La recepción del derecho a la protección de datos en México: breve descripción de su origen y estatus legislativo[1]

Lina Ornelas Núñez[*]
y Sergio López Ayllón

I. Introducción

John Rawls señala que una sociedad puede definirse como una asociación más o menos autosuficiente de personas que reconocen ciertas reglas de conducta como obligatorias en sus relaciones, y que en su mayoría actúan de acuerdo con ellas. En ese sentido, la sociedad se caracteriza típicamente tanto por un conflicto como por una identidad de intereses. Esta doble faceta en la caracterización de la sociedad surge debido a que, si bien es cierto que la cooperación social hace posible para todos una vida mejor de la que cada uno tendría viviendo en el aislamiento, también lo es que las personas no son indiferentes respecto a cómo han de distribuirse los mayores beneficios producidos por la colaboración.[2]

A lo largo de los estadios por los que ha pasado la historia de la humanidad, ésta se ha agrupado y gobernado bajo regímenes normativos muy diversos, creando importantes cuerpos normativos[3], no obstante lo cual hasta antes del siglo XVIII, no era posible aludir a la existencia de un conjunto de valores (listado de derechos) respecto de los cuales se tuviera la certeza histórica que el ser humano compartía en común. En ese sentido, la Ilustración señala el momento a partir del cual dio inicio la evolución de las instituciones que han forjado al Estado Moderno, entre cuyos productos se encuentran las declaraciones de derechos y las constituciones políticas.

Con las ideas de la Ilustración, comenzó una revolución normativa irreversible de la que derivarían, 200 años más tarde, instrumentos como la Declaración Universal de los Derechos Humanos, en la que se contiene en "germen" la síntesis de un movimiento

[*] Lina Ornelas es directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública (IFAI). Las opiniones aquí vertidas no representan necesariamente las institucionales. Por su parte, Sergio López Ayllón es profesor investigador del Centro de Investigación y Docencia Económicas (CIDE).

dialéctico que comenzó con la universalidad abstracta de los derechos naturales, pasó por la particularidad concreta de los derechos positivos nacionales y terminó con la universalidad ya no abstracta sino concreta de los derechos positivos universales, dando inicio a un largo proceso cuya realización última no podemos aún ver[4].

Constata lo anterior, la existencia de las distintas fases por las que han pasado los derechos humanos. En un primer tiempo se afirmaron los derechos de libertad, es decir, todos aquellos derechos que tienden a limitar el poder del Estado y a reservar al individuo o a grupos particulares una esfera de libertad frente al mismo. En un segundo momento se proclamaron los derechos políticos, al concebirse la libertad no sólo como el "no impedimento", sino positivamente como autonomía, teniendo por consecuencia una participación cada vez más amplia, difundida y frecuente de los miembros de una comunidad por el poder político (es decir, libertad dentro del Estado). Por último, se reconocieron los derechos sociales, que expresan la maduración de nuevas exigencias, de nuevos valores, como los del bienestar y de la igualdad no solamente formal, derechos a los que se podría llamar libertad a través o por medio del Estado.[5]

En prospectiva, y simplemente a manera de referencia, si a Locke, campeón de los derechos de libertad, alguien le hubiera dicho que todos los ciudadanos habrían debido participar en el poder político y peor aún obtener un trabajo remunerado, habría respondido que eran locuras. Lo anterior es así, toda vez que la persona respecto de la que Locke realizó estudios para definir la naturaleza humana, era únicamente el burgués o el comerciante del siglo XVIII, razón por la cual no pudo advertir las exigencias y reclamos de quien se ubicaba en otro estrato de la sociedad, lo cual le impidió abarcar el espectro completo de la naturaleza humana y con ello determinar los sujetos a quienes debía alcanzar la protección de los derechos humanos.[6]

Parafraseando a Bobbio, la Declaración Universal de los Derechos Humanos, representa la conciencia histórica que la humanidad tiene de sus propios valores fundamentales en la segunda mitad del siglo XX, es una síntesis del pasado y una inspiración para el porvenir, pero sus tablas no han sido esculpidas de una vez y para siempre[7].

El siglo XXI comienza con un despliegue tecnológico estelar. No puede concebirse más la vida de los seres humanos ni su interacción, sin el uso de tecnologías *urbi et orbi.* Dicha expansión conlleva el intercambio de flujos de información incluida la relativa a las personas. Ahora es posible a través de distintos medios acceder a la información de millones de seres humanos y sus actividades en cualquier parte del planeta. Sin embargo, frente al terreno ganado en materia de libertad de información y expresión, se ha irrumpido silenciosamente en el ámbito de lo privado, ya que la sencilla obtención de cualquier tipo de dato sobre una persona física posibilita la generación de perfiles sobre ella y afectar la esfera de sus derechos y libertades. Por ello puede afirmarse que los horizontes para la privacidad se están transformando en *terra incognita* debido a que sin que el propio titular del dato se entere, terceros -sean entes públicos o privados- tratan

su información a través de la utilización de todo tipo de tecnologías como la minería de datos, la geo-localización, la detección remota o la videovigilancia, todo lo anterior conectado a la w*orld wide web,* tecnologías que hoy en día ya han madurado y están plenamente disponibles en cualquier lugar del mundo.

