

## NÚMERO 64

MARÍA SOLANGE MAQUEO Y JIMENA MORENO

Implicaciones de una ley general en materia  
de protección de datos personales



### Importante

Los Documentos de Trabajo del CIDE son una herramienta para fomentar la discusión entre las comunidades académicas. A partir de la difusión, en este formato, de los avances de investigación se busca que los autores puedan recibir comentarios y retroalimentación de sus pares nacionales e internacionales en un estado aún temprano de la investigación.

De acuerdo con esta práctica internacional congruente con el trabajo académico contemporáneo, muchos de estos documentos buscan convertirse posteriormente en una publicación formal, como libro, capítulo de libro o artículo en revista especializada.

D.R. © 2014, Centro de Investigación y Docencia Económicas A.C.  
Carretera México Toluca 3655, Col. Lomas de Santa Fe, 01210, Álvaro Obregón, México DF,  
México.  
[www.cide.edu](http://www.cide.edu)

[www.LibreriaCide.com](http://www.LibreriaCide.com)

Dirección de Publicaciones  
[publicaciones@cide.edu](mailto:publicaciones@cide.edu)  
Tel. 5081 4003

## Agradecimientos

---

*Nuestro agradecimiento al Dr. Sergio López Ayllón, al Dr. José Roldán Xopa, a la Mtra. Lina Ornelas y a la Mtra. Eileen Matus por compartir sus ideas en materia de protección de datos personales.*

## Resumen

---

*Este documento explora algunas de las implicaciones que de la reciente reforma constitucional respecto de la protección de datos personales. Con esta reforma se introduce el mandato de emitir una ley general que establezca las bases, principios y procedimientos del derecho a la protección de los datos, lo cual trae aparejado facultades concurrentes de la Federación, las entidades federativas y los municipios en la materia. A pesar de las ventajas que esta ley representa, como la simetría del derecho en los tres órdenes de gobierno y la posibilidad de adoptar altos estándares internacionales de protección, también presenta importantes retos. Uno, por supuesto, consiste en el rol de los órganos garantes de las entidades federativas y su relación con el órgano autónomo federal; y, otro, hace referencia a las relaciones de nuestro país con la comunidad internacional. En ese contexto, ponemos especial énfasis en la importancia de que México sea parte de la Convención para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional como precedente para obtener la adecuación europea como país responsable en el tratamiento de datos personales.*

**Palabras clave: Datos personales, Derecho Constitucional, Derechos Humanos, Órgano constitucional autónomo.**

## Abstract

---

*This paper explores the implications of the recent constitutional reform to the right of personal data protection. This reform mandates to enact legislation to establish the basis, principles and procedures underlying the right to data protection. This implies a profound transformation of the way this right will be legally treated throughout the territory of the Mexican Republic. Despite the advantages of this law implies, like symmetry in the regulation in the three governing the federal and state and municipal level, and the possibility of adopting high international standards of protection, there are still serious challenges ahead. One, of course, is the role of the guaranteeing organizations of the states and their relation with the autonomous federal institution. The other challenge concerns these same relations with the members of the international community. In such context, we emphasize the importance of Mexico signing the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol as a precedent to obtain the european adequacy as a responsible country with personal data treatment.*

**Key Words: Personal data, constitutional law, human rights, autonomy agency.**

## Introducción

---

**E**l derecho a la protección de datos personales es una preocupación común de las sociedades modernas. Es en el ámbito de los derechos humanos donde inicia su tutela, a través del desarrollo del derecho a la privacidad o del derecho a la intimidad. Específicamente, la protección del individuo respecto de sus datos constituye un derecho fundamental que ha tenido diversas evoluciones y reflexiones tanto en el ámbito nacional como internacional. Es mediante el derecho internacional y el derecho comparado que se ha canalizado, desde hace varias décadas, la evolución del derecho interno con parámetros internacionales.

Observamos ya en el artículo 12 de la Declaración Universal de los Derechos Humanos, del 10 de diciembre de 1948, la prohibición de injerencias arbitrarias en la vida privada, familiar, domicilio o correspondencia. Asimismo, en el artículo 8 del Convenio para la Protección de los Derechos Humanos y Libertades también se establece el derecho al respeto de la vida privada y familiar, de su domicilio y correspondencia señalando como excepciones la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás.

De igual forma, el artículo 8° del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, adoptado por el Consejo de Europa el 4 de noviembre de 1950 y en vigor a partir de 1953, establece que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos del 16 de diciembre de 1966 y el artículo 11 de la Convención Americana sobre Derechos Humanos del 22 de noviembre de 1969, establecen la protección de la vida privada, familiar, de su domicilio o correspondencia ni de ataques ilegales a su honra o reputación.

Sin embargo, es evidente que esta rama abarca mucho más que el derecho a la intimidad o a la privacidad. El desarrollo tecnológico y el incremento en los flujos de información a nivel internacional no tiene fronteras y el intercambio de información con datos personales a través de las redes electrónicas ha llevado a la comunidad internacional a emitir una serie de regulaciones que tienen como objetivo proteger la información personal en el área de la transferencia de datos a nivel internacional. Queda claro que no existe actividad económica que para el desarrollo de la misma quede exenta de la interacción, explotación, aprovechamiento y transferencia de información personal, de ahí la importancia de proteger a nivel internacional los datos personales (Ornelas, Nuñez, 2010, 134).

En este sentido, observamos la importancia de la protección de datos personales en un mundo globalizado en donde la información personal se ha convertido en un activo fundamental y necesario para el desarrollo y crecimiento de las economías nacionales. Fortalecer el marco normativo nacional para la implementación de los

diversos instrumentos internacionales en esta materia puede ser un factor que fortalezca la integración de bloques comerciales de los que México ya es parte.

Uno de los propósitos fundamentales de la protección de datos de los Estados más desarrollados es su carácter preventivo. Se trata de proteger y evitar que los datos recogidos en un Estado salgan de su territorio sin una legislación específica o con niveles menores de protección (Conde Ortiz, 2005, 49). La intención es tener directrices uniformes de protección para evitar abusos respecto de la información solicitada. De ahí que sea importante que los principios y directrices de la materia se consoliden en el futuro, asegurando la transposición a derecho interno de aquellos principios que si no están incorporados se tomen en cuenta para poder afrontar de manera eficiente la tutela de los datos personales. Pero para que ello ocurra es necesario generar estándares homogéneos en toda la República Mexicana.

La recepción de los principios y bases internacionales en materia de protección de datos personales en nuestro sistema jurídico sólo será viable si se establecen mecanismos que permitan generar niveles de tutela del derecho simétricos en los distintos órdenes de gobierno y en los diversos sectores, tanto públicos como privados.

Así las cosas, el presente trabajo tiene por objeto identificar los retos que presenta la protección de datos personales en nuestro país, dado el contexto internacional y la fragmentación de nuestra legislación interna. Ambas perspectivas convergen en la necesidad de materializar la reforma constitucional de 2014 en la materia a través de la emisión de una Ley General.

Para tales efectos en este documento abordaremos los principales instrumentos internacionales que han servido de antecedente y guía para elaboración de las legislaciones de mayor alcance y protección de la persona respecto de sus datos personales.

A continuación analizaremos la forma en que este derecho fundamental se ha ido construyendo en nuestro sistema jurídico, desde su previsión legislativa, su inclusión en la Norma Fundamental hasta el contenido de la reciente reforma constitucional. Esta última trae aparejada importantes desafíos que tendrán que ser abordados tanto desde la perspectiva de los estándares internacionales hasta la adopción de medidas que sean congruentes con nuestro modelo federalista y con la autonomía de los organismos garantes del derecho en las entidades federativas.

### ***Instrumentos internacionales más relevantes en la protección de datos personales***

A) Convenio Número 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional.

En 1980 se publica la Recomendación de la OCDE sobre el flujo internacional de datos personales y la protección a la intimidad. Esta recomendación sirvió de base para la elaboración del Convenio Número 108 del 28 de enero de 1981, el cual fue redactado por un comité de expertos en la materia con el objetivo de obtener un convenio que desarrollara el artículo 8 del Convenio Europeo de Derechos Humanos y, a su vez, garantizara ciertos principios generales básicos para cualquier tratamiento de datos personales.

A este respecto, cabe mencionar que uno de los principales motivos por los que se decidió redactar un convenio y no un protocolo fue el deseo de que la norma resultante no se limitara al ámbito del Consejo de Europa, sino que existiera la posibilidad de que se adhirieran al mismo países que no fueran miembros.

