Esta obra forma parte del acervo de la Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM

www.juridicas.unam.mx

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES: SU PROTECCIÓN EN EL ÁMBITO DEL COMERCIO INTERNACIONAL Y DE SEGURIDAD NACIONAL

Lina Ornelas Núñez*

Edgardo Martínez Rojas**

SUMARIO: I. *Introducción.* II. *Actualidad del derecho a la protección de datos en México.* III. *Concepto y tipos de transferencias internacionales de datos personales.* IV. *Conclusiones.* V. *Bibliografía.*

I. Introducción

En las últimas décadas el desarrollo científico ha abierto una brecha tecnológica sin precedentes llevando al ser humano a explorar terrenos hasta ahora desconocidos, lo cual ha impactado significativamente y de diversas formas en el tejido social, provocando con ello la necesidad de conducir dentro de los causes del derecho esta nueva realidad. Dicho impacto se ha presentado como un fenómeno que trasciende fronteras y no sólo con un matiz doméstico, en el que es posible, gracias a los avances de la ciencia, intercambiar información a través de los medios telemáti-

* Abogada egresada de la Facultad de Derecho de la Universidad de Guadalajara; maestra en Cooperación legal internacional por la Universidad Libre de Bruselas *(Vrije Universiteit Brussel)*; coordinadora de subgrupos de trabajo de la Red Iberoamericana de Protección de Datos. Actualmente es directora general de clasificación y datos personales del Instituto Federal de Acceso a la Información Pública (IFAI).

** Abogado egresado de la Escuela Libre de Derecho; candidato a doctor por la Universidad San Pablo CEU, Madrid, España. Actualmente es subdirector de protección de datos en el IFAI.

cos. Ello ha traído consigo grandes ventajas en materia comunicaciones, como la transferencia de millones de datos a través de las herramientas que nos proporciona la nueva tecnología, el mejor ejemplo de ello es Internet.

La inmersión en este nuevo mundo ha puesto delante del hombre nuevos retos, entre otros, de qué forma canalizar en el cause de lo jurídico estos desarrollos, sin sobrepasar los límites de intervención del Estado en la actividad de los particulares, en donde aquel se constituya en el fiel de la balanza.

En el terreno de los derechos fundamentales, muchos han sido los efectos producidos por el avance tecnológico, entre otros en las esferas de la privacidad, la intimidad o más específicamente aún, en el terreno del derecho a la protección de los datos personales.[1]

Por lo anterior, desde hace décadas que se viene buscando la manera de dar una respuesta que satisfaga de la mejor forma posible al desafío que representa la evolución tecnológica en el terreno de la utilización y movilidad de la información de las personas.

Diversos modelos legislativos han sido aplicados, encontrando los primeros en Europa, en la que desde los años sesenta se ha trabajado de manera sistemática e institucional al respecto. Algunos años más tarde aparecen los primeros modelos normativos en América, quizá con menos fuerza y uniformidad, hablando en términos continentales.

El derecho a la protección de datos personales como hoy se encuentra perfilado en la doctrina más calificada es de reciente acuñación, encontrando su germen en el derecho a la intimidad personal y familiar, reconocido en diversos textos de carácter internacional en la época de la posguerra. Bajo esta atmósfera, la realidad europeo-americana se desenvuelve, a nivel internacional, en relación con los derechos humanos en las primeras décadas de la segunda mitad del siglo XX.

