Reino Unido, Sudáfrica y Tanzania. Su objetivo es "consolidar los esfuerzos realizados en los últimos años en materia de transparencia, acceso a información y combate a la corrupción por medio de la suscripción de iniciativas e instrumentos internacionales" (Presidencia de la República, 2014).

El Big data como herramienta para el Open Gov y el desafío a la privacidad

Visto lo anterior, tenemos que las TIC han fomentado procesos en los que se entretejen el ejercicio más efectivo de distintos derechos fundamentales y apuntando a la consolidación de las democracias, pero con la debida protección de los mismos para que no sean trasgredidos.En este tenor, uno de los fenómenos que ha contribuido a las políticas no sólo de *Open Gov*, sino de muchas otras cuestiones vinculadas con TIC y su acelerado desarrollo, es el conocido como *Big Data*.

En junio de 2014 se celebró en Infotec el Seminario Internacional *Big Data* para la información oficial y la toma de decisiones, en donde se persiguió el objetivo de reconocer los desafíos jurídicos, políticos y técnicos de este fenómeno. Así, se reconoció que"la generación y disponibilidad de información digital, así como el uso masivo de dispositivos electrónicos, hacen posible su empleo para generar información oficial, estadística y geográfica. La comunidad estadística ha reconocido el potencial que tiene el *Big Data* para ayudar a generar información actualizada y coherente en temas económicos, sociales y de medio ambiente, que apoyen la toma de decisiones públicas más eficientes. Sin embargo, para extraer su potencial, será necesario contar con la legislación y la regulación adecuadas que permitan la explotación de bases de datos para fines públicos, asegurar la privacidad y seguridad de la información, así como promover e impulsar que se utilicen las metodologías y tecnologías adecuadas, entre otros retos" (INEGI, 2014).

Esta realidad ha implicado distintos retos para el gobierno, la industria y la sociedad, por lo que, en principio, es necesaria una homologación normativa y conceptual en torno a diversos temas y aspectos relacionados con Internet y, por tanto, con *Big Data* y sus herramientas a nivel nacional, ya que existen definiciones disímbolas en las distintas regulaciones.Los derechos a la privacidad e intimidad de las personas —teniendo en cuenta que son derechos fundamentales— deben ser adecuadamente protegidos en el contexto de *Big Data*, aunque sin perder equilibrio con la libertad de expresión y el derecho a la información, toda vez que estos se encuentran en el mismo rango. Un método para proteger datos personales, que además está regulado en México, es la anonimización de la información y la adecuada y sencilla puesta a disposición del Aviso de Privacidad.

Para la actividad del gobierno —en su dimensión de *Open Gov*, pero no sólo en ésta—y para la generación de información oficial, la anonimización y el uso de los datos personales conforme a los principios de proporcionalidad, de calidad y de finalidad, son sumamente importantes y se debe garantizar su observancia también cuando se

use *Big Data* con dicho fin estadístico. No obstante, la protección de la privacidad no debe ser un límite para el aprovechamiento de las oportunidades que brindan "los grandes datos" y debe estar en equilibrio con respecto al denominado *Open Data*. Es decir, existe la necesidad de regular algunos aspectos de *Big Data*, pero sin llegar a una sobrerregulación que obstaculice su potencial y que sea acorde con las políticas nacionales de *e-government*.

En la creación de la normativa que se refiera a *Big Data* es sumamente importante tomar en cuenta el punto de vista técnico y adoptar un enfoque desde la interdisciplina. Asimismo, las estrategias y la regulación de *Big Data* que pretendan llevarse a cabo no deben descuidar la atención a las líneas y políticas de la gobernanza en Internet. Ahora bien, estos enfoques son parte de las reflexiones que poco a poco se van realizando sobre este fenómeno, pero es evidente que aún hay muchos elementos que es necesario discutir y, más aún, cuando volvemos al tema de la privacidad.