Los avances tecnológicos repercuten generalmente de forma positiva en la calidad de vida del ser humano, mas sería ingenuo desconocer que también con ellos nacen nuevos conflictos e interrogantes a los que el Derecho, en su objetivo último de ordenar la convivencia social, debe dar respuesta. La tecnología no ha de permanecer ajena al Derecho, ni evidentemente, a la Constitución, por más que la incesante innovación les obligue a ser objeto de continuas relecturas y adaptaciones, so riesgo de caer en la obsolescencia.[8]

Por esa razón y desde hace décadas, cada vez más países aprueban nuevas leyes sobre privacidad o protección de datos[9], esto en atención al menor o mayor grado de importancia que a la privacidad se le asigne, ya que está ligada al pasado cultural e histórico de cada sociedad.[10]

Recientemente la Cumbre Mundial de la Sociedad de la Información ha hecho un llamamiento para pedir normas "mundiales" para la privacidad en el sentido siguiente: *"Hacemos un llamamiento a todas las partes interesadas para garantizar el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de legislación, la aplicación de marcos de colaboración, mejores practicas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios".*[11]

Los párrafos precedentes sirven de preámbulo para abordar el estado de la cuestión en México, lo cual nos lleva a describir los alcances de este artículo.

A efecto de lo anterior, se narran los antecedentes del derecho a la protección de datos, desde los instrumentos internacionales de derechos humanos, hasta la regulación formulada por bloques económicos como la Unión Europea, la Organización para la Cooperación y el Desarrollo Económico, y del Foro de Cooperación Económica Asia Pacífico, así como la resolución que en esta materia elaboró la Organización de las Naciones Unidas.

Posteriormente se abordan las decisiones de la Comisión Europea sobre el nivel de adecuación que deben tener terceros países para la circulación de datos personales ya que arroja luz sobre algunos elementos indispensables a incluir en una regulación en la materia. Asimismo, se resaltan los aspectos esenciales de los apartados que contienen las directrices para la armonización del derecho a la protección de datos en Iberomérica como un insumo a considerar en la confección de una ley por su clara estructuración a manera de lista de verificación.

Posteriormente, se abordan las recientes reformas a los artículos 6, 16 y 73 de la Constitución Federal, estos últimos aún en ciernes, en cuanto al derecho a la protección de datos se refiere.

Finalmente en las conclusiones intentamos llevar a cabo un primer acercamiento en cuanto a los elementos mínimos o ejes fundamentales a partir de los cuales se debiera erigir la futura legislación en la materia para el caso mexicano, sobre todo abrevando de las experiencias internacionales y la propia realidad del país.

II. Antecedentes

1. Instrumentos internacionales

En los instrumentos internacionales, el artículo 12 de la Declaración Universal de los Derechos del Hombre[12] (10 de diciembre de 1948) establece el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques.

En el mismo sentido, el artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales[13] (14 de noviembre de 1950), reconoce el derecho de la persona al respeto de su vida privada y familiar de su domicilio y correspondencia.

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[14] (16 de diciembre de 1966), señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

En el mismo tenor, la Convención Americana[15] sobre derechos humanos (22 de noviembre de 1969) en su artículo 11 apartado 2, establece que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

2. Unión Europea

2.1 Los orígenes del derecho a la protección de datos

En 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a la intimidad. Como fruto de la Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre los "derechos humanos y nuevos logros científicos y técnicos[16]".

En un momento posterior, surgen diversas leyes nacionales, en 1977 era aprobada la Ley de Protección de Datos de la República Federal Alemana, mucho más ambiciosa

que su predecesora del *Land* de *Hesse*, en 1978 corresponde el turno a Francia mediante la publicación de la Ley de Informática, Ficheros y Libertades, aún vigente. Otros países entre los que se emitió regulación en la materia son Dinamarca con las leyes sobre ficheros públicos y privados (1978), Austria con la Ley de Protección de Datos (1978) y Luxemburgo con la Ley sobre la utilización de datos en tratamientos informáticos (1979)[17].

Hacia la década de los años ochenta surgen los instrumentos normativos en los que se plasma un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como las medidas de seguridad a observar por parte de los responsables de los ficheros. Es en esta década cuando desde el Consejo de Europa se dio un respaldo definitivo a la protección de la intimidad frente a la potencial agresividad de las tecnologías, siendo decisivo para ello la promulgación del convenio No. 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.[18]

2.2. Convenio 108 del Consejo de Europa

El Convenio 108 sobre protección de datos personales (en adelante el Convenio 108) entró en vigor el 1 de octubre de 1985 y es creado con el propósito de garantizar a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades, en particular, el derecho a la vida privada frente a los tratamientos de datos personales, conciliando el respeto a ese derecho y la libre circulación de la información entre los Estados.

De esta forma el Convenio 108 constituye el primer instrumento de carácter vinculante para los Estados en el que se plasman los principios de la protección de los datos de carácter personal.