El Convenio 108 entró en vigor el 1º de octubre de 1985 y los primeros cinco países que lo firmaron fueron Suecia, Francia, Noruega, España y Alemania. El Convenio 108 se conforma de 27 disposiciones divididas en 7 capítulos a través de los cuales se desarrollan reglas generales para establecer fundamentalmente la protección del respeto a la vida privada y simultáneamente la libre circulación de la información. Así, en ésta se establecen objetivos y campos de aplicación, los principios básicos de protección de datos personales, los cuales están orientados a facilitar los flujos transfronterizos de datos personales y la ayuda y cooperación mutua entre las Partes, entre otras cuestiones. “En cuanto al régimen sancionador previsto en el convenio, el artículo 10 remite la adopción del mismo a los Estados Parte. El convenio deja completamente abierta la cuestión relativa no sólo al tipo de sanciones que pueden preverse, sino también al sector jurídico en el que pueden integrarse.” (Da Cunha, 2010, p. 2)

En términos del artículo 1, el objeto y fin del Convenio 108 es garantizar, en el territorio de cada Parte, a cualquier persona física sea cual fuere su nacionalidad o residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de sus datos personales.

Así, a sus 20 años de vigencia y con la incursión de otros instrumentos internacionales en la materia -destacando a este respecto la Directiva 95/46/CE-, trajo como consecuencia natural y necesaria la adaptación de algunas de las disposiciones del Convenio 108 a las nuevas circunstancias de hecho y de derecho existentes.

De esta forma, el 8 de noviembre de 2001 se adoptó un Protocolo Adicional del Convenio Número 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y relativo a Transferencias de Datos, tendente a regular dos aspectos importantes:

- (a) Las transferencias internacionales de datos personales, y
- (b) la obligación a cargo de los Estados signatarios de contar con una autoridad independiente, cuya función principal sea velar por el cumplimiento de las disposiciones nacionales aplicables en materia de protección de datos personales.

B) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.

Esta Directiva tiene como objetivo general otorgar mayor protección de los datos personales de las personas e incrementar su flujo para transacciones económicas, comerciales, y el fortalecimiento del intercambio de información científica y técnica. Asimismo, establece los principios básicos para que las legislaciones nacionales tengan los mismos niveles de protección de datos personales que fluyen de un Estado a otro, garantizando en todo momento la protección de este derecho fundamental. Inclusive establece que cuando un país tercero no ofrezca niveles de protección adecuados debe prohibirse la transferencia de datos personales y los Estados adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate. Existen excepciones y se dan cuando el interesado haya dado su consentimiento, sea necesario para la celebración o ejecución de un contrato, sea necesaria para la salvaguardia de un interés público o en defensa en un procedimiento judicial o para el interés vital del individuo.

En ese sentido esta Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección aceptable; el carácter adecuado del nivel ofrecido de protección de un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias, en particular se tomará en cuenta la naturaleza de los datos, la finalidad y la duración del tratamiento previsto, las normas de derecho y las medidas de seguridad en vigor. Los Estados miembros se informarán en el caso en que un tercer país no garantice el nivel de protección adecuado. De ahí la importancia de tomarla en consideración, toda vez que si bien México no es parte de la Unión Europea, esta Directiva podría afectar sus relaciones económicas con países miembros.

En esta Directiva se deja ver cómo los datos no son propiedad de quien los posee, sino del titular, es decir, sólo el titular de la información tiene derecho a decidir la manera en cómo se presentan y se abandona la distinción formal entre las normas aplicables al sector público y privado (Conde Ortiz, 2005). El derecho a tutelar es el derecho a la vida privada, sin embargo, también se genera la protección de intereses del Estado para proteger la información más allá de la frontera comunitaria. Amplía los principios ya recogidos en otros instrumentos internacionales e impide la creación de barreras para la circulación de los datos personales en todos los Estados miembros de la Unión Europea a través del establecimiento de niveles de protección de los derechos y libertades de las personas en cuanto a que la protección de sus datos de carácter personal debe ser equivalente en todos los Estados miembros. De esta forma, como señala Da Cunha (2010, p. 4), “[l]a Directiva pretende facilitar la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.”

C) Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal (Resolución de Madrid), 5 de noviembre de 2009.

Este documento ha sido el resultado del trabajo de un Grupo de Trabajo liderado por la Agencia Española de Protección de Datos establecido a raíz de la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad que intenta conjuntar



legislaciones de los cinco continentes. En palabras de Artemi Rallo, Director de la Agencia Española de Protección de Datos, “[s]u carácter consensuado aporta dos valores añadidos esencialmente novedosos: de un lado enfatiza la vocación universal de los principios y garantías que configuran este derecho; del otro, reafirma la factibilidad de avanzar hacia un documento internacionalmente vinculante, que contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizando por las transferencias internacionales de información”.

Esta resolución ofrece un conjunto de principios, derechos, obligaciones y procedimientos que cualquier sistema jurídico de protección de datos y privacidad debe alcanzar. Así, el tratamiento de datos personales en el sector público o privado se deber llevar a cabo a través de un enfoque más uniforme a nivel internacional y considera el derecho a la protección de datos personales y de privacidad un derecho fundamental de las personas, independientemente de su nacionalidad o residencia.

Esta resolución tiene por objeto definir principios y derechos que garanticen la protección de la privacidad a nivel internacional en relación con los datos personales y facilitar el flujo internacional de los mismos, ya indispensables en un mundo globalizado y se aplica tanto al sector público como el privado.

Establece diversos principios:

a) Principio de lealtad y legalidad.- señala que el tratamiento de datos de carácter personal debe realizarse respetando la legislación nacional aplicable y los derechos y libertades de las personas de conformidad con la Declaración Universal de los Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos.

b) Principio de finalidad.- el cual indica que el tratamiento de los datos personales debe limitarse al cumplimiento de la finalidad para la cual fueron solicitados.

c) Principio de proporcionalidad.- el tratamiento de los datos personales debe ser adecuado y no excesivo en relación con la finalidad para lo cual fueron solicitados.

d) Principio de calidad.- los datos personales deberán ser exactos, completos y actualizados para el cumplimiento de su objetivo. El periodo de conservación de los datos deberá ser el mínimo necesario y cuando hayan dejado de ser necesarios deberán ser cancelados o convertidos en anónimo.

e) Principio de transparencia.- Deberán contar con políticas transparentes en el tratamiento de datos personales, los responsables deberán informar acerca de su identidad, de la finalidad para la que pretende realizar el tratamiento, de los destinatarios a los que prevé ceder los datos de carácter personal, entre otros. Además, la información debe ser inteligible, empleando un lenguaje sencillo y claro.

f) Principio de responsabilidad.- la persona responsable que maneje datos (persona física o jurídica, pública o privada) deberá de tomar las medidas necesarias para cumplir con los principios y obligaciones establecidos en este protocolo.

g) Principio general de legitimación.- se establece como regla general que para la obtención de los datos personales debe haber consentimiento libre, inequívoco e informado del interesado, cuando se justifique el tratamiento de los datos por la persona responsable, cuando el tratamiento sea preciso para el cumplimiento de una relación jurídica o de un mandato de ley.

D) Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC).

México es país miembro del APEC desde 1993, su inclusión tuvo como objetivo diversificar los vínculos económicos con Asia-Pacífico. Los países miembros firmaron el Marco de Privacidad cuyo principal objeto es por un lado, establecer normas efectivas de protección a la privacidad para evitar barreras a los flujos de información y por el otro incrementar el comercio electrónico y la economía en la región.

El incremento en el comercio electrónico ha llevado a los países a ajustar y crear medidas de seguridad específicas para dar confianza al consumidor en la protección sus datos. Las tecnologías de la información y de comunicación ofrecen grandes beneficios económicos a los gobiernos, empresas e individuo y su desarrollo es inminente de ahí la necesidad de desarrollar sistemas para proteger la privacidad de la información.

En este instrumento se establecen principios de privacidad fundamentales entre los que destacan la prevención de daño en el mal uso de la información proporcionada, el aviso de privacidad indicando el uso que se le va a dar a la información, la limitación en la recolección de la información, es decir que la información que se requiera sea proporcional al propósito de su uso, la obligación de que los tenedores de la información manejen estándares de seguridad homogéneos entre los miembros para resguardar la información, etc. Este Marco aplica a personas y organizaciones de los sectores público y privado que controlan la recolección, posesión, procesamiento, transferencias y revelación de la información personal.

E) Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana (2003).