En este sentido, son las Declaraciones de las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad (o *Privacy Conferences*) en donde se apunta claramente a los desafíos que presentan las TIC para la intimidad de las personas. En 2011 esa Conferencia (la número 33) se llevó a cabo en México y ahí se expresaba, en su Resolución, que existía preocupación[13] por parte de las autoridades internacionales en la materia en esos temas y es por lo que esa Conferencia adoptó una resolución sobre coordinación internacional para la aplicación de medidas protectoras de la privacidad (*Resolution on Privacy Enforcement Coordination at the International Level*), basada en los fundamentos de la Iniciativa de Londres, así como en la Directiva Europea de Protección de Datos y los Acuerdos Asia-Pacífico de Cooperación entre Autoridades de Protección de Datos.

Lo anterior responde a la necesidad de cooperación internacional en estos asuntos, ya que las modernas tecnologías, la globalización y la incursión en la Sociedad de la Información de varios países, ha difuminado en muchos casos las fronteras nacionales con respecto a la vulneración de los derechos fundamentales con las TIC. Es por ello que, como sucede en asuntos de cibercrimen o delitos informáticos, es necesario llegar a acuerdos transnacionales en materia de e-privacidad.

Además de dicha cooperación, en la Resolución de la Ciudad de México que estamos comentando, se dispuso tomar medidas en relación precisamente sobre fenómenos tales como el *Big Data*—al que definía como las "nuevas formas de almacenamiento de información en bases de datos de gran dimensión que posibilitan el rastreo y

13 De hecho, en los Considerandos se expone que "el creciente alcance global de las tecnologías de la información, tales como la Internet y la telefonía móvil, constituyen un reto y una oportunidad para conformar una comunidad capaz de hacerles frente mediante la elaboración de normas, estándares y metodologías con alcances semejantes al de aquéllas y no obstante las diferencias culturales, la diversidad de actores interesados y sin reparar en los enfoques locales o regionales que se adoptan respecto a la privacidad".

supervisión"— y el cómputo en la nube —o *cloud computing*, que plantea nuevos retos para la protección de la intimidad—, entre otros.

Al año siguiente, en octubre de 2012, en la ciudad de Punta del Este, tuvo lugar la 34° Conferencia Internacional. En su seno aparecen tres documentos muy importantes en relación con el tema que nos ocupa. Se trata de una Resolución sobre Cómputo en la Nube —tema que abordaremos en breve—, en donde se planteó que dicha tecnología está en desarrollo y falta transparencia en su uso; por lo cual las Autoridades de Protección de Datos se comprometieron a impulsar la gobernanza en este asunto, una Resolución sobre el Futuro de la Privacidad —en donde se comprometen a intensificar la cooperación en materia de flujos transfronterizos de información: "la tecnología ha hecho mucho más fácil la transmisión e intercambio de datos a través de las fronteras" y, también, en donde reconocen el impacto del uso de Internet combinado con el de dispositivos móviles— y la Declaración de Uruguay —en donde se reconoce la importancia del *Big Data* para los objetivos de los sistemas sanitarios, la eficiencia energética o la seguridad pública, pero también sus notables riesgos para la privacidad, sobre todo si los datos se utilizan para la elaboración de perfiles, cuyos algoritmos subyacentes requerirán validación continua—.

Finalmente, en la última Conferencia que se ha celebrado, la 36°, se firmaron siete documentos: Declaración de Varsovia sobre la *appificación* de la sociedad, Resolución sobre *Profiling*, Resolución en materia de *Enforcement*, Resolución sobre protección en encaje de datos y protección de la intimidad en el derecho internacional, Resolución sobre la transparencia en las prácticas en relación con datos personales, Resolución sobre educación digital para todos y Resolución sobre seguimiento web (*web tracking*) y privacidad. Como puede verse, cada vez son más los campos de acción en los que tienen que intervenir las autoridades que participan en la Conferencia, toda vez que los desafíos son cada vez mayores.