Por lo tanto, es precisamente en el ámbito de los derechos humanos donde inicia la zaga del derecho a la protección de datos personales, en-

[1] La expresión protección de datos hace alusión al amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte en su entorno personal, social o profesional. Véase Davara Rodríguez, Miguel Ángel, *Manual de protección de datos para abogados*, Navarra, Aranzadi, 2006, p. 177.

capsulado en otros derechos, el derecho a la privacidad o en el derecho a la intimidad, reconocidos expresamente en distintos instrumentos internacionales tanto del sistema universal como interamericano de derechos humanos.[2]

Conviene aquí hacer una distinción entre el derecho a la intimidad y el derecho a la protección de datos personales, ya que en ocasiones son términos utilizados de manera indistinta en la doctrina. Según señala Piñar Mañas, el derecho a la protección de datos de carácter personal:

> …presenta caracteres propios que le dotan de una naturaleza autónoma, de tal forma que su contenido esencial lo distingue de otros derechos fundamentales, específicamente, del derecho a la intimidad, en el que éste último, tiende a caracterizarse como el derecho a ser dejado solo y evitar injerencias en la vida privada mientras que el derecho a la protección de datos atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, partiendo del reconocimiento de que tales datos van a ser objeto de tratamiento por responsables públicos y privados.[3]

El concepto de privacidad a nivel internacional ha buscado evolucionar a la par del desarrollo de las tecnologías de la información, debido a que a través de las mismas es posible tratar datos personales, es decir recabar, utilizar, almacenar y transmitir, tanto en el sector público como en el privado, con una facilidad, hasta hace algunas décadas, inimaginable,

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

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

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

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

[3] Véase Piñar Mañas, José Luis, *La Red Iberoamericana de Protección de Datos (Declaraciones y Documentos)*, Valencia, Tirant lo Blanch, 2006, p. 32.

de manera tal que el tratamiento de datos personales sin una regulación adecuada puede llegar a constituir una seria amenaza a la privacidad.

Por lo anterior, la reacción en el terreno de los derechos humanos no se hizo esperar, y a partir de derechos preexistentes en el terreno de las libertades fundamentales, como el derecho a la intimidad, surge un nuevo derecho fundamental que posibilita la autodeterminación informativa de su titular.[4]

Resulta pertinente resaltar que el Tribunal Constitucional Español, en su sentencia 292/2000, del 30 de noviembre ha dado luz sobre los alcances del derecho fundamental a la protección de datos personales, estableciendo su carácter autónomo e independiente, cuyo contenido persigue garantizar un poder de control de los individuos respecto de sus datos personales, así como el uso y destino de los mismos, con el propósito de impedir su tráfico ilícito y lesivo.[5]

De la sentencia del alto tribunal se deduce que, a través de la regulación del artículo 18 numeral cuarto de la Constitución Española, el constituyente quiso garantizar un verdadero derecho fundamental a la protección de datos, cuya garantía deberá preservarse frente a cualquier invasión o intromisión ilegítima, merced a un sistema de protección específico e idóneo, marcando las diferencias existentes entre el "hábeas data y el derecho a la intimidad".

Como se puede ver, el impacto de la ciencia ha sido global,[6] influyendo prácticamente en todos y cada uno de los ámbitos de la convivencia humana, sin que hasta el momento sea posible afirmar que la fuerza con la que se ha intentado hacer frente a la situación hasta ahora generada por el avance tecnológico haya sido proporcional a la magnitud con la que la

4 El antecedente más importante de interpretación Constitucional se dio en Alemania con la sentencia del Tribunal Constitucional Federal Alemán sobre la Ley de Censos (1 BvR 209/83 ua), en el cual se reconoce la existencia de un nuevo derecho a la autodeterminación informativa, por el cual las personas pueden conocer quien, cuándo y cómo utiliza sus datos personales, además de reconocer que deben existir autoridades independientes que garanticen ese nuevo derecho.

5 Gómez Robledo, Alonso y Ornelas Núñez, Lina, *La protección de datos personales en México: El caso del Poder Ejecutivo Federal*, México, UNAM, 2006, pp. 15 y 16.

6 Ciertamente el desarrollo y creciente arraigo de las comunicaciones electrónicas en nuestra sociedad, en particular de Internet y su universo de servicios, ha supuesto un sinfín de nuevas necesidades o problemas en el contexto de la silenciosa revolución protagonizada por las nuevas tecnologías. Véase Ballesteros Moffa, Luis Ángel, *La privacidad electrónica*, Valencia, Tirant lo Blanch, 2005, p. 133.

misma se presenta, sin echar por tierra los loables esfuerzos hasta ahora llevados a cabo en la Unión Europea.