Hay que decir que el Convenio 108 no proporcionó la suficiente protección homogénea en materia de protección de datos que se había esperado. Esto debido esencialmente a la naturaleza del Convenio: el mismo a pesar de ser vinculante, establecía únicamente unos principios mínimos, permitiendo que posteriormente fueran los estados firmantes los que los desarrollaran.[19]

2.3 Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos

La Directiva 95/46, fue aprobada con un doble objetivo: por un lado garantizar el derecho a la vida privada reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos, en particular por lo que respecta al tratamiento de datos personales, ampliando los principios ya recogidos en otras normas internacionales y otorgando un mayor nivel de protección dentro de la Comunidad, sin disminuir el ya existente; y, por otro lado impedir la restricción de la libre circulación de los datos personales en todos los Estados miembros de la Unión Europea.[20]

El proyecto de Directiva 95/46, se inspira esencialmente en la doctrina constitucional alemana y en la ley francesa de 1978. Sin embargo, los trabajos se paralizan, dado que diversos estados consideran que no es posible la aprobación por parte de las instituciones comunitarias de una norma reguladora de un derecho fundamental de los ciudadanos, al no tener tal hecho cabida en las normas rectoras del Derecho Comunitario vigentes en ese momento.[21]

A partir de ese momento, los trabajos se centraron en la necesidad de adoptar un texto de Directiva 95/46 referido exclusivamente a la protección de datos de carácter personal como fundamento no a la protección de un derecho fundamental, sino la adopción de un marco comunitario que garantice la libre circulación de los datos de carácter personal, no pudiendo los Estados miembros invocar el derecho a la protección de datos como justificación para impedir dicha libre circulación.[22] La Directiva 95/46, finalmente, es aprobada el 24 de octubre de 1995.

2.4 Carta de Derechos Fundamentales de la Unión Europea

La Carta de Derechos Fundamentales de la Unión Europea fue aprobada por la cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza el 7 de diciembre de 2000, reconociendo entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8.

De esta forma, a partir de la Carta de Derechos Fundamentales de la Unión Europea, la protección de los datos de carácter personal se configura como un derecho fundamental y como un derecho autónomo del derecho a la intimidad y a la privacidad de las personas.

3. Recomendaciones de la Organización para la Cooperación y el Desarrollo Económico

La recomendación de la Organización para la Cooperación y el Desarrollo Económico (OCDE) en la que se contienen las "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales, adoptada el 23 de septiembre de 1980 (Recomendaciones de la OCDE), constituye el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos de carácter personal.[23]

Su adopción se funda en la constatación por parte del Consejo de la OCDE de la inexistencia de uniformidad en la regulación de esta materia en los distintos Estados miembros, lo que dificultaba el flujo de los datos personales entre los mismos..[24]

La primera parte de la Recomendación, establece las definiciones aplicables, la parte segunda establece los principios básicos aplicables al tratamiento de los datos personales, la tercera está dedicada a las transferencias internacionales de datos, la cuarta trata, en

términos generales, sobre los medios de implantación de los principios básicos expuestos en las partes anteriores y la quinta tiene que ver con cuestiones de asistencia mutua entre los países miembro.

4. Foro de Cooperación Economía Asia Pacífico.

Uno de los grupos formados por el Foro de Cooperación Economía Asia Pacífico (APEC), es el Grupo de Manejo del Comercio Electrónico (ECSG) establecido en febrero de 1999, y que dentro de sus principales actividades esta el desarrollo de legislaciones y políticas compatibles entre las Economías en el campo de la Privacidad, para lo cual ha desarrollado los lineamientos generales en la materia con el fin de que los mismos sean contemplados y establecidos en los cuerpos legales correspondientes y con esto lograr un flujo de datos seguro y sin obstáculos.

Los principios desarrollados para el Marco de Privacidad de APEC se basan en las Recomendaciones de la OCDE. Estos principios tienen como fin los siguientes aspectos: Proteger la Privacidad de información personal; prevenir la creación de barreras innecesarias al flujo transfronterizo de datos; fomentar la uniformidad por parte de empresas multinacionales en los métodos utilizados para la recolección, uso y procesamiento de datos personales; fomentar los esfuerzos nacionales e internacionales para promover y hacer cumplir las disposiciones legales de protección de datos personales.

La protección de la privacidad está diseñada para prevenir a los individuos a efecto de que sus datos no se recolecten erróneamente o bien se haga un mal uso de ellos, estableciendo medidas de resarcimiento proporcionales, en los casos que así proceda. Entre los principios que se reconocen encontramos el de aviso, limitación de la recolección, el de integridad de la información personal y el de salvaguardias a la seguridad, entre otros.

5. Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas

La Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas (Resolución 45/95 de la ONU) de 14 de diciembre de 1990, contiene fundamentalmente una lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial, entre otros, los de licitud, exactitud, finalidad, acceso y no discriminación.

III. Orígenes del derecho a la protección de datos en México

1. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y el derecho a la protección de datos personales

Con fecha 11 de julio de 2002, fue publicada en el Diario Oficial de la Federación la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (Ley Federal de Transparencia)[25], la cual tiene por objeto regular el derecho a la información en una de sus vertientes, la del acceso a la información.

Considerando lo anterior, conviene cuestionarse en qué punto se conectan el derecho de acceso y el derecho a la protección de datos, la respuesta está en los límites del derecho de acceso a la información.

En el caso mexicano los límites al derecho de acceso están señalados de manera expresa en la propia Ley Federal de Transparencia en los artículos 13 y 14 y en el artículo 18. Entre las hipótesis normativas previstas en el artículo 18 de la Ley Federal de Transparencia, se establece que como información confidencial serán considerados los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos señalados en la misma.

Los datos personales se definen como aquella información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad[26].