En la primera resolución acerca de las aplicaciones móviles, se reconoce la importancia de las mismas —suman ya 6 millones a nivel público y privado— y su potencial como posibles agentes vulneradores de la privacidad, ya que se utilizan en los teléfonos celulares, las tabletas y los coches, entre otros dispositivos. Se alerta así sobre las responsabilidades que tanto usuarios como fabricantes, tienen en relación a este asunto:

> Los creadores de aplicaciones no son conscientes de las implicaciones de privacidad de su trabajo y no están familiarizados con conceptos como la privacidad por diseño y por defecto. Los principales sistemas operativos y plataformas, ofrecen algunas opciones de privacidad, pero no permiten el control total por parte de los usuarios, de proteger sus datos personales y verificar qué información se recopila y con qué propósito.

Teniendo en cuenta los distintos actores que intervienen en esta dinámica, la Resolución considera que los usuarios deben poder tener más control sobre su información personal y sobre cómo utilizarla (autodeterminación informativa), los desarrolladores de aplicaciones deben partir desde la creación de las mismas que existe una normativa que les obliga a proteger la privacidad de los clientes y que no debe recogerse información de estos sin su consentimiento —teniendo en cuenta que esto, además, es una ventaja competitiva para las empresas—, los proveedores de sistemas operativos deben proceder con responsabilidad de sus plataformas y las autoridades de protección de datos deben ejercer sus funciones para regular estos asuntos y crear conciencia y cultura social y empresarial al respecto.

La Resolución sobre *Profiling* —creación de perfiles de usuario— se centra en el uso adecuado de sus herramientas, con la responsabilidad que ello implica, así como en el principio de información en materia de protección de datos y el correcto ejercicio de los derechos ARCO: de acceso, rectificación, cancelación y oposición al tratamiento de datos personales. La Resolución sobre *Enforcement* desarrolla y continúa lo que estipulaban anteriores documentos que hemos mencionado en cuanto a la necesaria cooperación internacional para la protección de la privacidad y la posibilidad de persecución del delito y reparación del daño en el ámbito internacional. Todo esto, debido a que las vulneraciones a la intimidad de las personas, en muchos casos, no conocen fronteras y jurisdicción competente.

Por su parte, la Resolución de la Conferencia sobre Educación Digital para todos hace hincapié en temas de reciente preocupación como son: el uso de las TIC por menores de edad —se entiende que estos requieren de una protección especial— y la generalización de un uso apropiado de la tecnología de la información, las telecomunicaciones e Internet por todos los sectores y grupos de la población. Una mayor alfabetización en el uso de los modernos dispositivos y sus aplicaciones y servicios requiere más autoprotección y cuidado de la privacidad por parte de las personas. En resumen, se persigue que las personas adquieran habilidades esenciales en el uso de las TIC, sean "actores informados y responsables en el entorno digital" y ejerzan un uso adecuado de sus derechos, sin olvidar sus deberes en este sentido.

Por último, la Resolución sobre seguimiento web o *web tracking*, que se refiere al rastreo de IP (*Internet Protocol*) y otras técnicas quepueden afectar la privacidadal permitir la creación de perfiles y el seguimiento de usuarios. Sobre todo, porque la recogida de datos está cada vez más combinada, ya que se recopila información sobre el dueño de un dispositivo, así como todo tipo de información referente a su actividad *online*, pero también con respecto a sus transacciones offline. Un ejemplo de ello son las medidas de seguridad adoptadas por los servicios financieros que, si bien persiguen un buen fin como lo es la protección frente a un fraude, pueden ser sumamente violentadores de la

intimidad de las personas, ya que incluyen en su tratamiento datos considerados como sensibles. El documento solicita quetodas las partes interesadas tomen medidas para evitar el mal uso de la información y la optimización de la seguridad y la privacidad en este terreno.