Considerando la importancia de los efectos producidos por el avance de la tecnología en relación con la privacidad de las personas, el presente artículo tiene como finalidad poner de manifiesto la importancia de conocer y contar con un derecho a la protección de datos personales y como se ha convertido en un asunto de interés internacional.

A efecto de lo anterior se describirán, en lo general, el concepto de derecho a la protección de datos y su recepción en México, para inmediatamente después enfocar el análisis en las transferencias internacionales de datos personales, abordando aspectos como definición y tipos de regímenes a que se sujetan las transferencias internacionales de datos, para de esta forma mostrar la importancia de contar con un instrumento que las regule, tanto en el terreno del comercio internacional, fundamentalmente dirigido al intercambio comercial desarrollado en el sector privado, como en el ámbito de la seguridad nacional, en cuanto a las transmisiones de datos que se producen entre Estados.

Conviene señalar que el estudio en relación con las transferencias internacionales de datos personales, dada la amplitud de la materia, se circunscribirá al comercio internacional en Internet, así como a la seguridad nacional.

II. Actualidad del derecho a la protección de datos en México

A manera de preámbulo, conviene apuntar que el primer instrumento legislativo, en el que se regula el derecho a la protección de datos de carácter personal es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LAI),[7] misma que, paradójicamente, tiene por finalidad proveer lo necesario para garantizar el acceso de toda persona a los documentos en posesión de las entidades públicas-gubernamentales en el ámbito federal.[8]

Como consecuencia de lo anterior, por lo que hace al ámbito de aplicación, la regulación establecida en la LAI se limita a los sistemas de datos personales del sector público-gubernamental a nivel federal.

[7] Publicada en el *Diario Oficial de la Federación* el 11 de julio de 2002.

[8] *http://www.ifai.org.mx*.

En cuanto a las disposiciones de carácter sustantivo como los principios, derechos y deberes en relación con el derecho a la protección de los datos de carácter personal en el capítulo IV, del título primero de la LAI se dispone lo siguiente:

> i. Se establecen los principios de calidad, finalidad y consentimiento (con un listado de excepciones al principio del consentimiento).
> ii. Se reconocen los derechos de los interesados al acceso, rectificación e información respecto a sus datos;.
> iii. Se señalan como deberes de los sujetos que traten datos personales el relativo a la adopción de las medidas necesarias que garanticen la seguridad de los datos personales, así como el de confidencialidad.
> iv. Se prevé la existencia de un registro ante el que se deben inscribir los "sistemas de datos personales".[9]

En relación con la autoridad la LAI prevé en su artículo 33 la existencia de una "autoridad independiente" denominada Instituto Federal de Acceso a la Información (IFAI),[10] al cual, por una parte, se le encomienda la función de garantizar el derecho de acceso a la información pública gubernamental y, por la otra, el derecho a la protección de datos de carácter personal.

Dicho lo anterior conviene preguntarse qué elementos de aquellos que componen la columna vertebral del derecho a la protección de datos no se encuentran presentes en el ordenamiento mexicano. En tal sentido, considerando los alcances del presente documento se han elegido tres instrumentos internacionales como referente para responder al cuestionamiento formulado, a saber la Directiva 95/46/CE del 24 de octubre de 1995 relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Di-

9 "Conjunto ordenado de datos personales" de acuerdo con la definición aportada por la propia LAI (artículo 3o., fracción XIII).