Aunado a lo hasta ahora descrito, en el capítulo IV de la Ley Federal de Transparencia se establecen una serie de disposiciones dirigidas a garantizar el derecho a la protección de datos personales, tales como principios, derechos de los interesados, la existencia de un registro de protección de datos, así como las algunas reglas en torno a los procedimientos de acceso y corrección de datos personales.

2. El Instituto Federal de Acceso a la Información Pública y la protección de los datos personales

Entre las funciones a destacar del Instituto Federal de Acceso a la Información (IFAI), para efectos de este estudio, se encuentran dos aspectos, en primer lugar el relativo al conocimiento y resolución de los recursos de revisión derivado de solicitudes de acceso y en segundo el relacionado con la expedición de disposiciones administrativas de carácter

general (Lineamientos) para la mejor aplicación de la Ley Federal de Transparencia.

El primero de los aspectos señalados cobra especial importancia en el desarrollo del derecho a la protección de datos en México, ya que es a través de las resoluciones emitidas por el Pleno del IFAI, que se establecen una serie de criterios relevantes respecto al acceso y corrección de datos personales, principalmente en los casos denominados de "tensión de derechos" (fotografías de servidores públicos, expediente clínico del entonces Presidente de la República, entre otros.)

En cuanto al segundo de los aspectos indicados, con fecha 30 de septiembre de 2005, el IFAI publicó en el Diario Oficial de la Federación los Lineamientos de Protección de Datos Personales[27], los cuales tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal, para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Derivado de los citados lineamientos, con fecha 23 de agosto de 2006, se publicaron las Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales, con el objetivo de constituirse en propuestas y sugerencias específicas que le permitiera a la Administración Pública Federal lograr una eficaz protección de los datos personales contenidos en sus sistemas de datos, según se desprende del último de sus considerandos[28].

Como se puede observar, la intervención del IFAI en esta materia es de la mayor relevancia ya que puede llegar constituirse en el factor que, por una parte, permita que el derecho a la protección de datos personales, dentro de los límites de la legalidad, responda a las exigencias a las que la realidad nos enfrenta, y por la otra facilite elementos orientadores que conduzcan al mejor entendimiento y aplicación de la norma jurídica a los casos que se les presenten.

3. El derecho a la protección de datos en la Constitución Política de los Estados Unidos Mexicanos

3.1 Artículo 6 de la Constitución Federal

Con fecha 20 de julio de 2007, fue publicada en el Diario Oficial de la Federación, la reforma al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, fundamentalmente, con el objeto de homologar el derecho de acceso a la información pública gubernamental, en cualquier punto del territorio nacional y en los tres niveles de gobierno. Al respeto, en el dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, de la Cámara de Diputados se señaló lo siguiente:

> La iniciativa que se dictamina, surge de un análisis pormenorizado y exhaustivo de una problemática nacional que no debemos aceptar: luego de cuatro años de marcha

> de las leyes de transparencia y acceso a la información, se ha cristalizado una heterogeneidad manifiesta y perjudicial de los cimientos para el ejercicio del derecho, que contienen diversas leyes, tanto federal como estatales.

La reforma al artículo 6 de la Constitución Federal plantea diversos nuevos retos a la transparencia gubernamental en nuestro país que se materializaron en siete fracciones. En las tres primeras se establecieron los principios fundamentales que dan contenido básico al derecho, mientras que en las fracciones cuarta, quinta y sexta se plantearon las bases operativas que deberán contener las leyes en la materia para hacer del derecho una realidad viable, efectiva y vigente, según señala el ya citado dictamen de la Cámara de Diputados.

El reformado artículo 6, fracción II, establece como parte de los principios en materia de acceso, que 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.

Al respecto, en el dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, de la Cámara de Diputados, en el apartado en el que se hace el análisis de la iniciativa, se indicó lo siguiente:

> En ella se establece una segunda limitación al derecho de acceso a la información, misma que se refiere a la protección de la vida privada y de los datos personales. Esta información no puede estar sujeta al principio de publicidad, pues pondría en grave riesgo otro derecho fundamental, que es el de la intimidad y la vida privada.
>
> Es fundamental esclarecer que aunque íntimamente vinculados, no debe confundirse la vida privada con los datos personales…
>
> La fracción segunda establece también una reserva de ley en el sentido que corresponderá a ésta, determinar los términos de la protección y las excepciones a este derecho…

El mencionado artículo 6, fracción II, tiene la virtud de ser la primera disposición en la historia de nuestro país que hace un reconocimiento expreso al derecho a la protección de datos personales en la cúspide normativa, dando continuidad a la labor iniciada por el legislador ordinario a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

3.2 Artículo 16 de la Constitución Federal

Del año 2000 al 2005 se promueven diversos proyectos legislativos en torno al tema en el Congreso de la Unión, sin que ninguno de ellos fructifique dada la ausencia de disposición constitucional que las sustente, hasta que en el mes de abril de 2006 se aprobó

en la Cámara de Senadores el Decreto por el que se adicionan dos párrafos al artículo 16 de la Constitución Federal para reconocer el derecho a la protección de datos personales, enviándose a la Cámara de Diputados para los efectos constitucionales conducentes.

Derivado de lo anterior, con fecha 20 de septiembre de 2007, se vota, con un par de modificaciones mínimas, la propuesta enviada en su momento por la Cámara de Senadores para reconocer el derecho a la protección de datos personales como derecho fundamental autónomo. En este momento la iniciativa regresó a la Cámara de su Origen (la de Senadores) en virtud de las pequeñas modificaciones efectuadas por la Revisora.