Privacidad, TIC y cómputo en la nube

Una vez definido el marco constitucional del derecho de acceso, del derecho a la información, de la transparencia y de la protección de datos personales, conviene regresar a la aseveración que hicimos en el apartado anterior.Se debe retomar este último derecho y diferenciarlo con el derecho a la privacidad y el derecho a la intimidad, para abordar luego lo que las TIC implican en este ámbito y su relación con la propia transparencia, la rendición de cuentas y el Estado de Derecho.

Así, las diferencias entre intimidad y privacidad se pueden entender de la siguiente forma: "la privacidad, desde la perspectiva *iusinformativa*, es el conjunto de mensajes que, desde un punto de vista negativo, la persona priva (es *privativo*) a una multitud su acceso y conocimiento" (Urzúa, 2012, p. 373). Desde un punto de vista positivo, se trataría del acceso a dichos mensajes a personas específicas que guarden cualquier tipo de lazos con el titular de la información que decide compartirlos con ellos.Por otro lado, la intimidad, de acuerdo también con Desantes, no es comunicable ni se expresa del mismo modo que la privacidad, sino que "radica en el fuero interno de la persona y al comunicarse deja de ser lo que era, porque su característica principal es ser inabarcable, que se traduce en su imposibilidad de formulación expresiva" (Urzúa, 2012, p. 374).

Ahora bien, como se ha escrito ya desde hace tiempo, las TIC pueden potenciar la vulneración de ambas esferas, por lo que la protección en este medio y en el llamado tránsito a la Sociedad de la Información debe ser mucho más amplio, máxime si se toma en cuenta que no todos los servicios asociados a ese mundo tienen las mejores medidas de seguridad y, además, se viven fenómenos como el cómputo en la nube[14]. El también llamado *cloud computing* se ha convertido en un desafío para la protección de los datos personales y la privacidad de los usuarios. Sin embargo, al ofrecer diversas ventajas a los sectores empresarial, gubernamental y social, es pertinente que se fomente su uso, pero siempre con un sentido de protección de los derechos fundamentales que pueden verse afectados.

14 Se entiende por cómputo en la nube o *cloud computing*, al "ecosistema de recursos tecnológicos de la información y la comunicación, que ofrece servicios escalables, compartidos y bajo demanda en diferentes modalidades y diversos usuarios a través de Internet" (Téllez, 2013, p. 5).

Entendido este desafío, vamos a analizar algunos elementos de la legislación mexicana en materia de protección de datos y que mencionan al *cloud*, para tener el referente de cómo el gobierno podría aplicarse también algunas de estas medidas cuando trate información de los ciudadanos. La legislación de protección de datos en México prevé medidas específicas para las empresas que, estando en posesión de información personal de sus usuarios o clientes, utilicen servicios en la nube. El Reglamento de la LFPDPPP integra una sección sobre el cómputo en la nube, además de la serie de medidas técnicas a las que se alude en referencia a una adecuada protección de la información personal por parte de los responsables de su tratamiento.

En primera instancia, la ley habla sobre las transferencias internacionales de datos[15] y, aunque en ese artículo 36º en concreto —que es en donde aborda el tema— no habla del cómputo en la nube, está claro que la misma interviene en dichas transferencias. Evidentemente obliga a que el tercero a quien se transfieran los datos se comprometa a protegerlos y a adoptar medidas de seguridad, en los mismos términos que el responsable[16], es decir, la empresa que los recopiló. Este punto, con toda evidencia, es importante para el tema que nos ocupa.

De este modo, aquel responsable que transfiera los datos debe comunicar el Aviso de Privacidad[17] al receptor de los mismos —un tercero que puede justamente tener servicios en la nube o bien ser incluso el prestador de los mismos a la empresa responsable—; en donde destaca la importancia de que el titular de los datos esté informado de la transferencia y de sus fines. Por su parte, el Reglamento de la Ley Federal de Protección de Datos mexicana sí se refiere específicamente al cómputo en la nube y la filosofía de protección en este terreno se relaciona estrechamente con el principio anterior.