10 Es importante destacar que de acuerdo con la LAI, el IFAI es la autoridad competente a nivel administrativo para conocer de cuestiones relacionadas con acceso a la información y protección de datos, únicamente por lo que se refiere al Poder Ejecutivo Federal (artículo 33), ya que los poderes Legislativo y Judicial, así como los órganos constitucionales autónomos cuentan con instancias espejo (artículo 61) al IFAI que llevan a cabo esta función de garante.

rectiva 95/46), la recomendación de la Organización para la Cooperación y Desarrollo Económicos en la que se contienen las "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales", adoptada el 23 de septiembre de 1980 (Recomendaciones de la OCDE) y la Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas (Resolución 45/95 de la ONU), del 14 de diciembre de 1990.

Entre los elementos comunes[11] en la Directiva 95/46,[12] en las Recomendaciones de la OCDE y la Resolución 45/95 de la ONU, en términos generales, se advierte la ausencia de los siguientes en la norma mexicana:

> i. Aplicación de la norma en la materia a los sistemas de datos personales de carácter privado.
> ii. Existencia de un régimen aplicable a los flujos transfronterizos de datos.
> iii. Reconocimiento de categorías especiales de datos.
> iv. Delimitación expresa en ley de los supuestos de excepción a los principios aplicables en la materia.

De modo que resulta evidente la necesidad de contar con una ley comprehensiva en materia de protección de datos personales que abarque tanto al sector público como al privado, que además de contener los principios de protección internacionalmente aceptados y tutele los derechos de sus titulares a través de la creación de una autoridad independiente, prevea un régimen aplicable a los flujos transfronterizos de datos personales.

Lo anterior, incrementa su importancia en el caso mexicano dado que a diferencia de muchos de los países de la región cuenta con condiciones geopolíticas únicas y que le son propias, debido fundamentalmente a dos factores, el primero, su posición geográfica colindante con los Estados Unidos de América, el segundo, los acuerdos comerciales en los que se ha integrado como el Tratado de Libre Comercio de América del Norte (TLCAN) y el Tratado de Libre Comercio con la Unión Europea (TLCUE), así como la pertenencia a la Organización para la Cooperación y Desa-

11 Comunes al menos en dos de los instrumentos jurídicos de referencia.

12 Se toma como referencia, al ser la norma jurídica conforme a la cual se encuentra regulado el derecho a la protección de datos en la Unión Europea.

rrollo Económicos (OCDE) y al Acuerdo de Cooperación Asia Pacífico (APEC), entre otros instrumentos internacionales.

III. Concepto y tipos de transferencias internacionales de datos personales

En términos del criterio hasta ahora utilizado, para efectos del concepto y tipos de transferencias en razón de los sujetos, se hará alusión a los instrumentos internacionales citados en el apartado anterior, así como a algunas disposiciones de carácter nacional que de los mismos han derivado.

Las Recomendaciones de la OCDE, establecen que por "circulación transfronteriza de datos personales" se entenderá los movimientos de datos personales a través de fronteras nacionales.[13]

Tanto en el caso de la Directiva 96/46, como en el de la Resolución 45/95 de la ONU, no se establece propiamente una definición de lo que para efectos de dichos instrumentos debe entenderse por transmisión internacional de datos personales.

No obstante lo anterior, y derivado de la transposición de la Directiva 95/46, en el Reino de España, fue expedida por la Agencia Española de Protección de Datos la Instrucción 1/2000,[14] del 1o. de diciembre, relativa a las normas por las que se rigen los movimientos internacionales de datos, la cual define las transferencias internacionales de datos como toda transmisión de los mismos fuera del territorio español, en particular, las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero.[15]

Las implicaciones de la definición propuesta en la Instrucción 1/2000, antes citada, nos lleva a hacer referencia a los tipos de transferencia que existen en razón de la calificación de los sujetos involucrados en la misma.

13 Numeral 1, inciso *a*.

14 La Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal, si bien al igual que sucede en el caso de la Directiva 96/46, establece un articulado dedicado a los movimientos transfronterizos de datos personales, tampoco establece qué debe entenderse por los mismos.

15 *https://www.agpd.es/index.php?idSeccion=77*.

De acuerdo con lo expuesto, en el ordenamiento español es posible distinguir dos modalidades de transferencias internacionales en función de la calificación del sujeto receptor de los datos.