El Proyecto de Decreto por el que se adicionan dos párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos establece:

> Artículo 16. 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 de procedimiento.
>
> Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y en su caso, obtener su rectificación, cancelación y manifestar su oposición en los términos que fijen las leyes.
>
> La Ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden, seguridad y salud públicos o para proteger los derechos de tercero.
>
> No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado cuando menos con pena privativa de libertad y existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado.

Con la reforma al artículo 16 constitucional finalmente se reconoce y da contenido al derecho a la protección de datos personales. En ese sentido, en la reforma se plasman los derechos con los que cuentan los titulares de los datos personales como lo son los de acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO).

Por otra parte, se hace referencia a la existencia de principios a los que se debe sujetar todo tratamiento de datos personales, así como los supuestos en los que excepcionalmente dejarían de aplicarse dichos principios.

Conviene destacar que inclusive antes de la reforma al artículo 6º constitucional y de la propuesta de reforma al 16, se venían haciendo esfuerzos muy loables en torno al derecho a la protección de datos personales, no obstante lo cual la dimensión de este derecho seguía sin tener la profundidad requerida para dotar al gobernado de un herramienta efectiva que le permitiera equilibrar su situación jurídica frente al vertiginoso desarrollo tecnológico y el pujante comercio internacional que al mismo acompaña.

A mayor abundamiento, conviene citar algunas de las razones que se plasman en la valoración de la minuta aprobada por la Cámara de Diputados (en su carácter de cámara revisora) en relación con la propuesta de reforma al mencionado artículo 16:

> Esta Comisión revisora resalta la relevancia de emitir un dictamen en el que por primera vez en la historia de México, se reconozca al máximo nivel de nuestra pirámide normativa la existencia de un nuevo derecho distinto y fundamental a la protección de datos personales, dentro del catálogo de garantías. Lo anterior, en razón de la evolución normativa experimentada en nuestro país, a partir de la regulación de la protección de datos personales en posesión del Estado regulada por la fracción II del artículo 6 constitucional. La intención de reformar el artículo 16 para incluir la protección de los datos personales, es un camino que desde hace algún tiempo inició el legislador mexicano.
>
> Derivado de lo anterior, la propuesta que se presenta ante esta Cámara Revisora, tiene como propósito consolidar el derecho a la protección de datos en nuestro país, extendiendo su ámbito de aplicación a todos los niveles y sectores, apuntalando, por una parte, la estructura edificada a través del artículo 6 fracción II de la Constitución Federal y de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para los sistemas de datos personales en posesión de los entes públicos federales y, por la otra, reconociendo la existencia del mismo respecto de los datos personales en poder del sector privado.

Hasta aquí en cuanto a las razones y alcances, en lo general, que produciría la reforma al artículo 16 constitucional de aprobarse por el Senado[29], y en su momento por las legislaturas estatales.

3.3 Artículo 73 de la Constitución Federal

De acuerdo con el proyecto de Decreto aprobado en la Cámara de Diputados (en su carácter de cámara de origen), la propuesta tiene por objeto dotar de facultades al Congreso Federal para que legisle en materia de protección de datos en posesión de los particulares, la cual es la siguiente:

> Artículo Único. Se adiciona la fracción XXIX-Ñ al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:
>
> Artículo 73. El Congreso tiene facultad:
>
> I. a XXIX-N. ...
>
> XXIX-Ñ. Para legislar en materia de protección de datos personales en posesión de particulares.

Entre las materias con las que se encuentra íntimamente vinculado el derecho a la protección de datos se encuentra el comercio internacional. Dentro de las razones históricas

que justificaron la creación de este derecho y sus consecuentes instrumentos regulatorios, está el impedir la restricción de la libre circulación de los datos personales entre Estados.

El mejor ejemplo de la situación previamente descrita es la Unión Europea, en la que se garantiza la libre circulación de personas, bienes y datos personales entre los países miembros, lo que desde luego no representa ningún contrasentido, considerando que los Estados miembros cuentan con regulaciones homogéneas a partir de las cuales los datos se encuentran igualmente protegidos en un país u otro de la Unión.

Existen dos razones que sustentan que la ley que regule los datos personales en posesión de los particulares sea federal: por una parte, el comercio internacional, en virtud de que el Estado Mexicano hacia el exterior es uno y como tal debe contar con una legislación uniforme en sus relaciones internacionales, independientemente del área del territorio nacional donde materialmente se estén tratando los datos personales, y por la otra, que la materia de comercio es federal, de conformidad con nuestra Ley Fundamental.

Respecto de los datos personales en posesión de los entes públicos estatales y municipales, corresponderá a las legislaturas estatales trazar el camino por el que encauzarán el derecho a la protección de datos personales, sobre la base constitucional que en su momento se apruebe.

De concretarse estas reformas, México se ubicaría entre la élite de países que cuentan con un derecho a la protección de datos personales a nivel constitucional, con lo que se contribuye a la consolidación democrática y económica de este país desde el terreno de los derechos humanos.

IV. Aspectos relevantes de la actualidad del derecho a la protección de datos que debieran tenerse como referente para la legislación mexicana

1. Nivel de adecuación de países terceros conforme a la Directiva 95/46/CE

Los artículos 25 y 26 de la Directiva 95/46/CE, establecen un régimen específico para los flujos transfronterizos de datos personales hacia países distintos de los estados miembros en los cuales se exige, como punto de partida, que el Estado al que se destinen los datos ofrezca un nivel adecuado de protección.