Derivada de la Cumbre Iberoamericana de Jefes de Estado y de Gobierno llevada a cabo en Santa Cruz de la Sierra, Bolivia en 2003 se creó un Grupo de Trabajo para la elaboración de una propuesta cuyo objeto sea contribuir a las iniciativas regulatorias de la protección de datos personales que surjan en la Comunidad Iberoamericana, para garantizar que el desarrollo del comercio a nivel mundial sea compatible con la protección de la información de las personas. Señalan que la protección de datos personales es un derecho fundamental de las personas.

Dichas directrices van en armonía con los estándares de la OCDE, la Resolución 45/95 de la Asamblea General de las Naciones Unidas del 14 de diciembre de 1990 en donde se enumeran una serie de principios en materia de protección de datos personales de aplicación mundial como garantía mínima de protección.

En estas directrices se establecen criterios de armonización entre los Estados Iberoamericanos que reconocen, ya sea por referencia directa de su Constitución, como consecuencia de las decisiones tomadas por los órganos judiciales el derecho de la persona a la protección de sus datos personales esencialmente mediante el reconocimiento del recurso al *habeas data*.

Asimismo, se establecen los principios, derechos y obligaciones que deberá contener una Ley nacional de protección de datos de carácter personal. Estas directrices se aplican a todo tratamiento manual o automatizado de datos de carácter personal y serán aplicables a los tratamientos que lleven a cabo todas las entidades de los sectores públicos y privados. Se establecen los principios relacionados con la finalidad y calidad de los datos,

de legitimación para el tratamiento, de transparencia, los derechos de acceso, rectificación y cancelación de los interesados (derecho Arco), de seguridad y confidencialidad entre otros.

### *La recepción del derecho a la protección de datos en México*

Dado el contexto internacional, México ha dado pasos importantes en la recepción del derecho a la protección de datos personales en nuestro sistema jurídico. No obstante, parte de los retos que afronta actualmente este derecho en nuestro país, se explica por la forma gradual y diferenciada en que éste se ha venido conformando normativamente.

Al respecto, cabe recordar que el derecho a la protección de datos personales, antes de elevarse a rango constitucional, ya se encontraba previsto tanto en la legislación federal, a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, como en el ámbito jurídico estatal.

En su texto original, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2002, establecía como uno de sus objetivos: “[g]arantizar la protección de los datos personales en posesión de los sujetos obligados” (artículo 4, fracción III). Para tal efecto, la citada Ley contemplaba los deberes de los sujetos obligados para recabar y tratar los datos personales, así como para permitir el ejercicio de los derechos de acceso y rectificación de los titulares de los datos (Capítulo IV del Título I de la Ley), siendo el entonces recién creado Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), el órgano garante de la protección de los datos personales en poder de las dependencias y entidades de la Administración Pública Federal (artículo 33). No obstante, a pesar de su protección legislativa, los datos personales en posesión de otros poderes del Estado o, incluso, de los órganos constitucionales autónomos, quedaban excluidos del ámbito competencial del IFAI. Además, como puede observarse, la citada Ley sólo contemplaba, de manera tímida, los derechos de acceso y rectificación de datos personales sin incluir los de oposición y cancelación del titular de los mismos.

Por su parte, las entidades federativas tuvieron un tratamiento normativo diferenciado del derecho a la protección de los datos personales. Mientras que algunas adoptaron el mismo esquema federal que incorpora el derecho en la ley de transparencia y acceso a la información; otras, como es el caso del Estado de Colima<sup>1</sup>, desarrollaron una legislación especial en la materia (esto es, contemplando el derecho a la protección de los datos personales en un cuerpo normativo distinto al de la transparencia y el acceso a la información) con un ámbito de protección más amplio – que incluso llegaba a incorporar los datos en posesión del sector privado–.

Posteriormente, en el año 2007<sup>2</sup> el derecho a la protección de datos personales se introduce de manera expresa en la Constitución Política de los Estados Unidos

---

<sup>1</sup> En concreto nos referimos a la Ley de Protección de Datos Personales del Estado de Colima, publicada en el Suplemento No. 1 del Periódico Oficial “El Estado de Colima”, núm.27, el 21 de junio de 2003.

<sup>2</sup> Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el 20 de julio de 2007.

Mexicanos mediante la modificación al artículo 6º, párrafo segundo, para quedar como sigue:

Artículo 6o.- [...]

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

[...]

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.

[...]

Sin embargo, dada su ubicación, podría considerarse que su inclusión en el texto constitucional obedeció más que al establecimiento de un derecho humano específico (diferenciado del derecho a la intimidad y a la privacidad), a la necesidad de establecer un límite constitucional al ejercicio del derecho de acceso a la información pública gubernamental, así como para imponer ciertas restricciones a las autoridades respecto del tratamiento de los datos personales.

No es sino hasta el año 2009, con la reforma a los artículos 16 y 73 fracción XXIX-O de la Constitución Política de los Estados Unidos Mexicanos que la protección de datos personales se introduce como un verdadero habeas data<sup>3</sup>. En términos del Dictamen de primera lectura por las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos de la Cámara de Senadores, con esta reforma “se asegura el derecho a la protección de datos personales a nivel nacional, extendiendo su aplicación a todos los niveles y sectores [...]”. Así, con esta propuesta se incluye de un modo explícito el derecho de toda persona a la protección de sus datos personales en una nueva dimensión que supone el “derecho a la autodeterminación informativa” (Basterra, 2008, p. 26), esto es, “el derecho de libertad informática o control de los datos personales” (Conde, 2012, p. 27).

En este sentido, la reforma de 2009 establece el derecho humano a la protección de los datos personales y sus correlativos derechos de acceso, rectificación, cancelación y oposición, mismos que no sólo se harán valer ante las autoridades gubernamentales en cualquiera de sus órdenes de gobierno, sino, además, ante los propios particulares que se encuentren en posesión de de datos personales.

Con base en estas reformas constitucionales, un año después, se expide por el Congreso de la Unión la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación el 5 de julio de 2010, así como su Reglamento, publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011.

---

<sup>3</sup> El habeas data se define como un recurso mediante el cual la persona titular del derecho puede tener conocimiento de los datos referidos y de la finalidad para la que están siendo tratados por un determinado responsable del tratamiento, pudiendo en su caso rectificar, cancelar o actualizar sus datos (Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, 2003).

De acuerdo con todo lo anterior, las diversas legislaturas estatales se dieron a la tarea de adecuar su normatividad al marco constitucional en la materia. De tal forma que mientras algunas disposiciones legales estatales quedaron derogadas -como en el caso de los estados de Colima, Jalisco, Querétaro y Tlaxcala (Piñar y Recio, 2013, p. 12)-, por lo que hace a la protección de datos personales en posesión de las personas físicas o morales de carácter privado, otras fueron de reciente creación.

No obstante los problemas que afronta el derecho a la protección de datos personales en nuestro sistema jurídico se hicieron patentes. Por una parte, estamos ante un problema de dispersión normativa que se manifiesta tanto en las diferencias entre el sector público y el sector privado, como entre el propio sector público en los diversos órdenes de gobierno. Mientras que el sector privado se rige por disposiciones de carácter federal, con validez en toda la República Mexicana, el sector público se encuentra escindido en disposiciones tanto de carácter federal como estatal. A todo lo cual se añade la diferenciación de ordenamientos en los que se regula el derecho a la protección de los datos. En algunos casos, algunas entidades federativas, como en el Distrito Federal, el Estado de México, Guanajuato, Oaxaca, entre otros, se emitieron leyes especiales en materia de protección de datos para el sector público. En otros casos, como en Aguascalientes y Coahuila y la propia Federación, se mantiene el derecho, con ciertas adecuaciones, en la legislación correspondiente a la materia de transparencia y acceso a la información pública gubernamental.

Todo lo cual redundando en la diferenciación de órganos garantes del derecho fundamental y en la dispersión de atribuciones de contenido y alcance diferenciado. Una complicación adicional deviene del carácter transversal de la protección de datos personales, toda vez que involucra a los diversos sectores públicos relacionados (esto es, salud, educación, energía, financiero, telecomunicaciones, etc.).