La primera modalidad se encuentra recogida en el artículo 11 de la Ley Orgánica 15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), según la cual el sujeto transmitente puede provocar una cesión o transmisión de datos a un tercero localizado en el extranjero, operación que supone que el tercero[16] que actúa por cuenta propia decidiendo sobre la finalidad, uso y contenido del tratamiento.

La segunda modalidad está directamente relacionada con la hipótesis prevista en el artículo 12 de la LOPD, ya que en ésta el sujeto que comunica los datos, lleva a cabo la transmisión de los mismos, a otro sujeto ubicado en el extranjero, para que se realice un determinado tratamiento a su nombre y por su cuenta.

En ese orden de ideas, si bien es cierto las transferencias "relevantes" para efectos del ordenamiento español son aquéllas que suponen una transmisión de un responsable a otro responsable, también califican como transferencias internacionales las que implican una transmisión de un responsable a un encargado.[17]

Aunado a lo anterior y debido a la gran relevancia que tienen en la actualidad las trasmisiones con fines comerciales, así como las gubernamentales por razones de seguridad nacional, se hará una mención especial a éstas en los apartados subsecuentes.

1. *Transferencias internacionales de datos personales con fines comerciales*

México tiene celebrados diversos acuerdos en materia de comercio internacional en diversos puntos del orbe, al amparo de los cuales el incremento de los flujos internacionales de datos promovidos en un contexto de internacionalización económica y de desarrollo tecnológico es cada día más grande.

16 Este tercero tiene la consideración de responsable del tratamiento.

17 Véase Sancho Villa, Diana, *Transferencia internacional de datos*, Madrid, Agencia Española de Protección de Datos, 2003, pp. 25-27.

Tal situación ha llevado en otras latitudes a la confrontación entre los intereses económicos de liberalización del tráfico de datos y la necesidad de proteger el derecho de las personas a disponer libremente de sus datos personales.

En el caso mexicano, derivado del intenso intercambio con sus socios comerciales (Estados Unidos de América y Canadá), se llevan a cabo constantes transferencias internacionales de datos personales, sin que hasta el momento exista una regulación mínima en la que se observen los principios internacionalmente reconocidos en la materia.

Lo anterior principalmente en la relación con los Estados Unidos de América, ya que el caso canadiense es distinto, toda vez que dicho país cuenta con leyes tanto a nivel federal como provincial en materia de protección de datos, así como con el reconocimiento de la Unión Europea de país con nivel adecuado de protección.[18]

Por lo que hace al Acuerdo de asociación económica, concertación política y cooperación entre la Comunidad Europea y sus Estados miembros, por una parte, y los Estados Unidos Mexicanos, por la otra, también denominado Tratado de Libre Comercio con la Unión Europea (TLCUE), el artículo 41 contempla la cooperación en materia de protección de los datos de carácter personal con vistas a mejorar su nivel de protección y prevenir los obstáculos a los intercambios que requieran transferencia de datos de carácter personal, y en su artículo 51 se señala que las partes se obligan a garantizar un grado elevado de protección respecto al tratamiento de los mismos.

Las disposiciones de referencia implican para el Estado mexicano un compromiso en dos vertientes, el primero implica el establecimiento de mecanismos que en este momento garanticen la protección de los datos personales provenientes de alguno de los países integrantes de la Unión Europea, y el segundo plantea la necesidad de resolver la cuestión mediante una solución de más largo alcance, en todos los sentidos, como lo sería el diseño de un marco normativo que sustente jurídicamente y con

[18] Para mayor referencia véase la Decisión de la Comisión del 20 de diciembre de 2001 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act*, consultable en *https://www.agpd.es/inex.php?id Seccion=256*.

amplio espectro el actuar de los sujetos involucrados en el intercambio de datos desde y hacia nuestro país.

