Fecha de recepción: 31 de enero de 2013 / Fecha de aprobación: 9 de abril de 2013

Revista de Derecho Comunicaciones y Nuevas Tecnologías

La autorregulación en materia de protección de datos personales: la vía hacia una protección global

Lina Gabriela Ornelas Núñez

Melissa Higuera Pérez

Universidad de los Andes

Facultad de Derecho

Revista de Derecho, comunicaciones y Nuevas Tecnologías

N.º 9, Junio de 2013. ISSN 1909-7786

La autorregulación en materia de protección de datos personales: la vía hacia una protección global

Lina Gabriela Ornelas Núñez*

Melissa Higuera Pérez**

Resumen

Nuestro mundo se encuentra girando en una imparable espiral de innovación. La tecnología brinda infinitas posibilidades de procesar y utilizar información. Esto facilita a los individuos el desarrollo de sus actividades pero también aumenta los riesgos de ser afectado por el uso ilegítimo de esta. La preocupación derivada de estos riesgos ha sido atendida por las distintas regiones del mundo a través de regulaciones en

Abstract

Our world is continuously moving due to an unstoppable technological rush. Information and communication technologies certainly bring us numerous possibilities to process information, including personal information. This allows us to carry out our activities very effectively but also increases the possibilities to be affected by the misuse of our information. Several regions had addressed their concerns

* Egresada de la Facultad de Derecho de la Universidad de Guadalajara y maestra en Derecho Internacional por la Universidad Libre de Bruselas. Se desempeñó durante doce años en el sector público en México y Europa, en particular para la Comisión Europea y las secretarías de Economía y Gobernación, en la que fungió como directora general adjunta en la Unidad para la Promoción y Defensa de los Derechos Humanos. Ha publicado, coordinado y colaborado en libros y numerosos artículos académicos en materia de protección de datos personales, entre los que se destacan los libros Protección de datos personales en México: el caso del Poder Ejecutivo; Protección de datos personales de menores en las redes sociales digitales y La Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento (en prensa); y el capítulo sobre México del libro Privacidad y derechos humanos 2005, 2006 y 2007, publicado por la organización Electronic Privacy Information Center (EPIC). Junto con José Luis Piñar Mañas coordinó el libro La protección de datos personales en México, Editorial Tirant lo Blanch, 2013. Durante nueve años colaboró con el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) en calidad de directora general de clasificación y datos personales y posteriormente como directora general de autorregulación en materia de protección de datos personales. Actualmente es profesora investigadora asociada en el Centro de Investigación y Docencia Económicas, CIDE A. C. Dirección electrónica: lina.ornelas@cide.edu.

** Licenciada en Derecho con mención honorífica por el Instituto Tecnológico Autónomo de México, con la tesis Protección de datos personales en México: diagnóstico y perspectiva; cuenta con un diplomado en Derecho de las Tecnologías de la Información y Comunicaciones, en la misma universidad. Actualmente es directora de Facilitación, en la Dirección General de Autorregulación del Instituto Federal de Acceso a la Información y Protección de Datos. Ha ocupado otros puestos relacionados con la protección de datos personales, como la Subdirección de Clasificación y Datos Personales y la Jefatura del Departamento del Registro Público de Consumidores (RPC) de la Procuraduría Federal del Consumidor, posición desde la cual participó en la concreción del proyecto del RPC, facilitando a los consumidores el ejercicio de su derecho de oposición al tratamiento de sus datos para fines publicitarios. Dirección electrónica: higuera_melissa@hotmail.com

materia de protección de datos. No obstante, estas visiones —y regulaciones— tienen claros limitantes territoriales que no permiten una protección global a un fenómeno global. La autorregulación aparece como una herramienta capaz de ampliar la protección de los individuos más allá de las fronteras, situación que será analizada en el presente artículo.

Palabras clave: datos personales, información personal, autorregulación, corregulación, minería de datos, privacidad, derecho a la protección de datos personales, responsabilidad demostrada, interoperabilidad, estandarización, transferencia internacional de datos, robo de identidad, Acuerdo de Puerto Seguro entre Estados Unidos y la Unión Europea, reglas corporativas vinculantes, Sistema de reglas transfronterizas de privacidad.

regarding the misuse of personal information by means of data protection legal frameworks. However, these approaches and regulations have inherent territorial limits. In this scenario, self-regulation appears as an important tool to grant a global protection for data subjects. This idea will be analyzed here of.

Keywords: personal data, personal information, self-regulation, corregulation, data mining, privacy, right to the protection of personal data, accountability, interoperability, standardization, international data transfer, identitytheft, Safe Harbor Framework, Corporate Binding Rules, cross border privacy rules system.

Sumario

Introducción: el futuro nos ha alcanzado

Con toda seguridad afirmamos que, desde mediados del siglo pasado, nuestro mundo se encuentra girando en una imparable espiral de innovación. La tecnología que brinda la computación ubicua y la comunicación a distancia han multiplicado exponencialmente las opciones para realizar nuestras actividades. De hecho, nos ha impuesto, de manera casi imperceptible, nuevas formas de vivir y de relacionarnos. Un buen ejemplo son las redes sociales que nos permiten tener cientos de "amigos" —a quienes, en muchas ocasiones, nunca hemos visto personalmente y probablemente no veremos— o las búsquedas de cualquier clase de información en línea a través de buscadores potentísimos, los cuales ponen a nuestra disposición toda clase de bien, producto o servicio sin que tengamos que salir de casa o los dispositivos inteligentes que posibilitan nuestra ubicación física en tiempo real y nos brindan soluciones inmediatas.

La "nube" parece ofrecer soluciones para todo y para todos: servicios de infraestructura, plataformas virtuales y aplicaciones informáticas a nuestra disposición en una misma ventanilla: Internet. Sin importar en dónde nos encontremos ni si se trata de un individuo, una gran corporación o una entidad gubernamental, la posibilidad de almacenar y consultar información, desarrollar o utilizar programas de todo tipo está al alcance a un precio accesible. Lo anterior, debido a que los servicios ofrecidos en la nube optimizan el uso de instalaciones informáticas ubicadas en cualquier parte del mundo.

El ámbito virtual parece no tener límites. No obstante, es necesario dejar en claro que las acciones realizadas en este no dejan de tener implicaciones en el mundo físico o "real". El tratamiento de datos personales realizado en estas plataformas virtuales y en la nube no es la excepción.

Las posibilidades de almacenar, procesar, transmitir, cruzar y utilizar información en pocas, grandes o ingentes cantidades —como en el caso del fenómeno del *big data*— son muy diversas. De la misma manera, los riesgos de ser afectado por el tratamiento no legítimo de nuestros datos, aún sin que nosotros tengamos conocimiento de ello, han aumentado. Hasta hace algunos años no existía la posibilidad de discriminación, por parte de un potencial patrón, hacia un joven recién egresado que solicita empleo, como resultado de la evaluación —con o sin conocimiento del propio joven— de la información personal "posteada" en su perfil de Facebook o de haber consultado una agencia de información de antecedentes judiciales y administrativos accesible en Internet. Otro riesgo de un mal uso de nuestra información, tanto en el mundo virtual como en el físico, sería la negación a una persona en particular del acceso a su expediente médico (ya sea en soporte físico o electrónico) para buscar un tratamiento alternativo, por parte de instituciones de salud públicas o privadas.

La creación de perfiles de acuerdo con los hábitos de navegación en línea para el ofrecimiento de bienes, productos o servicios —*behavioral targeting*— podría ser un arma de doble filo: si bien ofrecen a los usuarios artículos de su interés de conformidad con su perfil, los excluyen

de decidir sobre otros muchos productos o servicios, por mencionar lo menos. Lo anterior, sin menoscabo de que estos perfiles de navegación y consumo (que se construyen con base en información sobre las páginas web visitadas por un usuario de la red, la duración de dichas visitas, el número de clics que realiza sobre determinado ícono o los bienes solicitados en línea) podrían acabar en manos nada éticas que hagan un uso ilegítimo de estos para convertir a sus titulares en blanco de delitos. Más aún, considerando un posible cruce de dicha información con aquella que permite nuestra ubicación en tiempo real, ya sea por medio de geolocalizadores ligados a dispositivos móviles o en ocasiones por la imprudencia del propio titular de los datos que "informa" al público en general sobre su ubicación, a través de las redes sociales o un *tweet*, el riesgo va en aumento.

Los anteriores fenómenos de acopio, minería y transferencia de datos influyen de forma directa en la manera en que debemos redimensionar nuestro derecho a la intimidad o, mejor dicho, a decidir sobre la información que nos pertenece. Si bien no todos conocemos lo que se hace o puede hacerse con nuestros datos y nuestros derechos en relación con nuestra información, el tema de generar ciertas reglas para el tratamiento de datos personales de los individuos llegó para quedarse debido al aumento en delitos como el robo de identidad o el fraude financiero, con la utilización indebida de datos de tarjeta de crédito o el *phising*[1].

La preocupación derivada de este reto impuesto por la tecnología tiene alcances, tanto nacionales como internacionales. Varios países han invertido grandes esfuerzos en regular la materia y, como veremos más adelante, México ha obedecido a la misma tendencia. No obstante, aun y con el interés de diversos Estados, las regulaciones nacionales tienen, de manera concomitante, claros limitantes territoriales. Por ello, paralelamente y con un poco mayor alcance, diversos organismos internacionales y regionales han cristalizado su preocupación en instrumentos normativos —algunos potestativos u orientadores, otros vinculantes— que regulan la protección de datos personales buscando ampliar el amparo a los individuos y considerando, en todo momento, el necesario equilibrio entre esta y el libre comercio y flujo de bienes, personas e información.