Ante esta situación, que denota competencias diferenciadas y, con ello, un nivel de tutela del derecho fundamental asimétrico, conviene cuestionarse sobre la necesidad de homologar criterios. Como en su momento cuestionaron López Ayllón y Marván Laborde (2007, p. 32), “¿Debe haber 32 leyes de datos personales o una ley general aplicable a toda la federación?, o ¿se debe desarrollar el tema en el conjunto de leyes de transparencia sin esperar una nueva legislación?” Si bien estas interrogantes se produjeron con ocasión de la reforma constitucional de 2007 antes comentada, la necesidad de su resolución ha cobrado vigencia con la reciente publicación del Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, publicado en el Diario Oficial de la Federación el 7 de febrero de 2014, todo lo cual se refuerza por la dimensión del habeas data tras la reforma constitucional de 2009 y, por supuesto, con la reforma constitucional en materia de derechos humanos de 2011<sup>4</sup>, que incorpora el control de convencionalidad, el principio por persona y los deberes del Estado, en cualquiera de sus órdenes de gobierno y en el marco de sus competencias para promover, respetar, proteger y garantizar los derechos humanos.

---

<sup>4</sup> Decreto por el que se modifica la denominación del Capítulo I del Título Primero y reforma diversos artículos de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el 10 de junio de 2011.

## La reforma constitucional de 2014

Entonces, en el marco de la reciente reforma constitucional del presente año, nuestra Norma Fundamental establece los siguientes aspectos relevantes para el tema que nos ocupa:

1. En primer lugar se transforma la naturaleza jurídica del Instituto Federal de Acceso a la Información Pública y Protección de Datos, así como de sus homólogos en los Estados de la República y el Distrito Federal. En todos los casos se establece su condición de órganos constitucionales autónomos, esto es, independientes de los tres poderes tradicionales y con autonomía técnica, de gestión y presupuestaria y con personalidad jurídica y patrimonio propios. De tal forma que estos órganos se constituyen en organismos autónomos especializados responsables de garantizar la protección de datos personales.

2. Se legitima al órgano constitucional autónomo garante, la facultad para promover acciones de inconstitucionalidad, en contra de leyes de carácter federal, estatal y del Distrito Federal, así como de tratados internacionales de los que México sea parte, que vulneren el derecho a la protección de datos personales.

De igual forma se dota de esta facultad para promover acciones de inconstitucionalidad a los organismos garantes de las diversas entidades federativas, en contra de las leyes expedidas por sus respectivas legislaturas locales y, en su caso, por la Asamblea Legislativa del Distrito Federal (artículo 105, fracción I, inciso h).

En consonancia con lo anterior, se establece la procedencia de controversias constitucionales tratándose de conflictos competenciales entre dos órganos constitucionales autónomos, y entre uno de éstos y el Poder Ejecutivo de la Unión o el Congreso de la Unión sobre la constitucionalidad de sus actos o disposiciones generales. Siendo aplicable lo anterior al caso del nuevo órgano constitucional autónomo garante de la protección de los datos personales (artículo 105, fracción I, inciso l).

3. De igual forma, de manera consistente con la nueva naturaleza autónoma de los órganos garantes del derecho a la protección de datos personales, se establece la posibilidad de que sus miembros sean sometidos a juicio político (artículo 110, párrafos primero y segundo) y a la delcaración de procedencia por la comisión de delitos (artículo 111, párrafos primero y quinto).

4. Se amplía el abanico de los sujetos obligados por la legislación en materia de transparencia y acceso a la información pública, siendo esto aplicable también a los responsables en materia de protección de datos personales.

En consecuencia, los sujetos obligados por el artículo 6° constitucional, se extiende a “los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona, física, moral o sindicatos, que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal; con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros.” (artículo 6°, apartado A, fracción VIII, párrafo cuarto de la Constitución Política de los Estados Unidos Mexicanos).

5. Se expresa la obligación por parte de la Federación, los Estados y el Distrito Federal de establecer “procedimientos de revisión expeditos que se sustanciarán ante los organismos autónomos especializados e imparciales” a los que se refiere la Constitución (artículo 6o., apartado A, fracción IV). Con ello se pretende homologar la existencia de un recurso administrativo para los particulares ante los propios organismos garantes del derecho.

6. Se faculta al órgano constitucional autónomo de carácter nacional para conocer “de los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de los estados y el Distrito Federal que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley” (artículo 6o., apartado A, fracción VIII, párrafo cuarto de la Constitución).

De este precepto constitucional se desprende que el recurso de revisión ante el órgano garante nacional respecto de las resoluciones emitidas por los demás organismos autónomos locales podría proceder tanto en materia de acceso a la información como en materia de protección de datos personales, no sólo porque introduce aquellas resoluciones relativas a la confidencialidad (siendo uno de los ejes rectores de la protección de datos personales), sino además porque el término “información” abarca tanto a la información pública gubernamental como a cualquier información concerniente a una persona física, identificada o identificable.

7. Se establece para el órgano constitucional autónomo de carácter nacional la facultad de atracción para conocer, “de oficio o a petición fundada del organismo garante equivalente del estado o del Distrito Federal” de los recursos de revisión que por su interés y trascendencia así lo ameriten (artículo 6º., apartado A, fracción VIII, párrafo quinto). Como puede observarse de este precepto, la facultad de atracción queda en términos muy abiertos, por lo que su alcance y configuración estará sujeto a lo que disponga la ley reglamentaria.

8. En principio, las resoluciones del órgano constitucional autónomo serán vinculatorias, definitivas e inatacables para los sujetos obligados (artículo 6º., apartado A, fracción VIII, párrafo séptimo). No obstante, el Consejero Jurídico del gobierno podrá interponer recurso de revisión ante la Suprema Corte de Justicia de la Nación en los términos que establezca la ley, cuando se trate de resoluciones que puedan poner en peligro “la seguridad nacional” (artículo 6º, apartado A, fracción VIII, párrafo séptimo).

9. Se establece la obligación de todas las autoridades y servidores públicos para coadyuvar con el órgano constitucional autónomo (artículo 6º, apartado A, fracción VIII, párrafo décimo quinto). De acuerdo con el Dictamen aprobado por la cámara de origen en el proceso de reforma constitucional, con esta obligación se hace patente en la norma constitucional que aun cuando el organismo autónomo no pertenezca a la administración pública federal, las autoridades de ésta (así como de las entidades federativas en el ámbito de su competencia), deben estar en aptitud de proporcionar todo el auxilio y apoyo que requiera, todo lo cual se complementa con el sistema de

coordinación a que se refiere la propia Norma Fundamental (artículo 6°, apartado A, fracción VIII, párrafo décimo sexto).

10. El Constituyente Permente faculta al Congreso de la Unión para emitir una ley general que establezca las bases, principios generales y procedimientos del ejercicio del derecho a la protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales en todos los niveles de gobierno (artículo 73, fracción XXIX-S).

En el dictamen aprobado por la Cámara de Senadores como cámara de origen, se precisa la existencia de dos tipos de leyes: “una federal que será la que rijas las actividades del órgano garante federal, y una general que normará y unificará los procedimientos en todos los organismos garantes de los Estados y el Distrito Federal” (Dictamen de las Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos Primera; de Gobernación y de Anticorrupción y Participación Ciudadana en Materia de Transparencia, p. 266). Lo anterior se corrobora en el Decreto de reforma constitucional en el artículo segundo transitorio que establece la obligación del Congreso de la Unión para expedir la Ley General, así como las reformas que correspondan a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, a la Ley Federal de Datos Personales en Posesión de los Particulares, entre otros procedimientos.

En ese sentido pareciera que la reforma constitucional establece la existencia de, por lo menos, tres leyes en materia de protección de datos personales: Una ley federal (que puede o no coincidir con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental), una Ley General (que puede o no estar en la Ley General de Transparencia y Acceso a la Información) y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. A todo lo cual se añade la normatividad en el ámbito público de cada entidad federativa (que puede o no tener leyes especiales en la materia o refundirlas en la legislación de transparencia y acceso a la información). Así, el problema de la dispersión normativa y la falta de claridad en la disociación del derecho a la protección de datos personales y el acceso a la información pública continua siendo una tarea pendiente.

Por otra parte, cabe advertir que en el citado artículo segundo transitorio se establece el plazo de un año contado a partir de la fecha de publicación del Decreto para que el Congreso de la Unión emita dicha Ley General y adecúe la normatividad federal a la reforma constitucional. No obstante, el artículo quinto transitorio establece el mismo plazo para que las legislaturas locales hagan lo propio respecto de su propia normatividad, lo cual resulta incomprensible si tomamos en consideración que aún no hay una Ley General y que puede tardar un año su emisión. De tal forma que podría darse el caso de que las entidades federativas se vean obligadas a emitir una reforma a sus respectivas Constituciones y leyes de acuerdo con la Constitución Política de los Estados Unidos Mexicanos sin que aún se haya expedido la Ley General por el Congreso de la Unión para cumplir con el plazo constitucional.