Frente a esta realidad, en una búsqueda de una solución inmediata debemos resaltar, en términos muy generales, la importancia de los mecanismos explorados en el seno del *Asia-Pacific Economic Cooperation* (APEC),[19] ante la carencia de marcos normativos nacionales, como lo es el "Marco de Privacidad de APEC" que fue desarrollado sobre la base de las Recomendaciones de la OCDE.

La autorregulación en las transferencias internacionales de datos en México

Es innegable que la autorregulación constituye una herramienta atractiva para los sectores comerciales o de servicios, entre otras cuestiones, porque se ajusta a sus necesidades siempre cambiantes, por tanto, hace flexible su modificación en caso necesario, sin tener que pasar por el complejo aparato legislativo.

La autorregulación ha surgido como la reglamentación derivada de la autonomía privada de los empresarios que tratan datos o de las organizaciones en que se agrupan para adoptar códigos de conducta o códigos tipo, ajustados a las peculiaridades del sector que representan.

La autorregulación es un mecanismo que ha sido fomentado desde la OCDE y también desde la normatividad de la Unión Europea a través de la Directiva 95/46, la Directiva 2002/58/CE sobre tratamiento de datos personales y protección de la intimidad en las comunicaciones electrónicas, así como la Directiva 2000/31/CE sobre el comercio electrónico.

Según quedó apuntado en el apartado anterior, México no cuenta actualmente con un marco normativo nacional en materia de flujos trans-

[19] México tuvo un papel muy activo en el pasado foro denominado "APEC Australia 2007 meeting", en específico en el Seminario denominado "First Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, 2007: Creating Trust in developing Cross-Border Privacy Rules: Making Compliance Possible and Enforcement Credible when Personal Information Moves between Economies", cuyo centro de intercambio de experiencias y discusión fue el tema de la transferencia internacional de datos personales. También se participó en la Reunión del subgrupo de Privacidad de *APEC (Asia-Pacific Economic Cooperation)*.

fronterizos de datos de carácter personal, lo que no significa que la materia resulte del todo ajena en el país.

La Secretaría de Economía y la Procuraduría Federal del Consumidor, por una parte, y por la otra, la Asociación Mexicana de Internet (AMIPCI) suscribieron, en noviembre de 2006, un convenio de colaboración con el objeto de establecer los mecanismos de cooperación para dotar a la industria de un medio que brinde elementos de confianza al consumidor respecto al cumplimiento de obligaciones contraídas por los proveedores de bienes y servicios a través de Internet, relativos entre otros, a la existencia física del proveedor y a la protección de los datos personales del consumidor mediante la implementación y uso de sellos de confianza.

En el mencionado Convenio se reflejan los principios de APEC,[20] y su suscripción derivará en convenios específicos entre la AMIPCI y empresas privadas, a efecto de que la primera revise la adecuada protección de datos personales y otorgue, en su caso, sellos de confianza a las mencionadas empresas. La figura de los sellos de confianza (*trustmark*) se ha establecido en otros países para diversos fines y con resultados exitosos.

En ese sentido, la existencia de los sellos de confianza y en general, el acreditar que se cumple con los estándares establecidos en un instrumento nacido en el terreno de la autorregulación, puede reportar grandes beneficios en el ámbito comercial, como lo es la obtención de una cartera de clientes fiel a la empresa, debido a la certidumbre generada por ésta,

20 México intervino en los *Breakout Groups* que se formaron a efecto de analizar las diversas alternativas que existen para establecer *Cross Border Privacy Rules* (CBPR) que permitan la implementación del APEC *Privacy Framework* de manera uniforme, a efecto de que la protección que otorga una empresa a los datos personales de sus clientes, sea reconocida en la transferencia internacional de dichos datos, por los demás países pertenecientes a APEC.

Asimismo, participó en el Subgrupo de Privacidad de APEC, el cual depende del *Electronic Commerce Steering Group* (ECSG), el cual presidió (a través de la Secretaría de Economía), abordándose diversas cuestiones relativas a proyectos existentes en materia de protección de datos personales dentro de las economías de APEC.