La pregunta que surge entonces de manera inevitable es si será posible alcanzar una regulación mundial sobre protección de datos o si, en lugar de aspirar a ello, deben explorarse válidamente vías alternativas, tales como la autorregulación. Por ello, el objetivo del presente artículo es profundizar sobre la autorregulación en materia de protección de datos personales y destacar los argumentos que podrían llevarnos a apoyar nuestro punto de vista acerca de sus beneficios.

1 De conformidad con la Comisión Federal de Comercio de los Estados Unidos de América, el phising implica acciones de envíos de correos electrónicos o pantallas emergentes en nombre de determinada empresa u organización con la cual el titular tiene contacto (como un banco, un proveedor de servicios de Internet o hasta una institución de gobierno). Dicho mensaje solicitará algún tipo de actualización de datos, validación o confirmación de cierta transacción y vinculan al titular con un sitio web que aparenta ser el de la empresa u organización, sin serlo. El objeto de dicho sitio es obtener información del titular y robar su identidad. Para mayor información, visitar el sitio Internet de la Comisión Federal de Comercio: http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm, a julio de 2012.

I. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, ¿UN DERECHO FUNDAMENTAL?

En este primer apartado iniciaremos exponiendo que la naturaleza sobre el derecho a la protección de datos personales, entendido este, de manera simplificada, como el derecho de todos y cada uno de los individuos a decidir sobre cuáles de sus datos pueden ser usados y por quién, así como las circunstancias bajo las cuales serán utilizados[2], presenta ya cierta polémica.

Podríamos afirmar que el considerarlo o no como un derecho fundamental depende del enfoque y hasta de la cultura. A continuación abordaremos los dos principales puntos de vista en el mundo al respecto. Primeramente, expondremos el correspondiente al modelo global o integrador, con la Unión Europea como principal exponente, en donde se reconoce al derecho de protección de datos personales como un derecho fundamental. En segundo término presentaremos el modelo sectorial-autorregulador de Estados Unidos, calificado por algunos como una visión contrapuesta y quizá hasta irreconciliable con el modelo europeo por no considerarlo como un derecho fundamental. Por último, identificaremos y ubicaremos la visión mexicana, que retoma elementos de ambos modelos, basándose innegablemente en el esquema europeo en cuanto a los principios orientadores, y retomando las mejores prácticas del modelo estadounidense.

A. Europa

En el contexto europeo existe evidencia, desde 1967, sobre la preocupación por la potencial agresividad de las tecnologías de información a los derechos fundamentales de las personas, como consta en la Resolución 68/509/CE de la Asamblea del Consejo de Europa, que dio lugar a diversas recomendaciones y resoluciones sobre la materia. Algunos años después, como instrumento referente en este tema, se encuentra el Convenio No. 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108). El Convenio 108 establece principios y garantías que los Estados adheridos[3] deben observar en relación con ficheros y tratamientos automatizados de datos de carácter personal. Su objetivo es compatibilizar el derecho a la vida privada y el derecho de libre circulación de datos entre los diversos países firmantes. Cabe resaltar que hasta ese momento aún no se diferenciaba claramente el derecho a la protección de datos personales respecto del derecho a la vida privada.

Más adelante, durante los años noventa, el libre intercambio de bienes, personas, capitales e información —incluyendo la de carácter personal— cobra una importancia fundamental en la consolidación del mercado único europeo. Para

2 También conocido como autodeterminación informativa. Según el especialista español Miguel Ángel Davara Rodríguez, el derecho a la protección de datos personales es "[…] el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esa forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad".

3 Que pueden ser, tanto los Estados miembros del Consejo de Europa como Estados no miembros.

conciliar la necesidad de este libre flujo y el derecho de protección a los datos personales, surgió la 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 estos (Directiva 95/46/CE), que precisa y amplía los principios establecidos en el Convenio 108[4]. El objeto de dicha directiva es obligar a los Estados miembros a garantizar, mediante normativa nacional, el derecho a la intimidad de las personas en lo que respecta al tratamiento de sus datos personales, de conformidad con el contenido de la propia directiva. Para ello, establece una serie de principios, derechos de los titulares de los datos personales, excepciones y limitaciones a tales derechos, incluyendo la transferencia de datos a un país tercero únicamente cuando este garantice el nivel adecuado de protección para estos de conformidad con la propia directiva. Aunque hay otras directivas relevantes en el ámbito europeo, por cuestiones de espacio consideramos conveniente referirnos únicamente a la Directiva 95/46/CE, no sin mencionar que actualmente está siendo objeto de una revisión que desembocará en la emisión de una regulación distinta y aplicable de manera directa en los Estados miembros, sin necesidad de que estos tengan que transponer su legislación nacional.

Como es posible apreciar, toda esta regulación europea en la materia fue fortaleciendo paulatinamente la concepción del derecho de protección de datos personales como un derecho distinto al de la privacidad o intimidad, con características propias que integran una serie de principios, derechos para los titulares y obligaciones para quienes deciden sobre su tratamiento[5]. Al mismo tiempo, se reconoce la necesidad de prever procedimientos que garanticen a los titulares de la información el ejercicio de su derecho y la existencia de autoridades especializadas para garantizar su defensa. Todo ello, constituyendo el modelo global o integrador de protección de datos[6]. Culminando dicho modelo, en el 2000 se produce el reconocimiento del derecho a la protección de datos personales como un derecho fundamental, en el artículo 8 de la Carta Europea de Derechos Fundamentales. Es en este instrumento donde se diferencia expresamente del derecho a la vida privada y familiar, previsto en el artículo 7 de la misma carta.

B. Estados Unidos de América

En aparente oposición al modelo europeo se encuentra el modelo sectorial-autorregulatorio de protección de datos adoptado por los Estados Unidos de América. Este modelo se basa en la creencia de que la regulación excesiva por parte del gobierno inhibe el desarrollo de la economía, y que el mercado es capaz de au-

4 Véase CANALES GIL, Álvaro, El derecho fundamental a la protección de datos de carácter personal, Revista Jurídica de Castilla y León, n.º 12, abril 2007, p. 20 e HIGUERA PÉREZ, Melissa, El derecho a la protección de datos personales en México: diagnóstico y perspectiva, tesis de licenciatura, México, ITAM, 2009.

5 Tanto de carácter negativo como el no tratar la información de manera ilegítima; como positivo, como la obligación de proveer al titular de información relacionada con el tratamiento de los datos que realiza. Esta divergencia resulta fundamental para argumentar la diferencia del derecho a la protección de datos personales del derecho a la privacidad o intimidad que solo impone obligaciones de carácter negativo o de "no hacer".

6 Véase Manual de privacidad del curso en línea Aspectos Legales del Comercio Electrónico, Conferencia de las Naciones Unidas sobre el Comercio y Desarrollo, México, agosto 2007, pp. 24 a 26.

torregularse en la materia, siempre y cuando haya un interés real de los consumidores, como en el caso de la confianza necesaria para realizar compras a través del comercio electrónico. Únicamente sectores muy específicos y que impliquen alto riesgo, tales como el financiero o el de la salud, deberán ser regulados y supervisados, sin que para el resto de las materias exista una regulación general sobre protección de datos. Tampoco existe una autoridad controladora nacional, sino autoridades que regulan sectorialmente la materia, como el caso de la Comisión Federal de Comercio y la Comisión Federal de Comunicaciones.

Como ejemplos de las mencionadas regulaciones sectoriales se encuentran la Ley de portabilidad y responsabilidad de seguros de salud (*Health Insurance Portability and Accountability Act* –HIPAA) de 1996[7], la Ley para la protección de la privacidad infantil en línea (*Children's Online Privacy Protection Act* –COPPA) de 1998[8] , y la Ley de transacciones de crédito equitativas y precisas (*Fair and Accurate Credit Transactions Act* –FACTA), de 2003[9]. Dichas regulaciones favorecen el flujo de datos sobre los derechos de los individuos a controlar su propia información personal, aunque también establecen ciertos mecanismos de protección para determinada información personal. Adicionalmente, existen mecanismos que instrumentan el derecho de oposición del titular respecto a la utilización de sus datos con fines publicitarios como el *National Do Not Call Registry*, previsto por la Ley de telemercadeo y administrado por la Comisión Federal de Comercio, la Comisión Federal de Comunicaciones y el Departamento de Justicia, así como agencias gubernamentales de los Estados, según corresponda, y distintos métodos de vigilancia que incluyen investigaciones, requerimientos y sanciones de carácter civil.

También es justo hacer mención al hecho de que cuarenta y seis estados, el Distrito de Columbia, Puerto Rico y las Islas Vírgenes cuentan con regulación en materia de notificación por vulneraciones de seguridad que involucren información personal[10].

Como se puede apreciar, la protección a la privacidad en Estados Unidos también existe y se encuentra relacionada con materias muy concretas, que desde el punto de vista del legislador estadounidense representan, bien un riesgo real, bien una actividad o práctica injusta o engañosa de una empresa frente a un consumidor, impidiéndole una decisión informada acerca de los bienes o servicios que consume, o bien el

7 Esta ley regula la seguridad y la privacidad de datos personales relativos a la salud de los individuos. Asimismo, busca mejorar la eficiencia y eficacia del sistema de salud de los Estados Unidos alentando el intercambio vía electrónica de información. La ley establece además la obligación para el Departamento de Salud de expedir regulación que establezca estándares para el uso y la diseminación de información relativa a la salud.