## Implicaciones de una nueva Ley General en materia de protección de datos

### A) En el ámbito nacional

De todo lo anterior, podemos colegir que el órgano garante constitucional del derecho a la protección de datos personales presenta un desdoblamiento de funciones: (1) Por una parte es un órgano “federal”, cuyo ámbito de competencia se extiende a los sujetos obligados de carácter federal y, en su caso, a los responsables de datos personales del sector privado de conformidad con la LFPDPPP (esto es, en el supuesto de que no se cree una nueva entidad encargada de la protección de los datos personales en posesión de los particulares), y (2) Por otra parte se constituye en un verdadero órgano de carácter “nacional”, cuyas potestades están dirigidas a garantizar la efectividad del derecho humano a la protección de datos personales, toda vez que tiene la capacidad de intervenir tanto en el orden jurídico federal como estatal. Este último aspecto se manifiesta tanto en las facultades que le otorga la Constitución para ejercer el recurso de revisión de las resoluciones de los organismos autónomos especializados de las entidades federativas, como en su facultad de atracción. Precisamente esta segunda dimensión de las facultades del órgano constitucional autónomo es la que trae aparejada la necesidad de crear una Ley General cuyo objetivo, en términos de la propia Constitución, consiste en establecer “las bases, principios generales y procedimientos del ejercicio de este derecho.”

De esta forma, mediante una Ley General, se pretende implementar un piso mínimo que establezca la simetría en el ejercicio del derecho en cualquier orden de gobierno que garantice su plena efectividad.

Sin embargo, la reciente reforma constitucional no precisa a qué tipo de Ley General nos referimos.

Al respecto, cabe recordar que en nuestro sistema jurídico no tenemos un común denominador o tipología específica por lo que hace a las leyes generales. Sólo a manera de ejemplo baste citar tres casos: (1) la Ley General de Sociedades Mercantiles, que desarrolla una materia de carácter federal que no introduce propiamente una concurrencia entre los diversos órdenes de gobierno ni se trata de una ley materialmente emanada del texto constitucional. Probablemente, como lo hace notar el Ministro Cossío (2008, p. 873), este caso puede tratarse de un simple error de nomenclatura; (2) la Ley General de Salud o la Ley General de Educación, que suponen una competencia delegada en la Constitución para la determinación de la concurrencia y, por ende, distribuyen competencias entre los diversos órdenes de gobierno (Cossío, p. 874) y que, además, desarrollan materialmente el contenido constitucional del derecho a la protección de la salud y del derecho a la educación; y (3) la Ley General del Sistema Nacional de Seguridad Pública o la Ley General de Protección Civil, que no distribuyen competencias entre los órdenes de gobierno, sino que ponen especial énfasis en la organización de los sistemas de coordinación sobre las facultades constitucionalmente concurrentes.

No obstante lo anterior, nuestro más Alto Tribunal ha adoptado un sentido tradicional de ley general que si bien se adecúa a la distribución de competencias en materias de carácter concurrente, esto es, que competen a los tres órdenes de gobierno, previene de evitar vaciar de contenido a las competencias legislativas de carácter estatal en la

materia. Al respecto, la jurisprudencia de la Corte señala de manera textual lo siguiente:

**LEYES LOCALES EN MATERIAS CONCURRENTES. EN ELLAS SE PUEDEN AUMENTAR LAS PROHIBICIONES O LOS DEBERES IMPUESTOS POR LAS LEYES GENERALES.**

Las leyes generales son normas expedidas por el Congreso de la Unión que distribuyen competencias entre los distintos niveles de gobierno en las materias concurrentes y sientan las bases para su regulación, de ahí que no pretenden agotar la regulación de la materia respectiva, sino que buscan ser la plataforma mínima desde la que las entidades puedan darse sus propias normas tomando en cuenta su realidad social. Por tanto, cumpliendo el mínimo normativo que marca la Ley general, las leyes locales pueden tener su propio ámbito de regulación poniendo especial énfasis en determinados aspectos que sean preocupantes en una región específica. Si no fuere así, las leyes locales en las materias concurrentes no tendrían razón de ser, pues se limitarían a repetir lo establecido por el legislador federal, lo que resulta carente de sentido, pues se vaciaría el concepto mismo de concurrencia.

En este sentido, las entidades federativas pueden aumentar las obligaciones o las prohibiciones que contiene una ley general, pero no reducirlas, pues ello haría nugatoria ésta.

[J]; 9ª. Época; Pleno; S.J.F. y su Gaceta; Tomo XXXI, febrero de 2010; p. 2322.

Adicionalmente, cabe mencionar que el Dictamen aprobado por la cámara de origen de la multicitada reforma constitucional contempla un apartado que hace referencia al contenido mínimo de la Ley reglamentaria del artículo 6º constitucional. Si bien es cierto que esta propuesta no tiene un carácter vinculante para el Congreso de la Unión en uso de su facultad delegada para emitir una Ley General, pues no forma parte del Decreto aprobado por el Constituyente Permanente, reviste una importancia fundamental pues nos permite vislumbrar cuál es la posición de algunos de nuestros legisladores.

La propuesta en comento establece que la Ley General deberá comprender, entre otras cosas: la definición exhaustiva de los sujetos obligados, el ámbito de aplicación de la ley, las autoridades federales y locales; la competencia de los órganos garantes federales y locales o del Distrito Federal y municipales o delegacionales, la integración y funcionamiento, así como coordinación y desgloses respectivos; integración y mecánica de nombramientos de los integrantes de los órganos garantes, los requisitos de elegibilidad y perfiles requeridos; duración del cargo del presidente, incompatibilidad, mecanismos de renuncia, suplencia entre otros; los mecanismos de coordinación y auxilio de autoridades; el procedimiento de segunda instancia, mediante el recurso de revisión ante el IFAI, indicando plazos, notificaciones, requerimiento y resolución; supuestos para la procedencia del ejercicio de la facultad de atracción del órgano garante federal, siendo los criterios el interés general, los asuntos relevantes y los asuntos donde exista una contradicción de criterios; procedimiento, legitimación y personería de los organismos

garantes federales y locales en casos de acciones de inconstitucionalidad; juicio político y declaratoria de procedencia; y específicamente en materia de protección de datos personales en posesión de autoridades, “deberá establecerse un apartado especial que considere el tratamiento de datos personales en posesión de autoridades, en el cual se establezcan los parámetros bajo los cuales se debe proteger este derecho y las versiones públicas que los contengan” (p. 219).

De esta forma, como puede observarse, aún la propuesta de contenido de la Ley General sigue sin resolver a qué tipo de ley general hace referencia nuestra Norma Fundamental.

No obstante, el texto constitucional nos permite establecer ciertos parámetros que dirigirían el contenido de la ley reglamentaria, con base en los objetivos perseguidos:

(1) Por una parte se busca la creación de criterios uniformes que permitan brindar certeza y seguridad jurídica a los titulares de datos. Tratándose de un derecho fundamental es necesario uniformar los principios y criterios que deberán regir las relaciones jurídicas de los sujetos regulados que tratan datos personales con los particulares, tales como los principios de licitud, consentimiento, información, calidad, finalidad, lealtad y proporcionalidad, así como “la expectativa razonable de privacidad, las medidas proactivas de cumplimiento, el principio de responsabilidad” (Piñar y Recio, 2013, p. 12), entre otros. Ello, para evitar disparidades en los niveles de protección del derecho fundamental y, a su vez, orientar la función tanto de los sujetos obligados como de los organismos garantes del derecho.

(2) No debemos olvidar, como lo ha puesto de manifiesto Roldán Xopa, que la protección de datos personales comprende un conjunto de atribuciones que adoptan un “carácter transversal”, en el sentido de que incluyen cualquier materia o sector que implique el tratamiento de datos personales. En este sentido, existe una convergencia o “zona de encuentro”, como él le llama, tanto de autoridades federales, estatales y municipales, como de autoridades dentro de un mismo orden de gobierno en sectores diferenciados. A manera de ejemplo podríamos considerar el caso del sector salud, donde los órganos garantes de la Federación y las entidades federativas convergen con las diversas autoridades sanitarias.

En este sentido, la ley reglamentaria debe comprender ciertos parámetros que dirijan el proceso de diseño normativo y las decisiones administrativas en los distintos sectores y en los distintos órdenes de gobierno. Para ello es necesario definir, primeramente, en la ley cuál será el papel del órgano constitucional autónomo y de los demás organismos autónomos especializados frente a los reguladores sectoriales para definir criterios, interpretaciones y mejores prácticas.