Dentro de las funciones específicas del ECSG (establecido en febrero de 1999) está el desarrollo de legislaciones y políticas compatibles entre las economías en el campo de la privacidad, para lo cual ha desarrollado los lineamientos generales en la materia con el fin de que los mismos sean contemplados y establecidos en los cuerpos legales correspondientes y con esto lograr un flujo de datos seguro y sin obstáculos. En este caso es importante resaltar, como se parte de un mecanismo de autorregulación destinado a provocar una respuesta legislativa contundente.

en relación con el tratamiento de sus datos personales y su consecuente impacto económico, reflejado en las ganancias de la empresa.

En cuanto a las cuestiones que podrían mejorarse en el esquema de sellos de confianza está el que en su configuración e implementación se debería fomentar, entre otros elementos, la utilización de medios avanzados de cifrado para reforzar las garantías de confidencialidad de la información que circula por las redes abiertas de telecomunicaciones y en particular por Internet, y a través de la firma digital, la integridad de los mensajes y transacciones, sobre todo, porque no debemos olvidar que el acopio de datos permite obtener una evaluación de la personalidad de los individuos.

Es muy temprano todavía para determinar la eficacia de estos mecanismos en la efectiva protección de datos personales, ya que debemos reconocer que pueden tener deficiencias importantes como las señaladas anteriormente, a las que se puede agregar la carencia de verificación de la existencia de medidas de seguridad.

Sin embargo, y a pesar de lo anterior, deben alentarse modelos como el mexicano, que puede resultar ejemplar para el resto de los países de APEC, ya que la propia AMIPCI empieza a contar entre los poseedores de sellos de confianza con entidades gubernamentales, las cuales, voluntariamente aceptan que además de las reglas para llegar a ser miembros, se constriñan a la necesidad de cumplir con los Lineamientos de Protección de Datos Personales emitidos por el IFAI. Lo anterior con independencia de las facultades de dicha instancia como autoridad en materia de protección de datos dentro de la administración pública federal.

De modo que la ausencia de un marco normativo no impide la combinación entre el sector privado y el público para lograr objetivos conjuntos. De hecho, el alentar este tipo de esfuerzos puede llevar a que se logren mejores prácticas y soluciones de impacto inmediato que a través de las leyes resulta difícil alcanzar.

2. *Transferencias internacionales de datos personales entre gobiernos por motivos de seguridad nacional*

Los gobiernos, en el ámbito de la cooperación internacional con otros países en materia de lucha contra el terrorismo y las formas graves de delincuencia organizada, poseen sistemas de datos personales que permiten

detectar a aquellos individuos que constituyen o pueden constituir un riesgo o amenaza potencial a la seguridad de uno o varios Estados.

Consecuencia de lo anterior, los gobiernos han venido intercambiando datos de las personas con los fines antes señalados, sin embargo, luego de los atentados terroristas del 11 de septiembre 2001 en los Estados Unidos de América, así como los subsecuentes de Madrid y Londres en 2004 y 2005, respectivamente, se ha acentuado el valor de estas bases de datos, en el sentido de mantenerlas actualizadas, de ampliar los tipos de datos recabados (que pueden incluir las intervenciones telefónicas por ejemplo), así como los perfiles que de las personas pueden obtenerse y, finalmente, se ha propiciado un intercambio más profuso e intenso de manera transnacional.

En materia de privacidad, la circulación transfronteriza de la información personal, plantea desafíos únicos relacionados con la protección de las personas en el ámbito de su información privada. Por lo anterior, las autoridades de protección de datos personales a nivel internacional, han llamado la atención en repetidas ocasiones a los gobiernos, con el fin de encontrar un equilibrio entre la seguridad de los países y los límites en la comunicación de la información privada de sus ciudadanos. Para lograr este objetivo, los gobiernos, no pueden desconocer los alcances de los mandatos que tienen conferidos por ley. El reto en ese tenor, es lograr programas de información de inteligencia y análisis de riesgos que respeten en la mayor medida de lo posible las libertades y las garantías fundamentales de los gobernados.