8 Esta ley regula la recolección de información personal de niños menores de 13 años por parte de personas y entidades, así como los requisitos que un operador de un sitio de Internet debe incluir en su política de privacidad. Asimismo, contempla la necesidad de que la autoridad apruebe guías de autorregulación en la materia. La Comisión Federal de Comercio es la encargada de aplicar dicha ley.

9 Esta ley regula el derecho del consumidor a solicitar y recibir gratuitamente la información crediticia que le concierne, así como obligaciones de las instituciones de información crediticia en relación con la exactitud, comunicación al consumidor y a terceros, y almacenamiento de dicha información. Véase VUKOWICH, William T., Consumer Protection in the 21st Century. A Global Prospective, Estados Unidos de América, Transactional Publishers, Inc., 2002, pp. 332-335.

10 Para mayor información, consultar el sitio internet: http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx, a julio de 2012.

incumplimiento de promesas. En este sentido, si bien la protección de datos personales no es considerada un derecho fundamental, sino parte de la lógica del comercio justo, es importante mencionar que la administración del presidente Barack Obama impulsa una regulación federal que permita unificar criterios para la industria, de modo que se aminoren los costos de cumplimiento al tiempo que se garantice una protección homogénea de cara a los individuos[11].

C. México

En este país, no cabe duda que el derecho a la protección de datos personales es un derecho fundamental, reconocido en el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, desde el 1 de junio de 2009:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Es menester reconocer que antes de las reformas al artículo 16 constitucional, que finalmente dotaron de contenido a este nuevo derecho, ya el artículo 6 constitucional reconocía en el ámbito público la protección de datos no solo como un límite al acceso a la información, sino como una prerrogativa para que cualquier persona pudiera acceder y corregir los datos personales que obren en los archivos públicos en sus tres órdenes. Estas reformas del 2007 al artículo 6 constitucional se constituyen en el fundamento para la expedición de leyes especiales en la materia para el ámbito público[12].

Haciendo un enorme esfuerzo de síntesis, el marco de protección de datos en México parte de la consideración del derecho a la protección de datos personales como un derecho fundamental reconocido al más alto nivel de nuestra pirámide normativa, es decir, en sede constitucional. En el ámbito público las leyes secundarias despliegan este derecho ya sea por la vía de las leyes de transparencia y acceso a la información o bien a través de piezas legislativas especiales. Así, a nivel federal la materia se regula

11 Para mayor información, consultar el sitio internet (en inglés): http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b, a julio 2012.

12 A continuación se cita el actual texto del artículo 6to. de la Constitución Política de los Estados Unidos Mexicanos:

Artículo 6°.- […]

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.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

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

[…]

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

por el capítulo correspondiente de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y en algunas entidades federativas se cuenta con leyes especiales como es el caso del Distrito Federal y Guanajuato.

La asignatura pendiente se encontraba en el ámbito privado, ya que si bien existía regulación por la vía de diversas leyes sectoriales, solo hasta que se reformó el artículo 73 constitucional para dotar de facultades expresas y exclusivas al Congreso Federal[13], se expidió en 2010 una ley federal específica en la materia: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Como características esenciales de esta última ley se encuentran: el que prevé una serie de principios y deberes como ejes rectores que deben observar quienes deciden sobre el tratamiento de los datos personales; diversos procedimientos para el ejercicio y la protección de los derechos de acceso, rectificación, cancelación y oposición; una autoridad garante del derecho y diversas autoridades reguladoras; y un catálogo de infracciones y sanciones para aquellos que incumplan aspectos de dicha ley.

Al mismo tiempo, la LFPDPPP prevé distintos aspectos que la hacen una ley moderna, competitiva y flexible: da especial importancia a los principios de información y reconoce el consentimiento tácito para la mayor parte de tratamientos, lo que facilita el procesamiento y libre flujo de datos; evita cargas innecesarias para quienes deciden el tratamiento de datos personales como aquella obligación de registrar sus bases de datos personales ante la autoridad, o la de solicitar autorización previa para la transferencia internacional de datos o de limitar estas únicamente a determinados Estados que prevean regulación similar; por último, retoma el tema de la autorregulación en materia de protección de datos, objeto de análisis en las siguientes secciones del presente artículo.

Como se puede apreciar, la cultura prevaleciente en cada país o región determina la manera de percibir el fenómeno del tratamiento de datos personales y los derechos que las personas tienen en relación con su información. Por ejemplo, el ámbito europeo prioriza una visión garantista del poder de decisión de las personas respecto a su información y contempla diversas salvaguardas en ese aspecto, mientras que en la visión estadounidense —que prevalece en diversos países de la región Asia-Pacífico—, predomina la necesidad del intercambio internacional de información, no sin prever garantías muy concretas para sus titulares, como consumidores, bajo una óptica más pragmática.

II. ¿ESTANDARIZACIÓN O INTEROPERABILIDAD?

Como se menciona en la parte introductoria del presente artículo, las regulaciones nacionales y los derechos previstos en ellas enfrentan límites territoriales. En principio, una norma mexicana puede aplicarse únicamente en territorio mexi-

13 A continuación se cita el actual texto del artículo 73 de la Constitución Política de los Estados Unidos Mexicanos:

Artículo 73.- El Congreso tiene facultad: […]

XXIX- O. Para legislar en materia de protección de datos personales en posesión de particulares.

cano o en un territorio de otro país de conformidad con reglas claramente previstas —que en ocasiones se fundamentan en usos y costumbres— como las relacionadas con el derecho internacional privado en materia de comercio. Las autoridades nacionales, en el mismo sentido, tienen un alcance y jurisdicción determinados, entre otros aspectos, territorialmente.

Es verdad que hay regulación que puede tener mayores alcances, como es el caso de la Directiva 95/46/CE que, como fue expuesto anteriormente, obliga a todos los miembros de la Unión Europea a adoptar normas internas que reflejen todos los contenidos previstos en ella. Esto se debe, precisamente, a las disposiciones de los tratados supranacionales que los constriñen y a la emisión de directivas comunitarias que deben transponerse a los Estados miembros. Aún así, el ámbito de aplicación se limita al espacio europeo en el cual se ejercen las atribuciones de autoridades *ad-hoc*.

Por otra parte, nos encontramos frente al hecho de que el tratamiento de datos personales es un fenómeno internacional, claramente relacionado con aspectos que no tienen los límites territoriales nacionales —o regionales— convencionales. Nos referimos nuevamente a las tecnologías de la información y la comunicación (TIC) incluyendo tecnologías móviles vinculadas al Internet y otras redes de información. Dichas tecnologías, además de permitir el almacenamiento y utilización de grandes cantidades de información, posibilitan, al alcance de un *clic* y con costos cada vez más bajos, su transferencia a una multiplicidad de receptores ubicados en distintas partes de mundo. El otro fenómeno es el comercio internacional, el cual, en una gran cantidad de ocasiones, requiere de un flujo transfronterizo de datos personales. El fenómeno que conjunta a los dos anteriores es el comercio electrónico, el cual tiene la tendencia a convertirse en los próximos años en regla, más que en excepción.

Tanto el comercio internacional como las TIC tienen una naturaleza global. Es por ello que el tratamiento de datos personales relacionados con estas actividades, u otras con el mismo carácter transnacional, requiere de acciones de la misma magnitud para lograr el objetivo de garantizar la autodeterminación informativa de los individuos. Pero, ¿cómo lograr un acuerdo internacional habiendo distintos enfoques sobre el mismo fenómeno?, ¿de qué manera puede el derecho enfrentar la corriente globalizadora?

Una posible respuesta a lo anterior es la estandarización internacional de la protección de datos personales, es decir, la emisión y adopción de un estándar reconocido internacionalmente. Esta es la intención de los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, también conocidos como la Resolución o los Estándares de Madrid, de 2009, que tiene como uno de sus objetivos "[...] plasmar los múltiples enfoques que admite la protección de este derecho [a la protección de datos personales], integrando legislaciones de cinco continentes[14]. Si bien es cierto que los estándares son un gran paso en este camino, también es

14 Texto correspondiente a la presentación realizada por Artemi Rallo Lombarte a la Propuesta conjunta para la redacción de estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal, de 2009.

verdad que la estandarización ha sido cuestionada por tratar de imponer a los distintos Estados una misma y única visión sobre la protección de los datos personales, siendo que la realidad refleja una diversidad de visiones. Además, se ha cuestionado que una norma internacional no provee de suficiente flexibilidad para ajustarse a la realidad cambiante.

Otro camino posible es la interoperabilidad, una vía propuesta por los países del Foro de Cooperación Económica Asia-Pacífico (APEC, por sus siglas en inglés) y principalmente por los Estados Unidos de América, que parte del reconocimiento de la diversidad de visiones e incluso de regulaciones en materia de protección de datos. Esta alternativa establece que los distintos enfoques y modelos pueden construir puentes de comunicación identificando las coincidencias pero no necesariamente generando una única regulación. Como ejemplo de un mecanismo de interoperabilidad se encuentra el Acuerdo de Puerto Seguro, que se llevó a cabo para permitir transferencias de protección de datos personales de Europa a Estados Unidos. Este acuerdo, el cual tiene cierto grado de contenido autorregulatorio, será expuesto más adelante y presenta justamente la particularidad de resolver por la vía del acuerdo de voluntades, aspectos que la directiva europea no puede, dada su inaplicabilidad extraterritorial.

Otro intento identificado de acercamiento entre la visión europea y la estadounidense es el Sistema de Reglas Transfronterizas de Privacidad (CBPR, por sus siglas en inglés), también un modelo de autorregulación y certificación regional que representa la punta de lanza al crear mecanismos que permiten la interoperabilidad de diversos enfoques de protección de datos y que igualmente será expuesto más adelante.