(3) Dado que la protección de datos personales conlleva diversos procedimientos, tanto administrativos como jurisdiccionales, es necesario estandarizar ciertos elementos que garanticen el debido proceso y homologuen el ejercicio del derecho por parte de los titulares de datos.

En principio, la propia Constitución ya establece la necesidad de que en cada orden de gobierno se establezcan tanto los procedimientos de acceso, rectificación,

cancelación y oposición, así como un recurso de revisión llevado ante los órganos garantes del derecho.

Sin duda una cuestión delicada la conforma la posibilidad de que las decisiones de los organismos garantes especializados locales sean recurribles ante el órgano constitucionalmente autónomo. Si bien esta cuestión pudiera favorecer la estandarización de los criterios e interpretaciones en la protección del derecho, lo cierto es que supone una intromisión en las decisiones de los organismos autónomos locales e indirectamente de los servidores públicos responsables de datos personales. En principio, no queda claro cuál es el alcance de este recurso de revisión por el órgano constitucional autónomo en el texto constitucional, pero sin duda alguna lo convierte en una especie de tribunal de segunda instancia.

(4) En consonancia con lo anterior es necesario establecer las bases para el ejercicio de las acciones de inconstitucionalidad y la promoción de controversias constitucionales ante la Suprema Corte de Justicia de la Nación.

(5) La ley reglamentaria debe prever, pues deviene de manera directa del texto constitucional, la facultad de atracción del órgano garante federal. De esta forma, es necesario especificar los alcances de esta facultad por lo que hace a la definición de los supuestos de procedencia. Al respecto, se debe tener presente que esta facultad sólo es procedente cuando aún no existe una resolución definitiva por parte de los organismos autónomos especializados de las entidades federativas, pues como se especifica en el texto constitucional la facultad de atracción procede antes o durante el recurso de revisión.

Ya la Suprema Corte de Justicia de la Nación ha sentado jurisprudencia por lo que se refiere a la “importancia y trascendencia” para el ejercicio de la facultad de atracción por parte del propio Tribunal. Sobre el particular señala lo siguiente:

**FACULTAD DE ATRACCIÓN. LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN PUEDE EJERCERLA A EFECTO DE INTEGRAR JURISPRUDENCIA SOBRE UN PROBLEMA QUE IMPLICA EL ANÁLISIS DE DIVERSOS PRECEPTOS CONSTITUCIONALES Y LEGALES.**

Los requisitos de importancia y trascendencia para el ejercicio de la facultad de atracción se satisfacen cuando se solicita para integrar jurisprudencia por reiteración, y la problemática planteada implica el análisis e interpretación de diversos preceptos constitucionales y legales, ya que en tal supuesto, dicho ejercicio entrañaría la fijación de un criterio jurídico trascendente para casos futuros. Lo anterior es así, pues en atención al principio de legalidad, la jurisprudencia debe formularse con un grado suficiente de determinación que permita saber la conducta ordenada o prohibida, así como las consecuencias de su inobservancia, ya que de otro modo el objeto de vincular a las autoridades en el cumplimiento de la ley sería inalcanzable, pues la garantía de certeza se fundamenta en el principio de legitimación democrática.

[J]; 9ª. Época; Primera Sala; S.J.F. y su Gaceta; Tomo XXXIV, septiembre de 2011; p. 489.

Si bien es cierto que esta jurisprudencia hace referencia a la facultad de atracción conferida a este Alto Tribunal, lo cierto es que es trasladable, en la parte conducente, a la nueva facultad que se le confiere al órgano constitucional autónomo. De tal forma que el análisis y la interpretación de algún precepto constitucional o legal que entrañe la fijación de un criterio jurídico relevante que dote de certeza tanto a los sujetos obligados como a los titulares de derecho, permite justificar el ejercicio de esta facultad de atracción por el órgano constitucional autónomo.

(6) Prever facultades análogas para los órganos garantes del derecho tutelado para emitir medidas de apremio.

(7) Finalmente, del texto constitucional se desprende la necesidad de incluir en la ley reglamentaria los mecanismos de coadyuvancia y coordinación entre todos los servidores públicos de los distintos órdenes de gobierno. Tanto de las autoridades sectoriales en relación con los organismos autónomos garantes del derecho, como entre los propios organismos autónomos. Cabe advertir que esta posibilidad abre las puertas para la creación de un sistema nacional que promueva la articulación de las relaciones funcionales entre las dependencias, entidades, órganos e instituciones del sector público en los tres órdenes de gobierno, así como la participación de la sociedad en general.

Entonces, a pesar de que la Norma Fundamental establece estos parámetros, consistentes con los objetivos a los que obedeció la reforma constitucional del presente año, quedan varios aspectos aún sin resolver y que seguramente tendrán que ser tratados por nuestros legisladores. Sin pretender ser exhaustivas, cabe mencionar los siguientes: (1) la conveniencia de la homologación del diseño institucional de los organismos garantes del derecho, para lo cual es necesario tener presente que nuestro sistema jurídico “no reconoce un mismo tipo de autonomía constitucional” (Dictamen aprobado por la Cámara de Senadores, p. 247); (2) el establecimiento de las bases necesarias para que los organismos garantes tengan facultades similares de verificación en sus respectivos ámbitos de competencia. Esto implica definir la conveniencia de incluir en la ley reglamentaria la posibilidad de ejercer la verificación de oficio (además, por supuesto, de la que se derive del ejercicio de los derechos ARCO); (3) ciertos estándares para el cumplimiento del deber de adoptar medidas de seguridad en el tratamiento de los datos y del deber de confidencialidad. Todo lo cual supone especificar la definición de medidas de seguridad, establecer quién adoptara dichas medidas, cuál es el objeto que se persigue, el piso mínimo sobre qué medidas de seguridad deberán adoptarse, así como determinar a quién le corresponde el deber de confidencialidad –responsable, encargado y tercero- y la duración de la obligación (Recio, 2013, pp. 43 y 46).

De todo lo anterior podemos colegir que aún es pronto para pronunciarnos sobre la naturaleza de la ley general y sus implicaciones en la distribución de competencias. La reforma constitucional de este año deja abierta la posibilidad de constituir una Ley Marco que más que distribuir competencias entre órdenes de gobierno, establezca pisos mínimos para tutelar el derecho a la protección de datos personales, en consonancia con los deberes del Estado de promoción, respeto, protección y garantía de este derecho humano, poniendo especial énfasis en la creación de mecanismos de

coordinación. Sin que ello obste, por supuesto, para desglosar en su contenido las nuevas competencias del órgano constitucionalmente autónomo, en su función nacional, que devienen no de la Ley General sino de la propia Norma Fundamental.

Lo anterior, ciertamente, no es una tarea fácil pues la experiencia en nuestro sistema jurídico nos demuestra que las leyes generales presentan diversas complejidades, dado el carácter delicado y confuso que puede presentar la definición y distribución competencias en las materias concurrentes.

Así en un estudio elaborado por la División de Estudios Jurídicos del CIDE en materia ambiental (2012) pudimos observar como en diversas materias concurrentes se dificulta la interacción de los actores involucrados tanto por su diversidad como por la falta de una definición específica de sus competencias que, incluso, se llega a complicar por la dispersión normativa del objeto regulado. A manera de ejemplo, en materia forestal y agrícola intervienen diversas autoridades como la SAGARPA, la SEMARNAT, autoridades, estatales, municipales, agencias federales especializadas y particulares.

De igual forma, la materia de sanidad vegetal se encuentra definida principalmente en la Ley Federal de Sanidad Vegetal y en la Ley General de Desarrollo Forestal Sustentable. Esta legislación faculta a diversas autoridades como la SAGARPA, la SEMARNAT y la CONAFOR. Sin embargo, las leyes y los demás ordenamientos que regulan la sanidad forestal no se relacionan entre sí y no están claras las competencias de cada una de las autoridades involucradas. En esta materia existen diversos actores con facultades y competencias poco definidas sobre las funciones que cada uno debe desempeñar, inclusive existen casos en que hay un traslape de funciones. El resultado es que en esta materia tenemos una regulación dispersa, difusa, sin claridad competencial y que genera una indefinición en cuanto a la responsabilidad de cada uno de los actores.