En su artículo 52º define el *cloud* como el "modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente".En el mismo literal, ordena que las empresas sólo podrán utilizar servicios de cómputo en la nube a efectos de cumplimiento de la mencionada ley y, cuando contengan datos personales, el proveedor de servicios "en la nube" cumpla con las políticas de privacidad y protección de datos del responsable;

15 Dichas transferencias se definen en la Ley como "toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento" (artículo 3º, fracción XIX).

16 La Ley lo define como aquella persona física o moral de carácter privado que sola o conjuntamente trate datos personales.

17 El Aviso de Privacidad, contemplado por la norma mexicana, se define en el artículo 3.I de la LFPDPPP como aquel "documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15º de la presente Ley". Por su parte, el artículo 32º del Reglamento de la misma norma, establece en su artículo 24º que dicho Aviso deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.

guarde confidencialidad de la información personal; limite el tratamiento a la finalidad establecida con antelación, bajo consentimiento y expuesta en el Aviso de Privacidad; garantice la supresión de datos cuando un titular ejerza el derecho de cancelación e impida el acceso a personas no autorizadas; aplique las políticas de protección de acuerdo a lo que dice la normativa vigente —refiriéndose evidentemente tanto a Ley y el Reglamento, pero también a algunas disposiciones o lineamientos[18] que ha emitido el IFAI y la Secretaría de Economía[19] de México— entre otros.

En el caso de las subcontrataciones de servicios, entre las cuales pueden existir varias que se refieran al *cloud*, se dispone que dichas subcontrataciones se realicen mediante contrato que contenga cláusulas específicas sobre el compromiso del oferente del servicio de proteger los datos personales en los mismos términos del Aviso de Privacidad puesto a disposición por el responsable. Es pertinente, asimismo, mencionar el capítulo III del Reglamento, referente e las medidas de seguridad en el tratamiento de datos personales.

En el artículo 57º se menciona que tanto el responsable como el encargado[20] deberán establecer las medidas administrativas, físicas y técnicas para la adecuada protección de los datos personales, con arreglo a lo dispuesto tanto en la Ley como el Reglamento. La adopción de medidas de seguridad puede implicar una atenuación de sanciones, en caso de que se sufra algún ataque a las bases de datos, un *hackeo* de las mismas o similar y que, con ello, se vulneren los derechos de los titulares de la información. Ahora bien, para que una empresa determine qué medidas de seguridad son las más adecuadas, de acuerdo a su tamaño, el tipo de datos personales que trate y de qué tipo, entre otras cuestiones, debe tomar en consideración los siguientes criterios, mismos que podrían adaptarse a los tratamientos de datos personales por parte de las

18 Por ejemplo, los *Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a los que se refiere el artículo 44º de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, publicados en enero de 2013 por la Secretaría de Economía. Asimismo, esta institución ha emitido los *Criterios generales para la instrumentación de medidas compensatorias sin la autorización expresa del Instituto Federal de Acceso a la Información y Protección de Datos*, emitidos el 18 de abril de 2012. Ambos documentos, se publicaron en el *Diario Oficial de la Federación*. También se ha anunciado que próximamente se publicarán varios criterios con respecto a las medidas de seguridad que los responsables de la información personal deben implementar para una correcta protección de sus bases de datos. Por su parte, el IFAI ha publicado una *Guía práctica para generar el Aviso de Privacidad y las Recomendaciones para la designación de la persona o departamento de datos personales,* ambos de junio de 2011.

19 La Secretaría de Economía es el órgano regulador en la materia y la Ley en la materia le confiere diversas atribuciones con respecto a las empresas, entre las que tiene que fomentar la cultura de la protección de datos personales, entre otras.