En este apartado se identificó que el tratamiento de datos personales es un fenómeno internacional que requiere soluciones del mismo alcance, más allá de los límites inherentes a las regulaciones y autoridades nacionales. Sin descartar que en un futuro no muy lejano, la propia industria más que los gobiernos impulsen la creación de un estándar internacional, y dado que los avances tecnológicos no esperan, consideramos que deben buscarse alternativas que brinden soluciones a corto plazo, como podría ser la interoperabilidad entre modelos, a través de mecanismos de autorregulación.

III. LA AUTORREGULACIÓN COMO SOLUCIÓN

A partir de la consideración de que lograr un estándar internacional en materia de protección de datos aplicable a todos los países no es cercana aún, creemos que en el actual escenario internacional en el cual convergen distintos puntos de vista en relación con la protección de datos, la interoperabilidad propuesta puede alcanzarse a través de la autorregulación. Esta permite ampliar las garantías para los individuos más allá de las fronteras nacionales. Para apoyar dichas aseveraciones, a continuación se desarrollarán los conceptos de autorregulación, se identificarán algunas de sus características, posibles beneficios y se expondrán algunos ejemplos.

A. Una definición para el concepto "autorregulación"

Para Stefano Rodotà, la autorregulación es un concepto que puede comprenderse mejor al hablar, simultáneamente, de la ley o de regulación. La ley —o *hard law*— tiene una fuente pública y centralizada: el Estado; mientras que la autorregulación —o *soft law*—, tiene una fuente privada de múltiples actores[15]. Otra definición oportuna es la siguiente: "[...] al hablar de "códigos de conducta" nos podemos referir a reglas de comportamiento no exigidas por la ley, pero voluntariamente establecidas por los interesados, quienes dan publicidad a su compromiso de actuar conforme a esas reglas"[16].

Ya en el marco de la protección de datos, de conformidad con el Documento número 7 del grupo de trabajo de autoridades de protección de datos previsto en el art. 29 de la Directiva 95/46/CE (Grupo de Trabajo del Artículo 29), se define como código de autorregulación a "cualquier conjunto de normas de protección de datos que se apliquen a una pluralidad de responsables del tratamiento que pertenezcan a una misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por miembros del sector industrial o profesión en cuestión". De esta manera, podríamos concluir que la autorregulación es un conjunto de normas en una materia específica —en este caso, en materia de protección de datos personales— desarrolladas y obedecidas de manera voluntaria por quienes las desarrollan, es decir, por quienes tratan datos personales.

B. Autorregulación en materia de protección de datos personales

Al respecto, es oportuno señalar que en diversas regulaciones el término "tratamiento de datos personales" se entiende como cualquier operación que se realice en relación con datos personales de los individuos, es decir, con cualquier información relacionada con una persona física identificada o identificable. El tratamiento contempla desde la obtención, uso, modificación y transferencia hasta la cancelación o eliminación de los datos personales[17]. En este sentido, cualquier aspecto relacionado con la forma en que los datos personales son tratados podría ser autorregulado por los propios individuos que realizan el tratamiento de datos personales, más allá de lo que prevén las regulaciones emitidas en la materia por la autoridad reguladora de determinado Estado. Las personas físicas y morales que deciden sobre el tratamiento de datos personales podrían establecer reglas autoimpuestas para, por ejemplo, exigir consentimiento expreso siempre que sean tratados datos personales que afecten la esfera más íntima de una persona o datos sensibles[18], o cumplir con determinado estándar de

15 RODOTÀ, Stefano, "Códigos de conducta: entre hard law y soft law", en REAL PÉREZ, Alicia (coord.), Códigos de conducta y actividad económica: una perspectiva jurídica, Madrid, Marcial Pons Ediciones Jurídicas y Sociales, S. A., 2012, pp. 19-21.

16 REAL PÉREZ, Alicia (coord.), Códigos de conducta y actividad económica: una perspectiva jurídica, Presentación, Madrid, Marcial Pons Ediciones Jurídicas y Sociales, S. A., 2012, p. 13.

17 Por ejemplo, de conformidad con el artículo 2 de la Resolución de Madrid, el concepto tratamiento significa "cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización revelación o supresión".

18 De conformidad con el artículo 13 de la Resolución de Madrid, el concepto de datos personales sensibles abarca los datos de carácter

seguridad para los datos personales. Así, aquellas personas físicas o morales que desarrollen normas sobre cómo realizar el tratamiento de datos personales —en cualquiera de sus fases—, y voluntariamente las obedezcan, se estarían autorregulando en la materia.

C. Algunas características de la autorregulación

Como característica fundamental de la autorregulación en materia de protección de datos se encuentra la fuente de esta, es decir, son los propios sujetos regulados los que crean —y se someten voluntariamente— a la normatividad en la materia. Muchas veces intervienen en su creación algunos otros actores, incluyendo al propio Estado. Con esta definición, es válido interpretar que un código o instrumento de autorregulación puede ser adoptado, tanto por una empresa, por un pequeño grupo de empresarios del mismo sector como por todas las empresas de un sector determinado —incluso a nivel regional o internacional—, solo refiriéndonos al sector empresarial. Esto no significa que entidades de otros sectores, como el social o hasta el público, estén impedidas para adoptar esquemas de autorregulación.

De ella se deriva una segunda característica: la voluntariedad, que hace alusión a que la adhesión a determinado mecanismo de autorregulación es potestativa, así como el retiro de este de manera oportuna, es decir, sin mediar violaciones o posibles violaciones al mismo. Una tercera característica es que la autorregulación tiene la posibilidad de acercarse más a la realidad del objeto regulado, en virtud de que por ser los propios regulados quienes la crean, conocen mejor la naturaleza de sus actividades, es decir, son más reglas especializadas. Subrayamos una cuarta característica: tiene mayor flexibilidad para adaptarse al cambio en razón de que debe pasar por un proceso legislativo como en el caso de las leyes.

D. Beneficios de la autorregulación

Como incentivos principales para que las organizaciones se autorregulen en materia de protección de datos personales, enunciamos cuatro: i) Distinguirse frente a sus clientes como organizaciones seguras y preocupadas por garantizar la seguridad de la información de aquellos, lo que fortalece su reputación; ii) Contar con mecanismos de prueba adicionales que les permitan acreditar ante las autoridades de privacidad o protección de datos el debido cumplimiento de la ley, lo que se encuentra estrechamente vinculado al principio de responsabilidad demostrada o *accountability*; iii) En los casos de empresas transnacionales, la autorregulación permite unificar la política de protección de datos en todo el mundo, y con ello la simplificación de procesos y la eficiencia de los recursos; y IV) La autorregulación podría representar para las autoridades un elemento a considerar para disminuir el monto de sanciones económicas derivadas de

personal i) Que afecten la esfera más íntima del interesado y ii) Cuya utilización indebida pueda dar origen a una indiscriminación ilegal o arbitraria o pueda conllevar un riesgo grave para el interesado. Como ejemplos de datos sensibles, la Resolución de Madrid señala el origen étnico o racial, las opiniones políticas o convicciones religiosas o filosóficas, así como los datos relativos a la salud o a la sexualidad. Por sus características, es común que en diversas regulaciones esta clase de datos personales cuenten con mayor protección en comparación con otra clase de datos personales como, por ejemplo, los datos personales de contacto, cuyo uso no conlleva el mismo riesgo para su titular.

algún incumplimiento a la normatividad en la materia[19].

En el contexto internacional se ha hablado mucho de los beneficios de la autorregulación en materia de protección de datos personales. Por ejemplo, la Red Iberoamericana de Protección de Datos Personales (RIPD), tanto en la Declaración de Cartagena de mayo de 2004[20] como en la Declaración de México de noviembre de 2005[21], ha expresado su importancia. En esta última declaración manifestó que:

> los instrumentos de autorregulación pueden ofrecer un valor añadido en la protección de datos personales, bien porque la iniciativa empresarial pretenda significarse con un elemento de mayor calidad en el trato de los datos de sus clientes, ante la insuficiencia de las regulaciones aprobadas por el Estado o, añadiendo garantías adicionales a las contempladas en tales regulaciones; bien porque permitan adaptar la normativa a las especificidades que presenta el tratamiento de datos en un determinado sector de actividad, de forma que se generen estándares adaptados a las necesidades del sector, que faciliten su cumplimiento.

En esas mismas fechas fue creado por la RIPD un subgrupo encargado de analizar la validez y eficacia de ciertos códigos de conducta o instrumentos análogos.

Por su parte, la Declaración conjunta de la Unión Europea y los Estados Unidos de América sobre comercio electrónico, del 5 de diciembre de 1997, establece la necesidad de "asegurar la protección eficaz del derecho a la intimidad relativo al tratamiento automatizado de datos personales en redes de información globales" y destaca la importancia de la autorregulación como fruto de un acuerdo entre la industria y otros agentes del sector privado.

Por otro lado, la Organización para la Cooperación y el Desarrollo Económico (OCDE) señaló en la "Recomendación del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico"[22], de 1999, que dicha clase de comercio debe llevarse a cabo de acuerdo con principios de privacidad que proporcionen una efectiva y apropiada protección de este derecho a los consumidores. Para tal efecto, sugiere que los Estados, entre otras medidas, revisen, modifiquen y promuevan "prácticas autorregulatorias" para "hacerlas compatibles y aplicables al comercio electrónico". Allí mismo se destaca la importancia de la participación de "representantes de los consumidores en el desarrollo de mecanismos autorregulatorios efectivos que contengan reglas específicas y sustantivas aplicables a los mecanismos de atención de quejas y resolución de disputas".