Otro ejemplo esta en materia de forestación en donde las competencias se dispersan a lo largo de la Ley General de Desarrollo Forestal Sustentable. En esta área interviene la Federación para la emisión de normas de reforestación, la SEMARNAT que emite NOMs tendientes a regular los procesos de reforestación y restauración, las entidades federativas que elaboran y aplican programas de reforestación y llevan a cabo acciones de conservación y restauración de suelos, los municipios que participan en la planeación y ejecución de la reforestación, la SAGARPA que debe coordinarse con SEMARNAT y CONAFOR para cumplir con los objetivos del Servicio Nacional Forestal en la parte de reforestación. Asimismo, intervienen CONAGUA y CFE para el manejo eficiente e integral de las cuencias que promueven la reforestación que deberán coordinarse con SEMARNAT y CONAFOR. Esta multiplicidad de actores demanda un esfuerzo importante de coordinación que dificulta que los procesos de forestación sean eficientes.

Los convenios de colaboración entre agencias federales y entre diversos niveles de gobierno han tratado de dar una respuesta a esta problemática; sin embargo, la coordinación entre autoridades ha sido muy complicada y los resultados han sido poco alentadores.

El reto consiste en crear canales claros y directos de colaboración entre agencias federales y entre los diversos niveles de gobierno del país para lograr un uso eficiente de los recursos y cumplir con los objetivos previstos.

B) En el ámbito internacional

La necesidad de expedir una Ley General que contemple la protección de datos personales abre la posibilidad de generar estándares homogéneos de protección que se adapten a las exigencias del entorno internacional en la materia.

Si bien ya parte de nuestro sistema jurídico ha tomado como referencia altos estándares internacionales de protección de datos personales, como se pone de manifiesto en la exposición de motivos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, una ley general para el sector público en cualquiera de los órdenes de gobierno permite el establecimiento de una verdadera simetría de los principios, bases y procedimientos en todo el territorio de la República Mexicana que fortalezca el compromiso de construir el andamiaje jurídico que permita hacer efectivo este derecho fundamental dentro y fuera de nuestras fronteras.

La importancia de considerar los niveles de protección adoptados en el ámbito internacional para nuestro desarrollo legislativo se hace patente ante la posibilidad de que México sea parte del Convenio 108 que, a sus 30 años de vigencia, se encuentra en un proceso de modernización y replanteamiento a efecto de responder a las nuevas realidades retos y paradigmas que plantea la protección de la información personal en una sociedad donde el desarrollo vertiginoso y el uso ilimitado, y en ocasiones, indiscriminado de las tecnologías de la información cada día cobra mayor fuerza.

Esta modernización aborda aspectos del Convenio 108 relativos a su alcance y competencia, los principios y derechos de protección de datos personales reconocidos y de nuevo surgimiento, la incorporación de nuevos datos personales con el carácter sensible, la pertinencia de hacer públicas las vulneraciones de seguridad ocurridas, la conveniencia de establecer previsiones especiales en el tratamiento de datos de localización y tráfico derivados de las telecomunicaciones, el replanteamiento del régimen de transferencias de datos personales, entre otros temas.

De manera particular, el Convenio 108 en su artículo 23 numeral I señala que el Comité de Ministros del Consejo de Europa podrá invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera a éste, mediante un acuerdo adoptado por la mayoría prevista en el artículo 20, inciso d del Estatuto del Consejo de Europa y por unanimidad de los representantes de los Estados contratantes que tengan el derecho a formar parte del Comité Consultivo. Es importante tener en cuenta que 43 Estados miembros han firmado y ratificado el Convenio 108, destacando los países de Alemania, Italia, Portugal, Francia, España y Reino Unido, los cuales se caracterizan por tener un vasto y novedoso desarrollo normativo y jurisprudencial en la materia. En febrero de 2010, Uruguay inició las gestiones para ratificar el Convenio 108<sup>5</sup>.

La posibilidad de que México sea parte de este Convenio no es una cuestión menor. Existen diversas consideraciones que justifican la conveniencia de que nuestro país se adhiera al mismo, entre las que cabe mencionar las siguientes:

---

<sup>5</sup> Memoria Anual de 2010 de la Unidad Reguladora y de Control de Datos Personales de Uruguay. El texto completo se encuentra disponible en el siguiente vínculo de Internet: <http://www.datospersonales.gub.uy/sitio/pdf/memoria-anual-2010.pdf>

(1) *El derecho a la protección de datos personales como un derecho humano.* El Convenio 108 se distingue por establecer garantías mínimas para la efectiva protección y respeto de un derecho fundamental. Así, tanto México en su artículo 16 constitucional como la Unión Europea en el artículo 8 de su Carta de Derechos Fundamentales, se distinguen por reconocer en la máxima cúspide normativa de sus sistemas jurídicos a la protección de datos personales como un derecho humano con contenido y mecanismos propios.

Bajo este contexto, la adhesión de México al Convenio 108 beneficiaría a todos los mexicanos al ampliar las garantías de protección y respeto de su información personal dentro y fuera de nuestro territorio. Asimismo, México ratificaría su compromiso que tiene con el fomento, promoción y respeto de los derechos humanos, a nivel internacional. Muestra de ello, son las recientes reformas al artículo 1 de nuestra Constitución Política.

(2) *El libre flujo de información personal entre Estados Partes.* El Convenio 108 garantiza que ninguna Parte, amparada en proteger la vida privada, podrá prohibir o someter a autorización especial los flujos transfronterizos de datos personales con destino al territorio de otra Parte.

Por su parte, el Protocolo Adicional prevé como regla general que el flujo transfronterizo de información personal a un Estado u organización que no sea Parte del Convenio, sólo podrá llevarse a cabo cuando se asegure un nivel adecuado de protección, salvo que la legislación interna lo exceptúe a causa de intereses concretos del titular, o de intereses legítimos especialmente de carácter público, o bien, cuando se prevean garantías suficientes a través de cláusulas contractuales.

Así, la adhesión de México a este Convenio facilitaría:

(a) La apertura de flujos de inversión extranjera directa al brindar certeza jurídica en los intercambios comerciales transfronterizos con los Estados Partes, ya que evitaría la existencia de barreras encubiertas a dichos intercambios, lo que nos ubicaría en la tendencia mundial de alcanzar niveles de integración que permitirían la libre circulación de mercancías, personas, bienes y capitales, al tiempo que se protegería la información de las personas, convirtiéndose este derecho en un instrumento fundamental para dicha integración.

(b) La generación de empleos y fomento de la inversión extranjera, en razón de que las transferencias de datos desde la Unión Europea se llevarían a cabo sin necesidad de la autorización de las autoridades de protección nacionales. Ello traería consigo la inversión extranjera directa en el mercado del tratamiento de datos de dicho bloque económico.

(c) El fortalecimiento de la relación comercial entre México y los Estados Partes, al cumplir y compartir estándares internacionales en materia de privacidad, sin inhibir el flujo transfronterizo de la información y sin perjuicio del intercambio comercial que nuestro país tiene con sus socios de Norteamérica, Asia-Pacífico y otras economías del mundo.

Lo anterior, es así porque la importancia de la protección de datos personales está hoy en día fuera de duda, ya que no existe actividad económica que para el desarrollo de la misma esté exenta de la interacción, explotación, aprovechamiento y transferencia de información personal.



En este sentido, el Convenio 108 se constituiría en un mecanismo adicional a la normatividad mexicana existente que lograría equilibrar y conciliar la circulación de la información personal en un mundo globalizado, bajo determinados estándares y reglas mínimas enfocadas a evitar un flujo de los datos personales indiscriminado, y por consiguiente, que las personas pierdan ese poder de control que tienen sobre la información que les concierne.

(3) *La cooperación y ayuda mutua entre los Estados Partes.* El Convenio 108 compromete a las Partes a concederse intercambio de información sobre su derecho y práctica administrativa en materia de protección de datos personales, o bien, asistencia mutua para facilitar información fáctica relativa a un tratamiento específico.

Bajo este compromiso, la cooperación internacional hoy en día juega un papel fundamental ya que actualmente el desarrollo del derecho a la protección de datos personales se está enfrentando a procesos de globalización y de construcción de instrumentos internacionales y nacionales, que permitan garantizar al máximo su eficacia frente ataques que superan los límites fronterizos de cualquier Estado.

Así, uno de los mayores obstáculos que se presentan para alcanzar una efectiva tutela del derecho a la protección de datos personales, es la falta de instrumentos jurídicos o mecanismos de cooperación entre Estados y/o autoridades de protección de datos personales que desarrollen y conceptualicen la extraterritorialidad de conductas ilícitas o indebidas respecto al tratamiento de información personal, a través de la utilización de cada vez más novedosas y extraordinarias tecnologías de la información en las cuales el territorio físico no tiene transcendencia alguna.