20 Por su parte, el encargado es aquel que trata datos personales por cuenta del responsable, es decir, bajo las políticas y condiciones del Aviso de Privacidad que aquel estipuló ante el titular de los datos.

Administraciones Públicas (AAPP):

> Factores para determinar las medidas de seguridad
>
> Artículo 60º. 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.

En este sentido, para la implementación concreta de las medidas de seguridad, el responsable de las bases de datos personales debe establecer un inventario de la información bajo tratamiento, así como hacer un análisis de riesgos y de brecha entre las medidas ya existentes y las que aún no se tienen para detectar las posibles vulnerabilidades. En este análisis, evidentemente, se debe poner especial atención a los servicios que estén alojados en la nube, ya que esos son algunos de los que precisamente pueden ser más endebles. O bien, si se trata de servicios contratados con proveedores que tienen altas medidas en este sentido, quizá se trate de los más seguros.

De esos análisis debe derivarse, en caso de ser necesario, la capacitación del personal o del funcionariado que vaya a encargarse de implementar las medidas y que pueda

responder a eventuales y necesarias auditorías, tanto internas como externas. Asimismo, las personas designadas para cumplir con esta función deben tener la capacidad, con dicha formación y las habilidades que posean, de responder a las vulneraciones de seguridad, que el artículo 63º de la Ley enumera como la pérdida o destrucción no autorizada de los datos personales; el robo, extravío o copia no autorizada; el uso, acceso o tratamiento no autorizado; y, el daño, alteración o modificación no autorizada.

Si sucede alguna de las vulneraciones mencionadas, el responsable debe informar de inmediato al titular de la información para que incluso pueda tomar medidas personales para protegerse. Ésta es una disposición que está presente también en algunas disposiciones europeas y que cobra mucha fuerza en las propuestas de Reglamento en materia de privacidad y protección de datos personales que se discute en aquella comunidad de naciones. Ahora bien, como hemos dicho, los mecanismos de autorregulación son bien aceptados en términos internacionales y, también, a nivel local.

En México, por ejemplo, forman parte de los factores que incentiva la propia norma[21], para que las empresas adopten medidas adicionales de aquellas a las que la Ley les obliga, para proteger la privacidad. El objetivo de estos esquemas de autorregulación vinculante es que el principio de responsabilidad que marca la LFPDPPP se vea potenciado con su utilización. En el ámbito del cómputo en la nube esto es particularmente cierto, ya que precisamente la responsabilidad de contratar servicios de ese tipo, más que delimitar la misma —no se trata de pasar la información a un servidor que no se tiene a la vista y olvidarse del tema— se ve incrementada, porque habrá que asegurarse que la empresa que presta el servicio se obligue en los mismos términos que el responsable del tratamiento de la información personal.

Sin embargo, como alertamos antes, hemos estado hablando de una regulación que aplica al sector privado únicamente —pero que podría ser integrada en sus términos para garantizar la privacidad en el entorno del cloud por las AAPP—. Para el sector público, lo que está en esa línea es el *Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y la Comunicación y de Seguridad de la Información* (conocido como MAAGTIC-SI). Sin embargo, en este documento no se menciona el cómputo en la nube.

En donde sí se hace referencia al mismo y que es de aplicación al sector gubernamental es el Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal de septiembre de 2011. Incluye una definición clara del *cloud*, además de otras conceptualizaciones como la portabilidad

21 En este sentido, el artículo 81º del Reglamento de la Ley de protección de datos estima que "cuando un responsable adopte y cumpla un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda, en caso de verificarse algún incumplimiento a lo dispuesto por la Ley y el presente Reglamento, por parte del Instituto. Asimismo, el Instituto podrá determinar otros incentivos para la adopción de esquemas de autorregulación, así como mecanismos que faciliten procesos administrativos ante el mismo".

en la nube. No obstante, uno de los puntos que más llama la atención es el relacionado con el denominado Gobierno Abierto —al que volveremos más abajo— y al conocido como Gobierno 2.0, uno de los fenómenos que está en boga en la actualidad a nivel internacional. Todo ello se refiere a potenciar la rendición de cuentas y la transparencia al máximo, promoviendo las formas de participación ciudadana; entre otras cosas.