19 En México, el Reglamento de la LFPDPPP establece, en su artículo 81, lo siguiente: "Cuando un responsable adopte y cumpla un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de la sanción que corresponda, en caso de verificarse algún incumplimiento a lo dispuesto por la Ley y el presente Reglamento, por parte del Instituto. […]".

20 El texto de la Declaración de Cartagena, de 2004, puede ser consultado en el siguiente vínculo electrónico: http://www.redipd.org/actividades/encuentros/III/index-ides-idphp.php

21 El texto de la Declaración de México, de 2005, puede ser consultado en el siguiente vínculo electrónico: http://www.redipd.org/actividades/encuentros/IV/index-ides-idphp.php

22 El texto del documento puede consultarse en el siguiente vínculo electrónico: http://www.oecd.org/sti/consumer/34023784.pdf.

Finalmente, el Marco de privacidad de la APEC de 2005 contempla, dentro de sus orientaciones, que las Economías miembro deben tomar en cuenta para implementar dicho marco, varias opciones para hacerlo efectivo y asegurar la privacidad de los individuos, lo que comprende métodos legislativos, administrativos, autorreguladores de la industria o una combinación de estos.

De esta manera, ya en diversos foros se ha reconocido la importancia de la autorregulación en materia de protección de datos personales.

E. ¿Quién desarrolla el código o instrumento de autorregulación?

Como ya se mencionó anteriormente, de manera general son los propios sujetos regulados quienes crean o se someten a mecanismos de autorregulación, aunque pueden ser involucrados otros actores adicionales. Ello nos lleva a prever que existen distintas modalidades de mecanismos de autorregulación en función de los sujetos involucrados en su producción. Cuando en el desarrollo o conocimiento de los contenidos de un mecanismo de autorregulación se involucra a actores adicionales, incluidos, en su caso, los titulares de los datos, las organizaciones de consumidores, y probablemente a la propia autoridad, ocurre que aumentan las garantías para los titulares de los datos. Ello se infiere, en tanto se reduce la posibilidad de que exista algún conflicto de interés al haber una identidad entre quien crea, aplica y se encuentra sujeto a la norma.

Como un excelente ejemplo de lo anterior están los códigos de conducta regulados en el Capítulo V de la Directiva 95/46/CE, que prevé códigos que afectan a un sector. En este caso se involucra a la autoridad, ya sea comunitaria o nacional, en la evaluación de estos. En palabras de Stefano Rodotá:

> La regulación del procedimiento de elaboración de los códigos de conducta comunitarios y nacionales, contenida en el art. 27 de la Directiva es, precisamente, de carácter multinivel. Se trata de un procedimiento plural, con múltiples sujetos, que implica la colaboración entre organizaciones representativas de los sectores interesados y organismos de control, el grupo de trabajo de autoridades de protección de datos previsto en el art. 29 de la Directiva y las autoridades nacionales de control, que supervisan la conformidad de los códigos a la Directiva y a las leyes nacionales de transposición. Evidentemente, estamos ante códigos que no son expresión de una simple autorregulación de sector, sino el resultado de la colaboración entre sujetos públicos y privados, incluso con diferencias relevantes entre ordenamientos jurídicos [...][23].

En el ámbito del derecho comparado, nos encontramos que para España un código tipo en materia de protección de datos —que puede tener el carácter de código deontológico o de buena práctica profesional— puede ser promovido por una sola empresa o entidad, una asociación o un sector, pero también por administraciones públicas y corporaciones de derecho público. En la regulación de protección de datos de este país[24], alineada a la Directiva

23 RODOTÀ, Stefano, op. cit., nota 11, p. 27.

24 La Ley Orgánica 15/1999 de Protección de Datos Personales (LOPD), en su artículo 32 y el Reglamento de la LOPD, regulan los códigos

95/46/CE, se prevé que dichos códigos sean inscritos en el Registro General de Protección de Datos o en los registros creados por las Comunidades Autónomas, cuando corresponda. El registro señalado podrá denegar la inscripción en él cuando el código presentado no se apegue a las disposiciones legales y reglamentarias en la materia.

En México, la LFPDPPP, en su artículo 44, prevé que las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculantes en la materia, que complementen lo dispuesto por la mencionada Ley. De esta manera, se contempla también que prácticamente cualquier persona física o moral de carácter privado que decida sobre el tratamiento de datos puede desarrollar esquemas de autorregulación como pudieran ser códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos[25]. El mismo artículo prevé que tales esquemas serán notificados de manera simultánea a las autoridades sectoriales correspondientes y al Instituto, lo que implica una participación de la autoridad.

En el caso estadounidense y con la deficiencia inherente de las generalizaciones, podríamos afirmar que la autorregulación es percibida de manera distinta. Difícilmente podemos observar una "autorregulación regulada" como en el caso de España o México, y la participación de una autoridad *ex ante* no está prevista en dichos procesos. Regresamos a la cuestión de diversidad de culturas y enfoques. Al respecto, expondremos más adelante y con mayor profundidad el caso del Acuerdo de Puerto Seguro alcanzado entre Estados Unidos y Europa, a fin de ilustrar un poco más la lógica del esquema estadounidense en cuanto a la autorregulación en materia de protección de datos personales.

F.¿Autorregulación pura o corregulación?

En seguimiento al tema anterior, vale la pena enfatizar que de ninguna manera pensamos que la autorregulación puede o debe sustituir a la ley o regulación emitida por el Estado. Sin embargo, insistimos en la necesidad de que la regulación emitida por el Estado debe ser asertiva al momento de reglamentar cualquier fenómeno social, incluido el relacionado con la protección de datos, y buscar instrumentos que la complementen y faciliten su cumplimiento como en el caso de la autorregulación. De este modo, sostenemos que la regulación y la autorregulación en materia de protección de datos son complementarias[26]. En ello coinciden desde el cate-

tipo, quién los puede suscribir, su contenido y el procedimiento para su inscripción ante la autoridad correspondiente. La Agencia Española de Protección de Datos, autoridad española en la materia para organismos públicos nacionales y privados, ha incluido en su sitio web información para la elaboración de códigos tipo. Asimismo, los códigos tipo inscritos en el Registro General de Protección de Datos pueden ser consultados en dicho sitio

25 No se hace mención a la posibilidad de que entidades gubernamentales puedan adoptar este tipo de mecanismos en virtud de que la mencionada ley no aplica al sector público. Sin embargo y aunque no hay previsión al respecto, no encontramos, por el momento, algún impedimento para que el sector público pueda autorregularse en la materia.

26 Incluso la propia LFPDPPP mexicana reconoce este hecho en el primer párrafo de su artículo 44, que establece: "Artículo 44. Las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley. […]

drático Stefano Rodotà[27] hasta el propio Peter Fleischer, responsable mundial de privacidad de Google[28]. Cada uno tiene virtudes propias: la especialidad, flexibilidad y potencial alcance transnacional de la autorregulación versus el respaldo de la maquinaria estatal en el caso de la ley.

La autorregulación pura, entendida como aquellas normas creadas por los propios sujetos regulados, en la cual no interviene algún tercero —o autoridad— en ningún momento, podría carecer de la fuerza y el compromiso requeridos para presentarse como una herramienta eficaz. Es por ello que se exige un mínimo de reglas que garanticen la eficacia de los propios esquemas de autorregulación. Bajo esta óptica es que nos referimos a una corregulación más que a una autorregulación pura, ya que una parte de la reglamentación nace de una fuente privada que es el acuerdo de voluntades de un sector concreto para adecuarse a la norma general emitida por el Estado, logrando ir más allá en la consecución de garantías reforzadas para los individuos usuarios de los servicios del sector de que se trate.

De esta manera, el contenido de los códigos de autorregulación puede variar según las características de sus promotores y de su entorno. De hecho, la intención de los códigos o instrumentos de autorregulación es ampliar o adecuar los preceptos de la regulación nacional en la materia, de conformidad con las peculiaridades del sector. En este caso, las empresas buscan dar constancia a sus clientes de su interés en proteger aspectos de estos que van más allá de la normativa, por ejemplo, mecanismos eficientes de resolución de controversias que ofrezcan directamente a los titulares, alternativas que permitan el ejercicio de sus derechos de protección de datos personales sin la intervención de la autoridad. No obstante lo anterior, también es viable que las empresas adopten códigos u otros instrumentos de autorregulación para reglar materias que no están normadas por la regulación nacional.

Existen regulaciones nacionales que establecen contenidos obligatorios —y potestativos— para estos instrumentos como sucede en España. En el caso de México, la LFPDPP prevé que la Secretaría de Economía, en coadyuvancia con el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), el órgano garante de la protección de datos en México, fije los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere la misma Ley. De esta manera, la propia LFPDPPP, su reglamento y los parámetros antes mencionados generarán ese marco mínimo de reglas en donde deben moverse los esquemas

27 Stefano Rodotà señala que la relación ente el hard law y el soft law ha sido presentada en ocasiones como una relación de conflicto pero que, en la actualidad, la relación es más de complementariedad "si se atiende al resultado del sistema jurídico más que la forma de los instrumentos utilizados". RODOTÀ, Stefano, op. cit., nota 11, p. 22.