A efecto de lo anterior, la Comisión Europea decide si un país tercero se adecua al nivel de protección de datos establecido en la citada Directiva 95/46/CE, teniendo en cuenta el dictamen que para el caso elabore Grupo de trabajo de protección de las per-

sonas en lo que respecta al tratamiento de datos personales, creado en virtud del artículo 29 de la mencionada Directiva teniendo como base el documento de trabajo del Grupo sobre transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, aprobado el 24 de julio de 1998, cuyo Capítulo 1 analiza qué debe entenderse por "protección adecuada".

Dicho documento delimita dos tipos de análisis que habrían de efectuarse sobre la legislación del Estado de destino de los datos, a fin de poder delimitar si la misma resulta adecuada: el relativo a su contenido sustantivo y el relacionado con los mecanismos y procedimientos de aplicación de la legislación sustantiva.

En cuanto al contenido sustantivo, la legislación del Estado de destino habría de contener los principios básicos de protección de datos que tradicionalmente son reconocidos por los acuerdos y directrices internacionales adoptados en este ámbito, considerándose como tales los siguientes: 1. Limitación de la finalidad; 2. Calidad y proporcionalidad de los datos; 3. Transparencia; 4. Seguridad y confidencialidad; 5. Derechos de acceso, rectificación, supresión y bloqueo de los datos; 6. Restricciones a la transferencia ulterior; 7. Categorías especiales de datos; 8. Marketing directo; 9. Decisión individual automatizada.

Aunado a lo anterior, la Comisión Europea verifica que el ámbito de aplicación de la regulación de un tercer estado contemple a los sectores público y privado, que exista una autoridad independiente, dotada con facultades de inspección y sanción ante la cual puedan acudir los interesados para hacer efectivos sus derechos frente a los responsables de los tratamientos de datos.[30]

2. Directrices para la armonización de la protección de datos en la comunidad Iberoamericana, el cual constituye un modelo acerca de lo que debe contener una legislación en los estados miembros.

Los días 13 y 14 de noviembre de 2003, en la ciudad de Santa Cruz de la Sierra, Bolivia, se llevó a cabo la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, de la que derivó la Declaración de Santa Cruz de la Sierra, la cual fue suscrita por el Presidente de la República.[31]

Es a partir de la integración de México en la Red Iberoamericana de Protección de Datos, que se ha cobrado conciencia plena sobre el tema gracias al acercamiento con otros países en los que ya se cuenta con una legislación integral y vigente, a través de los cuales fue posible conocer los efectos positivos que produce el contar con instrumentos normativos en la materia de protección de datos personales.

En el V Encuentro Iberoamericano de Protección de Datos[32], se aprobó por los miembros de la Red, el documento que contiene "Las directrices para la armonización

de la protección de datos en la comunidad Iberoamericana, el cual constituye un modelo acerca de lo que debe contener una legislación en los estados miembros"

Entre los elementos que debe contener una ley de protección de datos de acuerdo con las directrices de referencia podemos destacar los siguientes aspectos:

- En cuanto al ámbito de aplicación, la necesidad de dirigir la legislación a todo tipo de tratamiento de datos sea manual o automatizado llevados a cabo por las entidades de los sectores público y privado.
- En relación con el régimen de excepciones al ámbito de aplicación el sustraer o modular, según el caso, cuestiones relativas a seguridad nacional, el orden público, la salud pública o la moralidad y dicha medida resulte estrictamente necesaria y no excesiva en el ámbito de una sociedad democrática.
- Respecto a las disposiciones generales fijar los principios de calidad de los datos (lealtad, licitud, proporcionalidad, exactitud y conservación), legitimación del tratamiento, transparencia e información al interesado, entre otros.
- En torno a los derechos que se reconozcan los de acceso, rectificación, cancelación y oposición respecto de los cuales se establezcan, procedimientos claros, expeditos y gratuitos o sin gastos excesivos.
- En cuanto a la seguridad y confidencialidad en el tratamiento que se adopten de medidas técnicas y organizativas necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.
- Respecto del régimen de transferencias internacionales de datos como regla general que éstas se efectúen únicamente al territorio de Estados cuya legislación recoja los mínimos requeridos para tales efectos, en una situación similar a la que ocurre en el caso de las autorizaciones que realiza la Comisión Europea en la Unión Europea.
- En relación con la autoridad de control que está se diseñe de tal manera que pueda actuar con plena independencia e imparcialidad, con mecanismos que garanticen la independencia e inamovilidad de las personas a cuyo cargo se encuentre la dirección de dichas autoridades.

Asimismo se sugiere que la autoridad de control cuente como mínimo con competencias para conocer de las reclamaciones que les sean dirigidas por los ciudadanos, en particular en cuanto al ejercicio de sus derechos, para realizar las averiguaciones e investigaciones que resulten necesarias para el cumplimiento de la regulación, así como para imponer sanciones, en los casos que así lo amerite

- También deberá establece la necesidad de contar con un registro de los tratamientos llevados a cabo por los sectores público y privado, al que puedan acceder los interesados, a fin de poder ejercer sus derechos.