Este conjunto está sumamente relacionado con el tema que nos ocupa, ya que hace referencia no sólo a la apertura y la no opacidad, sino precisamente al uso de las tecnologías, en donde la privacidad de los usuarios —en este caso, en su condición fundamentalmente de ciudadanos— debe ser protegida de manera adecuada. En esos términos, la privacidad es una condición para que la seguridad de los datos y las personas dé confianza para utilizar las herramientas que los gobiernos promuevan para la citada participación ciudadana. De este modo, la e-confianza, se ubica como elemento esencial en la evolución hacia una auténtica Sociedad de la Información y el Conocimiento, por lo que es ese elemento central que debe garantizarse a las personas, en cuanto a la participación democrática, pero también con respecto a los servicios que se le brinden.

Un ejemplo es la aparición de Cédulas de Identidad Ciudadana, de las cuales se ha escuchado hablar en México, y que contendrán información sumamente sensible de las personas, ya que se prevé que contengan datos biométricos y que se les inserte una etiqueta de radiofrecuencia o RFID[22]. Aun cuando la utilidad de dichas cédulas es evidente, los riesgos casi son mayores, por lo que la seguridad que se tome en este caso será la clave para que su uso no se salga de control e incluso se propicie la comisión de delitos y se atente contra la seguridad de las personas.

Asimismo, debemos mencionar, como parte de estas cuestiones de privacidad y TIC aunadas a la transparencia y el derecho a la información, que en México se utiliza la Firma Electrónica Avanzada[23] para los servicios fiscales y para obtenerla el ciudadano debe aportar una cantidad ingente de datos, varios de ellos sensibles. Se requiere además de toda la información de la persona (nombre, domicilio, teléfono, número de identificación fiscal, etcétera), el acta de nacimiento, la identificación oficial vigente —que a su vez contiene los datos anteriores más la edad, el sexo, la clave de elector, la firma y la huella digital del dedo pulgar derecho— y durante el trámite se obtienen del titular más señas como la captura del iris de ambos ojos, la fotografía de frente, la toma de las diez huellas dactilares y la firma autógrafa.

22 Las etiquetas de radiofrecuencia son aquellas que permiten la ubicación concreta de un objeto "gracias a una onda emisora incorporada en el mismo que transmite por radiofrecuencia los datos identificativos del objeto, siendo esta identificación normalmente unívoca" (INTECO/AEPD, 2010, p. 5).

23 La Ley de Firma Electrónica Avanzada define a la misma como aquel "conjunto de datos y caracteres que permite la identificación del firmante, que ha sido creada por medios electrónicos bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos, la cual produce los mismos efectos jurídicos que la firma autógrafa" (artículo 2.XIII).

Como puede verse, la información es sumamente sensible y delicada, por lo cual su protección se hace muy necesaria. Si bien la obtención de esta información es para "garantizar el vínculo que debe existir entre un certificado digital y su titular", su protección es altamente importante. En este sentido, el Sistema de Administración Tributaria (SAT) que emite la firma avanzada, sostiene que "los datos personales antes citados serán incorporados y protegidos en los sistemas del Servicio de Administración Tributaria, de conformidad con los Lineamientos de Protección de Datos Personales y con las diversas disposiciones fiscales y legales sobre la confidencialidad y protección de datos, a fin de ejercer las facultades conferidas a la autoridad fiscal"[24]. Por el momento, la firma electrónica sólo es utilizada con fines fiscales, pero hay diversas propuestas de modificación de la legislación aplicable que apuntan a que su uso se extienda a muchos otros trámites y servicios, no solamente de gobierno, sino privados.