28 Al responder una pregunta sobre la relación entre la regulación y la autorregulación, durante una conferencia que pronunció en inglés, en marzo de 2009, Peter Fleischer manifestó: "[…] Usted ha dicho que la autorregulación y la regulación son complementarias. Sí, por supuesto. Y yo las veo interactuar de la siguiente manera. Para mí, un código de conducta se instaura para satisfacer necesidades específicas. Las leyes tienen que ser muy amplias, tienen que ser muy generales. En cambio, los códigos de conducta pueden ser más específicos, con ellos se puede profundizar en los temas comunes y particulares de cada sector. Creo que esta es una razón muy útil pues los códigos de conducta se pueden desarrollar y enmendar más rápidamente, pueden resolver un problema. […] . FLEISCHER, Peter, "On Line Privacy and Codes of Conduct", en Códigos de conducta y actividad económica: una perspectiva jurídica, Madrid, Marcial Pons Ediciones Jurídicas y Sociales, S. A., 2012, pp. 147-148.

de autorregulación que deseen ser reconocidos por la autoridad y establecerán el contenido básico de los esquemas de autorregulación[29].

En este apartado, nos parece oportuno referir algunos principios que hemos identificado como especialmente relevantes y que necesariamente deben preverse al desarrollar mecanismos de autorregulación que busquen mayor eficacia, y cuyo cumplimiento no solo se base en la buena fue de quienes se adhieren a ellos: i) La obligatoriedad, que hace alusión a la naturaleza vinculante por parte de aquellos que han decidido adherirse voluntariamente a un esquema de autorregulación y la necesidad de sanciones en caso de incumplimiento, ii) La transparencia, entendida como la necesidad de hacer del conocimiento de todos aquellos sujetos interesados, el contenido del mecanismo de autorregulación, y iii) La continua evaluación de la eficacia del mecanismo adoptado.

En relación con este último punto, que estimamos de importancia toral, profundizamos en el sentido de que la evaluación de los códigos o instrumentos de autorregulación es indispensable para que estos alcancen su objetivo. Esta evaluación se refiere, entre otros aspectos, al propio contenido del mecanismo y su concordancia con la regulación existente en la materia, en caso de que la hubiera; al nivel de obediencia general por parte de los adheridos y al apoyo o ayuda prestados en el marco del mecanismo de autorregulación a los titulares de los datos que sufran algún problema relacionado con el tratamiento de sus datos.

29 Artículo 43, fracción V de la LFPDPPP.

Una vez adoptada una definición del concepto autorregulación y de haber expuesto sus características, de conocer la relación complementaria entre la ley y la autorregulación, así como de establecer los principios básicos sobre los que se montan los mecanismos eficaces de autorregulación, consideramos relevante exponer tres ejemplos representativos de mecanismos de autorregulación que pretenden solucionar el aspecto del fenómeno transnacional de la protección de datos.

IV. EJEMPLOS REPRESENTATIVOS

A continuación exponemos tres ejemplos relevantes de mecanismos de autorregulación que aportan elementos de acercamiento entre países que no comparten la misma visión sobre la protección de datos personales. Ellos permiten la interoperabilidad de distintos regímenes y proveen las condiciones requeridas para realizar transferencias internacionales de información personal, sin sacrificar la protección de la privacidad de los individuos. Aunque necesariamente las partes involucradas se ven obligadas a ceder en ciertos aspectos, como sucede en cualquier negociación justa, esto no implica la imposición de un único modelo o visión.

A. El Acuerdo de Puerto Seguro entre Estados Unidos y la Unión Europea (Safe Harbor Framework)

Como ya expusimos anteriormente, Estados Unidos de América y la Unión Europea sostienen ciertas diferencias relacionadas con la protección de datos. Esta situación, la cual aparente-

mente no debiera generar mayores consecuencias, creó una indiscutible tensión en lo que se refiere a la transmisión de datos personales desde un Estado miembro de la Unión Europea hacia los Estados Unidos de América. Lo anterior, debido a que la Directiva 95/46/CE referida anteriormente establece, en su Capítulo IV, artículo 25, que los datos personales en posesión de cualquier sujeto obligado dentro de la Unión Europea podrán ser transmitidos, sin la autorización previa de la autoridad de protección de datos de cada Estado miembro, a aquellos países fuera del espacio europeo únicamente cuando dichos países garanticen una adecuada protección a la privacidad[30].

Inicialmente, esta protección se garantizaba al contar con una regulación nacional que contemplara prácticamente los mismos aspectos integrados en la propia Directiva 95/46/CE (lo que podría significar una especie de estandarización), requisito no satisfecho por Estados Unidos, por lo que las transmisiones de datos personales a este país generaban un riesgo legal a cualquier sujeto obligado de la Unión Europea. Derivado de lo anterior y con la intención de garantizar a la Unión Europea los niveles de seguridad requeridos por la Directiva 95/46/CE, sin acceder a cambiar de manera radical su regulación interna para adecuarla a un modelo con el que no comulgan, las autoridades comerciales de Estados Unidos desarrollaron una solución intermedia a través del Acuerdo de Puerto Seguro, aprobado por la Unión Europea en el 2000, lo que permitió el intercambio de información de datos personales entre Europa y las empresas estadounidenses que estuvieran inscritas en dicho acuerdo[31].

El Acuerdo de Puerto Seguro es un procedimiento anual que las empresas en Estados Unidos que así lo deseen pueden seguir ante las autoridades de comercio, y que implica su autocertificación del cumplimiento de una serie de principios internacionales de privacidad establecidos en la Directiva 95/46/CE[32]. El gobierno de Estados Unidos cuenta con una lista de las empresas adheridas al marco normativo de dicho acuerdo, con lo que se facilita el conocimiento sobre si una empresa se encuentra autocertificada. Para calificar en el programa una empresa puede: i) adherirse a un mecanismo de autorregulación —tal como algún programa de sello de privacidad— que satisfaga los requerimientos del Marco de Puerto Seguro o ii) desarrollar su propia política de autorregulación que satisfaga los requerimientos del Marco.

Entre los requisitos que deben satisfacer los mecanismos de autorregulación autocertificados en el Marco de Puerto Seguro se encuentra un procedimiento de resolución de controversias que investigue y resuelva sobre quejas individuales, así como procedimientos de verifica-

30 Este principio tiene muy pocas excepciones, como es el caso de que la transmisión de información se realice con consentimiento del titular de la información, tal como lo establece la Directiva 95/46/CE, en su artículo 26(1)(a). La declaratoria de país adecuado a la Directiva 95/46/CE la realiza la Comisión Europea, luego de un exhaustivo análisis del marco normativo integral en materia de protección de datos. Los países que actualmente cuentan con el nivel adecuado pueden ser consultados en el sitio internet (en inglés): http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm, a julio de 2012.

31 Para mayor información, consultar el sitio internet (en inglés) del Marco del Puerto Seguro: http://www.export.gov/safeharbor/doc_ safeharbor_index.asp, a julio de 2012.

32 Tales como el de información, calidad, seguridad, opción y acceso.

ción de cumplimiento. También se les requiere prever sanciones y la reparación del daño para el caso de algún incumplimiento derivado de los principios previstos. La sanción debe ser lo suficientemente severa para asegurar el cumplimiento por parte de la empresa y deberá incluir la publicidad del incumplimiento y la correspondiente cancelación de datos, bajo ciertas circunstancias. Asimismo, puede implicar la suspensión de la membresía de la empresa a algún programa de privacidad y, por lo tanto, del programa de Puerto Seguro.

Igualmente, dependiendo del sector, alguna autoridad tal como la Comisión Federal de Comercio u otra equivalente federal o estatal, puede exigir el cumplimiento del Marco de Puerto Seguro. Cuando una empresa se encuentre comprometida con un determinado sistema de autorregulación en cumplimiento del Marco de Puerto Seguro e incumpla con dicha autorregulación, el incumplimiento podrá ser sancionado en términos de una ley federal o local que prohíba actos injustos o engañosos. Tanto la Comisión Federal de Comercio como el Departamento de Transporte han manifestado a la Comisión Europea que realizarán las acciones necesarias frente a las empresas que manifiesten su cumplimiento del Marco de Privacidad de Puerto Seguro y no honren dicha manifestación.

Las empresas reincidentes no podrán recibir los beneficios que aporta el Marco de Puerto Seguro y dicha circunstancia deberá hacerse de conocimiento de la autoridad. En este caso, el Departamento de Comercio indicará en una lista pública cualquier notificación que reciba en este sentido y aclarará cuáles empresas no podrán ser objeto de los beneficios del Marco de Puerto Seguro. En caso de que una empresa desee autocertificarse nuevamente, deberá proveer suficiente información sobre su anterior participación en el programa.

Por lo descrito en este apartado, identificamos en el Acuerdo de Puerto Seguro varios elementos relevantes. En primer lugar, la voluntariedad por parte de las empresas estadounidenses para autocertificarse ante el programa; en segundo lugar, una serie de requisitos de forma y de fondo que deben ser satisfechos por las empresas autocertificadas, es decir, estas deben comprometerse con el cumplimiento de principios previstos en la Directiva 95/46/CE y con la realización y adopción de determinados procedimientos; por último, se prevé la participación de la autoridad en la administración de la lista de empresas autocertificadas, pero principalmente en la sanción de aquellas que no cumplan el programa, o mejor, que no honren sus promesas relacionadas con la protección de los datos ante los consumidores.