Bajo este contexto, la adhesión de México al Convenio 108 facilitaría la institucionalización de mecanismos vinculantes de cooperación y asistencia en la materia que permitan hacer efectivo el derecho a la protección de datos personales entre los Estados Partes.

(4) *Un precedente para la adecuación europea.* La adhesión de nuestro país al Convenio 108 constituiría un precedente en las gestiones y acciones destinadas a obtener el reconocimiento de la Unión Europea como un país con un nivel adecuado de protección de datos personales, facilitando el libre flujo de éstos entre sus Estados miembros y nuestro país sin mayor requerimiento adicional por parte de las autoridades de protección de datos personales europeas.

Es importante tener en cuenta que el Convenio 108 sólo es aplicable al tratamiento de datos personales automatizados; en términos del artículo 3, numeral 2, inciso c del Convenio, es conveniente que México al momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión haga saber mediante declaración expresa dirigida al Secretario General del Consejo de Europa que el Convenio 108 también será aplicable a bases de datos personales que no sean objeto de tratamiento automatizado. Lo anterior, en razón de que la normatividad mexicana en materia de protección de datos es aplicable a todo tipo de tratamiento, independiente si éste es físico o automatizado.

## Conclusiones

---

Las medidas que en los últimos años ha venido adoptando nuestro país en materia de protección de datos personales, con un claro sentido progresivo, presentan beneficios interdependientes pero diferenciados. Por una parte, conllevan el fortalecimiento de un derecho fundamental cuyo objetivo consiste en garantizar la libre autodeterminación de la propia información, así como la adopción de medidas de seguridad en el tratamiento de los datos por parte de sus responsables. Pero, por la otra, ante el incremento en el comercio electrónico, favorece el intercambio comercial, las transacciones económicas y la información científica y técnica compartida, con países que exigen ciertos estándares adecuados de protección de los datos personales que fluyen de un país a otro. En ese sentido, se trata de un derecho cuya dimensión no sólo redundaría en beneficio del titular de los datos dentro del ámbito de sus derechos humanos reconocidos, sino que, además, permea de manera directa en el desarrollo económico del país.

La inclusión de México como parte del Convenio 108 es un primer paso para el reconocimiento y adopción de directrices que establezcan los mínimos indispensables para resguardar la seguridad de la información personal y generar confianza entre los países. México debería pugnar por obtener el reconocimiento de la Unión Europea como un país con un nivel adecuado de protección de datos personales, ya que favorecería el flujo comercial de manera importante, generando beneficios no sólo respecto de los países miembros de la Unión sino también respecto de otros Estados con los que tenemos celebrados tratados comerciales.

En consecuencia, el desarrollo de nuestro derecho interno no puede permanecer aislado a los estándares de protección de los datos personales que se han venido gestando en nuestro entorno internacional. A todo lo cual se añade la perspectiva de los derechos humanos que introduce explícitamente los deberes de promoción, protección, garantía y respeto del Estado, de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad. Así, estas dos dimensiones se constituyen en los principales referentes que deben informar nuestra legislación interna.

Pero para que ello sea posible es necesario adoptar ciertos criterios homogéneos aplicables tanto para el sector público en cualquiera de los órdenes de gobierno, como para el sector privado. En principio la creación de una Ley General, aplicable para el sector público, permitirá establecer un piso mínimo común que contemple los principios, bases y procedimientos en materia de protección de datos personales para la Federación, las entidades federativas y los municipios. No obstante, es importante considerar que este piso mínimo debe de ser congruente con la legislación federal aplicable al sector privado. De lo contrario, la simetría de los niveles adecuados de protección de datos personales no sería factible. Lo cual también redundaría en posibles contradicciones con los estándares internacionales. De tal forma que el diseño de la nueva Ley General en materia de Protección de Datos Personales presenta importantes retos de carácter sustantivo.

De manera adicional, cabe considerar que la creación de una Ley General supone importantes retos que surgen a raíz del modelo federalista en nuestro país. El equilibrio entre la búsqueda de niveles estandarizados de protección del derecho sobre los datos personales y la soberanía de las entidades federativas no es una cuestión fácil de resolver. La experiencia en otros ámbitos nos ha enseñado las dificultades que supone el desarrollo legislativo y la distribución de competencias en las materias de carácter concurrente. Los mecanismos de coordinación y colaboración entre el órgano garante y los organismos autónomos son fundamentales para utilizar los recursos de manera eficiente y establecer los mínimos necesarios en la protección de datos personales de ahí la importancia de establecer un sistema nacional que se encargue de promover la colaboración entre los diversos actores.

A esta dificultad se añade, por supuesto, el carácter de autonomía constitucional que la propia Norma Fundamental le otorga a los órganos garantes del derecho. De ahí que la Ley General tenga que poner sumo cuidado en el desarrollo normativo del derecho a la protección de datos personales para evitar vaciar de contenido a las competencias legislativas de las entidades federativas en la materia y cuidar las relaciones de independencia entre el órgano autónomo de carácter nacional y de los organismos autónomos especializados de los estados y el Distrito Federal. Este último aspecto se manifiesta particularmente en las facultades de atracción y de revisión que le concede la propia Constitución al órgano constitucional autónomo de carácter nacional respecto de los procedimientos y recursos que se lleven en el ámbito local.

## Bibliografía

---

- Basterra, Marcela (2008), *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados Derecho Constitucional Provincial Iberoamérica y México*, Buenos Aires y México, Ediar y UNAM.
- Conde Ortiz, Concepción (2005), *La Protección de Datos Personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Madrid, Dykinson, S.L.
- Cámara de Senadores del Congreso de la Unión (2013), *Dictamen de las Comisiones Unidas de Puntos Constitucionales; de Estudios Legislativos Primera; de Gobernación y de Anticorrupción y Participación Ciudadana en material de transparencia*, aprobado por el Pleno de la Cámara el 20 de diciembre de 2012. Disponible en:  
[http://www.diputados.gob.mx/LeyesBiblio/votos/20131126\\_trasp.htm](http://www.diputados.gob.mx/LeyesBiblio/votos/20131126_trasp.htm)
- Cossío Díaz, José Ramón (2008), “Jerarquía, división competencial en relación con los tratados internacionales en Derecho Mexicano”, *Anuario Mexicano de Derecho Internacional*, vol. VIII, Instituto de Investigaciones Jurídicas de la UNAM.
- Da Cunha Lopes, Teresa M. G. (2010), “La creación de una Política Europea de Protección de Datos Personales”, *Revista de Derecho Informático*, núm. 140, marzo, Alfa-Redi. Disponible en:  
[http://www2.congreso.gob.pe/sicr/cendocbib/con2\\_uibd.nsf/F1864D09F0ABB51F052577DD00752891/\\$FILE/Creación\\_Polit\\_Europea\\_Protec\\_Datos\\_Pers.pdf](http://www2.congreso.gob.pe/sicr/cendocbib/con2_uibd.nsf/F1864D09F0ABB51F052577DD00752891/$FILE/Creación_Polit_Europea_Protec_Datos_Pers.pdf)
- Ferrer Mac-Gregor, Eduardo y Carlos María Pelayo (2012), “La obligación de “respetar” y “garantizar” los derechos humanos a la luz de la jurisprudencia de la Corte Interamericana. Análisis del artículo I del pacto de San José como fuente convencional del derecho procesal constitucional mexicano”, *Estudios Constitucionales*, Año 10, Núm. 2, Centro de Estudios Constitucionales de Chile Universidad de Talca.
- López Ayllón, Sergio y María Marván Laborde, *Coordinadores* (2007), *La transparencia en la República: un recuento de buenas prácticas*, México, IFAI/CIDE.
- Piñar Mañas, José Luis y Miguel Recio Gayo (2013), *Código de Protección de Datos Personales en México*, México, Tirant lo blanch.
- Recio Gayo, Miguel (2013), *Esquemas de la Ley de Protección de Datos Personales y su Reglamento*, México, Tirant lo Blanch.
- Upegui Mejía, Juan Carlos (2007), “Diez ideas para un régimen de datos personales en clave latinoamericana”, *Derecho Comparado de la Información. Nueva Serie*, núm. 10, Julio-Diciembre, Instituto de Investigaciones Jurídicas de la UNAM.



Documentos  
de trabajo  
**eBooks** **Novedades**  
Fondo  
editorial  
**Revistas** **LIBROS**

[www.LibreriaCide.com](http://www.LibreriaCide.com)