24 Sitio web oficial del Servicio de Administración Tributaria de la Secretaría de Hacienda y Crédito Público, en referencia a los requisitos para obtener la FIEL (firma electrónica avanzada). Disponible en: http://www.sat.gob.mx/sitio_internet/e_sat/tu_firma/60_11506.html

Referencias

- Ackerman, J. (2008). *Más allá del acceso a la información: transparencia, rendición de cuentas y Estado de Derecho*. México: Siglo XXI editores, 404 pp.
- Arellano, W. (2012). La reforma constitucional de telecomunicaciones de 2013. *Mediatelecom. Agencia Informativa*. Recuperada de: http://www.mediatelecom.com.mx/index.php/agencia-informativa/colaboradores/item/45851-la-reforma-constitucional-en-materia-de-telecomunicaciones-de-2013
- Carbajal, C. (2011). *La transparencia y la rendición de cuentas como elementos esenciales para la consolidación de un verdadero Estado de Derecho*. México: CAIPEC, 5to Premio Regional de Ensayo sobre Transparencia, 7 pp.
- Carbonell, M. (2011). L*os derechos fundamentales en México*. México: Universidad Nacional Autónoma de México, Editorial Porrúa y Comisión Nacional de los Derechos Humanos, 1111 pp.
- Código Civil Federal, publicado en el Diario Oficial de la Federación el 26 de mayo de 1928.
- Código Penal Federal, publicado en el Diario Oficial de la Federación el 14 de agosto de 1931.
- Constitución Española de 1978, publicada en el Boletín Oficial del Estado el 27 de diciembre.
- Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 5 de febrero de 1917.
- Convención Americana de Derechos Humanos de 1969.
- Declaración Universal de los Derechos Humanos de 1948.
- Directiva 2002/58 del Parlamento Europeo y del Consejo, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas, publicada en el Diario Oficial de las Comunidades Europeas el 12 de julio.

Instituto Nacional de Tecnologías de la Información y la Comunicación y AGENCIA Española de Protección de Datos. (2010). *Guía sobre seguridad y privacidad de la tecnología RFID*. Madrid: Inteco, 49 pp.

Ley Federal de Derechos de Autor, publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996.

Ley Federal de Protección de Datos en Posesión de Particulares, publicada en el Diario Oficial de la Federación el 5 de julio de 2010.

Ley Federal de Telecomunicaciones, publicada en el Diario Oficial de la Federación el 7 de junio de 1995, reformada el 11 de abril de 2006.

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.

López, S. (1984). *El derecho a la información*. México, Miguel Ángel Porrúa y Universidad Nacional Autónoma de México, 224 pp.

López, S. (2009). *El acceso a la información como un derecho fundamental: La reforma al artículo 6° de la Constitución mexicana*. México: IFAI, Cuadernos de Transparencia número 17, 66 pp.

López, S. y Arellano, D. (coords.) (2008). *Estudio de materia de transparencia de otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*. México: Centro de Investigación y Docencia Económica, Instituto Federal de Acceso a la Información y Universidad Nacional Autónoma de México, 96 pp.

Piñar, J. L. (2008). *¿Existe la privacidad?* Madrid: CEU Ediciones, 49 pp.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el *Diario Oficial de la Federación* de 21 de diciembre de 2011.

Téllez, J. (2013). *Lex Cloud computing. Estudio jurídico del cómputo en la nube en México*. México: Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 733 pp. Serie Doctrina Jurídica.

Urzúa, C. (2012). Lo público y lo privado: la sociedad de la información y el conocimiento en Chile. En Arellano, W. (Coord.). *La Sociedad de la Información en Iberoamérica. Estudio multidisciplinar*. México: Fondo de Información y Documentación para la Industria Infotec, pp. 365-381.

http://www.inegi.org.mx/eventos/2014/big-data/presentacion.aspx

http://cdn.mexicodigital.gob.mx/EstrategiaDigital22DIc2014.pdf