En este último punto encontramos un elemento característico de la visión estadounidense, en el sentido de que el sistema de autorregulación basado en el Acuerdo de Puerto Seguro —como otros existentes en diversas materias— se basan en la buena fe de quien se adhiere a ellos. Una cuestión sin lugar a dudas cultural donde la confianza es fundamental. Esto se traduce en que la actuación *ex ante* de la autoridad es prácticamente nula, con el objeto de no intervenir en el cauce de la ley de la oferta y la demanda. Solo en el caso de existir algún incumplimiento por parte del proveedor a sus promesas frente

a los consumidores, las autoridades de comercio y otras competentes aplicarían todo el rigor de la ley sancionando actos considerados como desleales o engañosos para el consumidor —*actuación ex post*—, más que violaciones a un derecho fundamental.

B. Reglas corporativas vinculantes (Corporate Binding Rules)

Las reglas corporativas vinculantes (BCR, por sus siglas en inglés) son normas internas —tal como códigos de conducta— adoptadas por un grupo empresarial de carácter multinacional, que determinan la política de privacidad de dicho grupo en relación con el tratamiento de datos personales. En especial, establecen aspectos relacionados con las transferencias internacionales de datos entre empresas del mismo grupo ubicadas en países que no provean un nivel adecuado de protección, de conformidad con la Directiva 95/46/CE, tal y como se señala en los primeros dos párrafos del apartado anterior.

Las BCR son adoptadas voluntariamente por aquellas compañías multinacionales que deseen acreditar suficientes garantías de una adecuada protección a la privacidad y a derechos y libertades fundamentales, para satisfacer el supuesto del apartado 2 el artículo 26 de la mencionada directiva. De esta manera, las BCR afirman que las transferencias internacionales de datos entre empresas del grupo que las adopta son seguras y que garantizan un nivel adecuado de protección de datos personales. Esto se presenta como una alternativa más para empresas ubicadas en el espacio económico europeo que realizan transferencias de datos personales a empresas ubicadas en países que no satisfacen el nivel adecuado de protección de conformidad con la Directiva 95/46/CE. La adopción de BCR les permite evitar la posible carga que representa firmar cláusulas contractuales tipo, solicitar la autorización de la transferencia a la autoridad de protección de datos, o bien solicitar el consentimiento de los titulares cada vez que tengan la intención de realizar transferencias internacionales de datos personales a empresas que pertenezcan al mismo grupo que no estén ubicadas en la zona económica europea. Las transferencias internacionales de datos hacia empresas que no pertenezcan al mismo grupo no se encuentran cubiertas por las BCR[33].

Aquellas empresas cuyas BCR hayan sido evaluadas y aprobadas de conformidad con el procedimiento ante autoridades europeas para ello establecidas, serán habilitadas para realizar transferencias internacionales de datos entre ellas. Otros beneficios identificados para las empresas que cuentan con BCR consisten en permitirles armonizar sus prácticas de protección de datos, prevenir riesgos derivados de las transferencias internacionales de datos, comunicar al exterior las políticas de privacidad adoptadas por el grupo y contar con directrices de actuación para sus empleados en relación con el tratamiento de datos personales.

En el caso de las BCR se identificó una alternativa europea al Acuerdo de Puerto Seguro para las transferencias de datos desde países europeos

33 Para mayor información, consultar el sitio internet (en inglés): http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm, a julio de 2012 o el documento de trabajo número 74 del Grupo de Trabajo del Artículo 29.

a empresas ubicadas en países que no garantizan un nivel adecuado de protección, de conformidad con la Directiva 95/46/CE. En este caso, existe también el elemento de voluntariedad por parte de los grupos empresariales de carácter internacional para desarrollar y adoptar sus BCR; igualmente, existe una serie de requisitos de forma y de fondo que deben ser satisfechos por estos grupos, que incluyen también el cumplimiento de principios previstos en la Directiva 95/46/CE, así como la realización y adopción de determinados procedimientos; por último, coincidentemente, se prevé la participación de autoridades de protección de datos europeas. No obstante, en relación con este último punto, las autoridades europeas tienen una fuerte presencia *ex ante* respecto de las BCR, que involucra su evaluación y aprobación. De nuevo aparece el factor cultural reflejado en el hecho de que la tutela de un derecho fundamental de ninguna manera puede dejarse únicamente al devenir de las leyes del mercado.

A decir de José Luis Piñar Mañas, catedrático de Derecho Administrativo y exdirector de la Agencia Española de Protección de Datos:

> Finalmente, el instrumento de las BCR se admitió como complemento del marco regulador. [...]. Ése es, quizá, el futuro a seguir: potenciar y fomentar el juego entre regulación y autorregulación, revisando la teoría de las fuentes, dando paso a la regulación y reconocimiento de los códigos de conducta, pero dando asimismo la última palabra a las normas jurídicas, y en primer término a la Ley, sobre todo cuando (y este es nuestro caso) hablamos de un derecho fundamental, como es el derecho a la protección de datos, cuya definición y garantía no puede dejarse en manos de la autorregulación, pero cuya efectividad depende en gran medida de instrumentos como los códigos de conducta[34].

C. Sistema de reglas transfronterizas de privacidad (Cross Border Privacy Rules System)

En 2004, los ministros de las veintiuna economías del APEC avalaron el *Marco de Privacidad del organismo,* mismo que se compone de un conjunto de nueve principios orientadores y una guía de implementación para ayudar a sus miembros a desarrollar enfoques nacionales para la protección de los datos personales. Uno de los objetivos del marco es avanzar en la creación de mecanismos regionales para promover y fortalecer la privacidad de los individuos, además de mantener la continuidad de los flujos de información entre sus economías y otros socios comerciales. Destaca como uno de estos mecanismos el Sistema de Reglas Transfronterizas de Privacidad (CBPR, por sus siglas en inglés), desarrollado por el Subgrupo de Privacidad de APEC (DPS, por sus siglas en inglés)[35]. Dicho sistema es un proyecto regional cuyo objetivo principal es facilitar el flujo de información entre respon-

34 PIÑAR MAÑAS, José, "Códigos de conducta y espacio digital. Especial referencia a la protección de datos", en: REAL PÉREZ, Alicia (coord.), Códigos de conducta y actividad económica: una perspectiva jurídica, Madrid, Marcial Pons Ediciones Jurídicas y Sociales, S. A., Madrid, 2012, pp. 176-177.

35 En el marco de las actividades de APEC —establecido desde 1989 y dedicado a facilitar y fomentar el crecimiento del comercio y la inversión en la región Asia-Pacífico— se encuentra el Comité Ejecutivo de Comercio Electrónico (ECSG, por sus siglas en inglés) que promueve el desarrollo de esta actividad a través del impulso de ambientes legales, regulatorios y de políticas públicas. Dentro del ECSG, se encuentra el DPS cuyo trabajo en privacidad y protección de datos es consistente con el marco normativo de APEC, evitando barreras innecesarias al comercio entre las economías Miembros de APEC pero garantizando la privacidad de los individuos.

sables ubicados en distintas economías de la región reconocidos por cumplir con el Marco de Privacidad de APEC.

Una vez concluidos los trabajos que definieron teóricamente el sistema CBPR, en septiembre de 2011 (San Francisco, Estados Unidos), fue ratificada, en noviembre de ese mismo año, en Honolulú, Hawaii, la *Declaración de los líderes de APEC* que contiene el compromiso de implementar el sistema CBPR para reducir las barreras al flujo de información, proteger la privacidad de los consumidores y promover la interoperabilidad entre los regímenes de privacidad que prevalecen en la región.

Las economías APEC que así lo decidan pueden participar en el sistema CBPR una vez manifiesten su interés y el DPS, a través del Panel Conjunto de Supervisión (JOP, por sus siglas en inglés), haya evaluado y aceptado dicha solicitud, supuesto que procede cuando la economía postulante acredite satisfacer los requisitos para ello establecidos[36]. El sistema CBPR se compone de diversos niveles: i) Responsables/organizaciones certificadas, ii) Terceros certificadores (AA, por sus siglas en inglés), iii) Autoridades de privacidad o protección de datos nacionales y iv) El propio DPS, con el JOP como su órgano ejecutivo.

El sistema CBPR parte de la existencia de un conjunto de reglas y políticas de protección de datos personales —apegadas al Marco de Privacidad de APEC— desarrolladas por aquellas organizaciones que tratan datos y los transfieren a través de las fronteras. Dichas reglas y políticas deben ser validadas por un tercero certificador y son la base para la cooperación entre autoridades de privacidad de las economías APEC. El sistema tiene cuatro componentes principales: i) La autoevaluación de dichas reglas y políticas, ii) La revisión de cumplimiento, iii) El reconocimiento o certificación y iv) La resolución de controversias o exigibilidad.

Identificamos en el sistema CBPR elementos relevantes: la voluntariedad también está presente; igualmente se prevén requisitos de forma y de fondo que deben ser satisfechos por las economías participantes y por otros actores, como los terceros certificadores, que tienen una función primordial en el sistema al ser quienes revisan y acreditan el cumplimiento por parte de las empresas, de los requisitos establecidos en el programa. Finalmente, también se prevé la participación de las autoridades de protección de datos de las economías participantes, para valorar a quienes desean ser reconocidos por terceros certificadores en el sistema CBPR, a través del JOP, para atender quejas no resueltas por las empresas ni por los terceros certificadores y, cuando sea requerido, para realizar investigaciones y sancionar.

36 Como el hecho de contar con normas nacionales que se apeguen al Marco de Privacidad de APEC; que cuenten con al menos una autoridad que permita la verificación de dichas normas, que haya suscrito el Acuerdo de Cooperación para la Ejecución de Privacidad Transfronteriza entre Autoridades de Privacidad de APEC (CPEA, por sus siglas en inglés); y que se haya identificado en la economía postulante, al menos un posible tercero certificador.