V. Conclusiones:

El derecho a la protección de datos personales ha experimentado un desarrollo muy basto a nivel europeo extendiéndose a otras latitudes sobre todo en razón del avance tecnológico, la ubicuidad de la computación y los intercambios globales.

Del análisis efectuado podemos decir que este nuevo derecho sitúa a la persona como el centro de la protección, mas que al dato *per se*. Dado que la norma secundaria derivara de un derecho fundamental reconocido al más alto nivel de la pirámide normativa será necesario esperar la aprobación definitiva de las reformas constitucionales a los artículos 16 y 73, para conocer los alcances que a este derecho quiso dar el constituyente.

Una mirada crítica a los modelos existentes de protección de datos personales puede permitirnos el diseño de una ley moderna que recoja las mejores prácticas, los mecanismos mas adecuados de tutela y modelar instituciones eficaces. Los retos no son pocos en este tema. Por su complejidad y múltiples conexiones con otros derechos, el de la protección de datos se antoja laberíntico.

Derivado de los desarrollos normativos descritos en este artículo, a continuación y solo a modo indicativo, consideramos que los ejes fundamentales de una ley de protección de datos personales pueden ser los siguientes:

a) En primer lugar el objeto de la norma debería ser garantizar la protección de los datos de carácter personal reconociendo los derechos y principios que rigen la materia. En ese sentido, la ley debe posibilitar de manera equilibrada por una parte, la legítima y controlada transferencia y utilización de datos genéricos con el consentimiento tácito de los titulares y cuando se trate de datos sensibles solo mediante el consentimiento expreso e informado. Una regulación demasiado estricta sería de difícil cumplimiento, sobre todo en una era donde la tecnología avanza con tal rapidez.

b) El ámbito de aplicación de la Ley podría abarcar tanto la regulación para aquellos sistemas (bases) de datos personales públicos como privados, o bien sólo para éstos últimos, dejando a las leyes de transparencia o especiales, la regulación para los públicos (en armonía con lo dispuesto por la fracción II del recién reformado artículo 6 constitucional).

c) Debieran preverse los principios de protección de datos personales reconocidos a nivel internacional, tales como el de licitud, calidad, proporcionalidad, consentimiento, finalidad, información y seguridad. De la claridad en las definiciones y alcances de dichos principios, dependerá la operatividad y efectividad de la ley. Tal es el caso del consentimiento del titular de los datos, el cual se erige como la columna vertebral de este nuevo derecho. Las reglas para otorgarlo, obtenerlo o revocarlo en razón de la naturaleza del dato deben ser claras e incluir todos los supuestos.[33]

d) Los Derechos de los titulares de los datos personales deben incluirse de manera contundente y clara como lo son, el de acceso, corrección, cancelación y oposición, así como al recurso ante una autoridad independiente que los tutele de manera eficaz. Como todo derecho encontrará sus límites en la propia norma.
e) La existencia de una autoridad independiente y especializada que garantice la tutela del derecho a la protección de datos, con facultades para sancionar. En este punto puede explorarse la conveniencia de que un mismo órgano se encargue de garantizar el derecho de acceso a la información así como el de protección de datos a nivel nacional, o bien se cree una autoridad distinta e independiente. [34]
f) Por su parte, la ley deberá prever disposiciones para el adecuado tratamiento, confidencialidad y custodia de los datos personales sensibles por los efectos socioeconómicos negativos en el corto y mediano plazo que su liberación no controlada puede ocasionar, por lo que la Ley deberá contemplar el tratamiento diferenciado de datos de acuerdo con su naturaleza y grado de protección que ésta conlleva.
g) Se estima que debiera valorarse la utilidad de la existencia de un Registro de Protección de Datos, ya que con ello se dota al gobernado y a la autoridad de un instrumento general de consulta y control respecto de los datos que los sujetos obligados poseen. Sus requisitos deben ser sencillos para permitir su operatividad.
h) Asimismo, debe preverse un apartado de transferencias internacionales de datos, a efecto de que la protección alcance dentro y fuera del territorio nacional, sin que con ello se vulneren las reglas del derecho internacional,[35] así como mecanismos de cooperación internacional en la materia.

Este trabajo intenta poner sobre la mesa que no estamos frente a un debate cerrado y propone nuevas ópticas de análisis a la problemática de ingeniería jurídica que ocupará un lugar central en la agenda legislativa de nuestro país y sobre todo, en el devenir de la sociedad que se avecina en materia de privacidZad.

Notas

[1] *Memorias del II Congreso Mexicano de Derecho Procesal Constitucional*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México, 2007.

[2] *Vid*. RAWLS, John. *Teoría de la Justicia*, México, Fondo de Cultura Económica 1979, p. 1.

[3] El Código de Hammurabi en la antigua Mesopotamia, las XII Tablas y el denominado *Corpus Iuris Civilis* en Roma, así como el derecho común europeo en la Alta Edad Media, entre otros.

[4] *Vid*. PECES- BARBA, Gregorio. *Derecho positivo de los derechos humanos*, Madrid, Debate, 1987,

[5] *Vid*. BOBBIO, Norberto. *El tiempo de los derechos*, Madrid, Sistema, 1991, p 109.

[6] *Vid*. PECES- BARBA, Gregorio. *Op.cit.*, p 139.

[7] BOBBIO, Norberto. *La herencia de la gran revolución*, Madrid, Sistema, 1991, p.172.