Cobra especial importancia en el sistema la cooperación internacional entre autoridades de la región Asia-Pacífico para la vigilancia y supervisión del sistema. Ello, independientemente del acercamiento que cada Economía pudiera tener respecto a la protección de datos. Efectivamente, la propia normatividad del sistema señala que este no desplaza ni modifica leyes o regulaciones locales de las Economías miembros; de hecho, las complementa. En el caso de que la regulación de privacidad doméstica exceda lo previsto en el sistema CBPR, las disposiciones de dicha regulación continuarán siendo aplicables en su totalidad. Por el contrario, cuando sean las disposiciones del sistema CBPR las que excedan lo dispuesto por leyes locales, los actores que deseen operar dentro del mencionado sistema en las Economías donde se prevean dichas leyes deberán sujetarse voluntariamente a aquellos requerimientos adicionales previstos por el programa.

Es por lo anteriormente presentado que se ha insistido en que el sistema CBPR es un modelo de autorregulación y certificación regional, que representa una importante tendencia en mecanismos que permiten la interoperabilidad de diversos sistemas de protección de datos sin imponer un modelo único, lo que significa la interacción entre distintas visiones, culturas y acercamientos al fenómeno de la privacidad y protección de datos. Debido a que el sistema CBPR ya está terminado en su fase teórica, aún falta ponerlo en práctica y analizar su posible comunicación con otros sistemas como el europeo, que es la intención del Subgrupo de Privacidad de APEC. Estados Unidos es la primera Economía que ha solicitado participar en el programa y también es intención de México hacerlo. Por el momento, habrá que estar atentos a la entrada en operación del sistema antes de aseverar que se antoja el modelo a seguir, aunque hay excelentes expectativas.

V. CONCLUSIONES

Es innegable que la explotación de la información personal ha crecido de manera exponencial, debido a que se trata de un fenómeno ínti-

mamente relacionado con el comercio internacional y las tecnologías de la información y las comunicaciones. El derecho y sus mecanismos tradicionales de creación, implementación y observancia se han visto rebasados por la espiral globalizadora, por ello, resulta indispensable iniciar la discusión desde el ámbito jurídico de la adecuación de los marcos normativos ya sea nacionales o supranacionales, para dar asidero a nuevas figuras como la autorregulación vinculante, cuyas características y alcances permitirán la mejor observancia de las leyes.

No cabe duda de que el compartir entre las naciones, industria e individuos distintas visiones sobre la privacidad y la protección de datos desde un enfoque cosmopolita, permitirá poner a prueba nuevas formas de resolver conflictos en el terreno de lo práctico más que del deber ser o la teoría, sobre todo ante fenómenos como el del cómputo en la nube. Como vimos, un ejemplo muy claro de enfoques pragmáticos es el acercamiento a la protección de datos de la Unión Europea y la de Estados Unidos de América, ya que estaba claro para los funcionarios gubernamentales, tanto de Washington como de Bruselas, que el comercio y el crecimiento económico transatlántico no podía detenerse por las que pudieran considerarse barreras encubiertas en nombre de la privacidad y la protección de datos.

También observamos que tanto la estandarización de la normativa para la protección de datos como la interoperabilidad de los distintos modelos ofrecen posibles soluciones para dichas interrogantes, siendo esta última la que nos parece más viable y cercana. Lograr que los distintos Estados acuerden una misma concepción y regulación requerida para la estandarización se antoja aún algo lejano. En cambio, la interoperabilidad, entendida como el reconocimiento mutuo de distintos modelos o visiones a partir de las coincidencias, parece ofrecer una solución hacia una comunicación más tangible.

La autorregulación, por su parte, aporta a la interoperabilidad una herramienta invaluable. Sus características de voluntariedad, especialización, flexibilidad y potencial largo alcance (inclusive transnacional) pueden ser retomadas —ya lo han sido— por sistemas de autorregulación que permiten ampliar la protección de datos personales más allá de las fronteras. Al respecto, es indispensable dejar en claro que aunque existen tantas formas de autorregulación como sujetos susceptibles de adherirse a ellas, nosotros hacemos especial alusión a aquellos sistemas o mecanismos de autorregulación que cuentan, además, con ciertos parámetros mínimos. Nos referimos a ciertos contenidos, procedimientos y autoridades que respalden y vigilen en un último nivel su debido funcionamiento, y siempre considerando la autorregulación como un aspecto complementario a los propios sistemas jurídicos existentes.

Se considera como de avanzada el modelo mexicano de autorregulación previsto por la propia ley y desarrollado en el Reglamento de manera armónica con el principio de responsabilidad o rendición de cuentas por parte del responsable del tratamiento de datos. Lo anterior es así ya que no se deja enteramente a la voluntad de las partes el cumplir con puntos mínimos regulatorios, sino que se abre la puerta para añadir

novedosos esquemas de complementariedad y especialización de aspectos que la norma no prevé. Por su parte, los modelos europeo y de Asia-Pacífico nos brindan un abanico de opciones a ser considerado para la emisión de los parámetros de autorregulación correspondiente.

En toda esta discusión no debe perderse de vista que el valor jurídico tutelado por la norma es el de la autodeterminación informativa y, por ende, el derecho a la privacidad y la protección de datos, ya que la información presente, pasada y futura de los individuos se encuentra concentrada en apenas una veintena de compañías que monopolizan la explotación de perfiles y los diferentes usos secundarios que pueden exprimirse, literalmente, a los datos con fines de venta de bienes o servicios. En no pocas ocasiones la minería de datos y la publicidad acarrean afectaciones a la dignidad humana ante la discriminación o el impedimento para el goce de otros derechos y libertades.

Para las autoridades de protección de datos debiera ser una prioridad el promover la adopción de esquemas de autorregulación por parte de los sujetos a quienes aplica la norma, lo que permitiría un bajo nivel contencioso ante dichas autoridades y un alto nivel de acatamiento de las disposiciones. El modelo de APEC permite vislumbrar que en un futuro cercano, cuando la Secretaría de Economía y el IFAI operen los parámetros de autorregulación publicados oficialmente el 17 de enero de 2013, que desarrollan el modelo de certificación de empresas que demuestren su cumplimiento con la ley, México, por el número de empresas que cumplan con garantizar la protección de datos, sea considerado un puerto seguro para atraer inversión extranjera directa de Canadá, Rusia o Japón, por mencionar algunas economías de APEC. Al mismo tiempo, se debe buscar obtener por parte de la Unión Europea el nivel de adecuación que muestre a México como un país que garantiza la debida protección de la información personal, dejando atrás la mala reputación de paraíso de datos.

Algunas propuestas ya están en la mesa. Ahora solo falta vigilar su desempeño e implementar mejoras que permitan perfeccionar un régimen global de protección de datos personales para todos y cada uno de los ciudadanos del mundo digital.

VI. REGULACIÓN CONSULTADA

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

Convenio nº. 108 del Consejo de Europa, del 28 de enero de 1981.

Carta Europea de Derechos Fundamentales, del 2000.

Estándares internacionales sobre la protección de datos personales y privacidad “Resolución de Madrid”.

Directrices para la protección de la intimidad y el flujo transfronterizo de datos personales de la OCDE, de 1980.

Declaración de Cartagena de la Red Iberoamericana de Protección de Datos Personales, de 2004.

Declaración de México de la Red Iberoamericana de Protección de Datos Personales, de 2005.

Marco de privacidad de APEC, de 2005.

Recomendación del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico, de 1999.

Constitución Política de los Estados Unidos Mexicanos.

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

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

Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Reglamento de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Ley de Portabilidad y Responsabilidad de Seguros de Salud, de Estados Unidos de América.

Ley para la Protección a la Privacidad Infantil en Línea, de Estados Unidos de América.

Ley de Transacciones de Crédito Equitativas y Precisas, de Estados Unidos de América.

Bibliografía

Arenas Ramiro, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, 2006.

Canales Gil, Álvaro, El derecho fundamental a la protección de datos de carácter personal, *Revista Jurídica de Castilla y León*, nº. 12, abril 2007.

Davara Rodríguez, Miguel Ángel, *Nueva guía práctica de protección de datos. Desde la óptica del titular del fichero*, Madrid, Editorial ASNEF, 2001.

Gómez Robledo, Alonso y Ornelas Núñez, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, UNAM, Instituto de Investigaciones Jurídicas, 2006.

Higuera Pérez, Melissa, *El derecho a la protección de datos personales en México: diagnóstico y perspectiva,* tesis de Licenciatura, México, ITAM, 2009.

Naciones Unidas*, Manual de privacidad del curso en línea Aspectos Legales del Comercio Electrónico*, Conferencia de las Naciones Unidas sobre el Comercio y Desarrollo, México, 2007.

Ovilla Buenos, Rocío, *La protección de datos personales en México*, México, Editorial Porrúa, 2005.

Palazzi, Pablo, *La transmisión internacional de datos personales y la protección de la priva-*

cidad, Buenos Aires, AD-HOC S. R. L., 2002.

REAL PÉREZ, Alicia (coord.), *Códigos de conducta y actividad económica: una perspectiva jurídica,* Madrid, Marcial Pons Ediciones Jurídicas y Sociales, S. A., 2012.

SOLOVE, Daniel J. *The Digital Person. Technology and privacy in the information age*, Nueva York, New York University Press, 2004.

TRONCOSO REIGADA, Antonio. La *protección de datos personales. En busca del equilibrio*, Valencia, Tirant lo Blanch, 2010.

VUKOWICH, William T., *Consumer Protection in the 21st Century. A Global Prospective*, Estados Unidos de América, Transactional Publishers, Inc., 2002.