[8] GUERRERO PICÓ, María del Carmen. El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal. Estudios de Protección de Datos. Agencia de Protección de Datos de la Comunidad de Madrid. Thomson Civitas, 2006.

[9] El último reporte sobre Privacidad y Derechos Humanos 2006 del E*lectronic Privacy Information Center (EPIC*), da cuenta de los desarrollos constitucionales, legales y del marco regulatorio en materia de protección a la privacidad en mas de 75 países alrededor del mundo. Ver www.epic.or

[10] Esta afirmación corresponde, entre otros a J. DHONT y M. V. PEREZ ASINARI, *"New Physics and the Law. A comparative Approach to the EU and US Privacy and Data Protection Regulation, looking for Adequate protection"* en Flujos transfronterizos y extraterritorialidad: La postura europea, PUOLET, Ives, Revista Española de Protección de Datos p.112. Julio-Diciembre 2006. Thomson Civitas.

[11]Idem.

[12] http://www.un.org/spanish/aboutun/hrights.htm.

[13] http://www.derechos.org/nizkor/espana/doc/conveudh50.html.

[14] http://www.derechos.org/nizkor/ley/pdcp.html.

[15] http://www.oas.org/juridico/spanish/Tratados/b-32.html.

[16] *Vid.* Piñar Mañas, José Luis. El derecho fundamental a la protección de datos personales, en Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Valencia, 2005, p 20.

[17] *Ibidem*.

[18] *Idem*, pp. 20-21.

19 Vid. ARENAS RAMIRO, Mónica. El derecho fundamental a la protección de datos personales en Europa, Valencia, Tirant lo Blanch, p. 156.

20 ARENAS RAMIRO, Mónica. op. cit., pp. 277-278.

21 PUENTE ESCOBAR, Agustín. Breve descripción de la evolución histórica y del marco normativo internacional de la protección de datos de carácter personal, en Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Valencia, 2005,, p. 43.

22 Idem.

23 Vid. PUENTE ESCOBAR, Agustín. op. cit., p 51.

24 Ibidem.

25 http://www.diputados.gob.mx/LeyesBiblio/decre/LFTAIPG_06jun06.doc.

[26] Artículo 3 fracción II de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

27http://www.ifai.org.mx/pdf/ciudadanos/cumplimiento_normativo/datos_personales/lineamientos_protdaper.pdf.

[28]http://portaltransparencia.gob.mx/pot/marcoNormativo/consultar.do?method=consultar&idMarcoNormativo=39&idDependencia=06738&_idDependencia=06738

[29] Los cambios realizados por la Cámara de Diputados que motivaron el envío del proyecto de decreto de regreso a la Cámara de origen (Senado) son los siguientes: en el primer párrafo de la propuesta se omitió la palabra destrucción y se sustituyó por la expresión "manifestar su oposición". En el segundo párrafo se cambió de posición la palabra público, que anteriormente sólo calificaba a la palabra "interés" para adjetivar las palabras "interés, seguridad y salud" con el calificativo "públicos".

[30] La Comisión Europea ha emitido a la fecha 6 decisiones de nivel adecuado de protección de datos a los siguientes países en orden cronológico: Suiza, Estados Unidos de América (Acuerdos de Safe Harbour), Canadá, Argentina, Guernesy e Isla de Mann.

[31] Entre los puntos a resaltar en la citada Declaración se destaca el identificado con el número 45, que señala lo siguiente: "45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra comunidad. "

[32] Celebrado en noviembre de 2007 en la ciudad de Lisboa, Portugal.

[33] Así por ejemplo, debiera incluirse un doble esquema conocido como el enfoque *opt in- opt out*, por el cual, en el primer supuesto, necesariamente debe obtenerse el consentimiento previo, libre, expreso e informado de su titular para el tratamiento de los datos especialmente protegidos o sensibles como lo son los relativos a la salud, la preferencia sexual, la religión u opiniones políticas; mientras que en el segundo, los datos no sensibles pueden transmitirse con un consentimiento tácito y solo mediante la oposición expresa a que los datos sean utilizados, los usuarios de los mismos estarían impedidos de tratarlos. Lo anterior podría generar beneficios al propio titular como consumidor, así como a la economía en general permitiendo que varios agentes económicos utilicen la información con fines de mercadeo de bienes o servicios.

[34] El primer modelo funciona en países como Reino Unido donde el *Infomation Commissioner* es la misma autoridad para resolver sobre las negativas de acceso a la información así como para velar por la protección de datos personales. Ello tiene la complejidad que conlleva el administrar dos piezas legislativas distintas, pero también puede tener ventajas como el hecho de que una sola autoridad concentre los criterios de apertura y protección evitando posibles conflictos como en el caso francés en el cual, la Comisión de Acceso a Documentos Administrativos (CADA) no en pocas ocasiones se encuentra contrapuesta con la Comisión Nacional de Libertades Informáticas (CNIL). Otra ventaja puede ser el ahorro en los costos de creación institucionales.

[35] En ese sentido, siguiendo la tendencia global de negocios debe preverse la posibilidad de utilizar mecanismos alternativos como los contractuales, así como incluir mecanismos de autorregulación o códigos de conducta de sectores involucrados como las denominadas *"Cross Border Privacy Rules"* entre empresas de la misma familia que llevan a cabo transferencias internacionales de datos, códigos de ética o sellos de confianza que aseguren el adecuado tratamiento de los datos.