Diversas son las medidas que los gobiernos han establecido para hacer frente al terrorismo en el plano doméstico como en el internacional, consecuencia de las cuales el Estado se ha visto en la necesidad de "irrumpir" en ámbitos de la esfera jurídica del ciudadano que pueden llegar a provocar una colisión de derechos.

Por una parte, se tiene la obligación del Estado de evitar la realización de actos lesivos de la seguridad nacional, y por la otra, el derecho de los ciudadanos a conservar un espacio propio dentro del cual desarrollarse libremente y sin injerencia alguna, incluido el propio Estado.

Los alcances de las disposiciones en materia de protección de datos personales en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental son limitados ya que el legislador en México, no estableció un régimen especial para regular sistemas de datos personales

para la investigación del terrorismo y de formas graves de delincuencia organizada.

Con el fin de poner de relieve la importancia que en los últimos años ha cobrado el tema de la transferencia de datos personales entre gobiernos, con motivos de seguridad nacional, se expondrá de manera muy breve la problemática surgida a partir de los requerimientos efectuados por el gobierno norteamericano a las compañías aéreas o marítimas que operan en su territorio.

La transferencia de datos a raíz de la Patriot Act y la respuesta de la Unión Europea

Entre otras muchas cuestiones, los lamentables sucesos del 11 de septiembre vinieron a demostrar que el terrorismo es un problema no sólo internacional, sino mundial (cuestión que desafortunadamente se ha venido corroborando con posteriores ataques en ciudades europeas, así como en oriente medio y el sureste asiático).

Considerando los niveles que ha alcanzado el problema del terrorismo, no hay lugar a dudas de la necesidad que a nivel mundial existe de hacerle frente, la pregunta es ¿cómo hacerlo? Está claro que al interior cada país decidirá "soberanamente" cuál es la mejor estrategia para encararlo, dentro de los límites de su orden jurídico nacional. El problema se presenta respecto de las decisiones que se adopten con efectos que trasciendan al ámbito internacional.

Como es de conocimiento público, con motivo de los ataques terroristas del 11 de septiembre de 2001, los Estados Unidos de América adoptaron diversas medidas para hacerle frente a tal problema. Entre las mismas, el gobierno norteamericano expidió la *Patriot Act* (Ley Patriota) en octubre de 2001, cuya finalidad, en términos generales, es salvaguardar la seguridad nacional en los Estados Unidos de América (en adelante EUA).

En este sentido y a raíz de la *Patriot Act*, EUA emitió disposiciones[21] que establecen la obligación de que las compañías aéreas o marítimas que operen en su territorio le faciliten los datos relativos a los pasajeros y

[21] La *Aviation and Transportation Security Act* (noviembre de 2001) y la *Enhanced Border Security and Visa Entry Reform Act* (mayo de 2002).

la tripulación. Estas transferencias se realizarán en un medio electrónico y deben ser completadas antes del despegue del avión.

Dicho medio electrónico es el Sistema de Información Avanzada sobre Pasajeros (APIS) y se compone de una lista de datos respecto de cada persona física que viaja de y a Estados Unidos. En un principio, los datos requeridos estaban intrínsecamente relacionados con el vuelo tomado, el visado o el permiso de residencia para los Estados Unidos, así como con información identificativa como la que figura en los pasaportes. Sin embargo, ahora no sólo se requieren esos datos sino otros más. En general, los datos que se transfieren son los siguientes: nombre, fecha de nacimiento, nacionalidad, sexo, número de pasaporte y lugar de expedición, país de residencia, número de visado en los EUA, lugar y fecha de expedición (si corresponde), número de registro extranjero (si corresponde), domicilio en los EUA durante la estancia, así como cualquier otro dato que se considere necesario para identificar a los viajeros, fecha de la reservación, la agencia de viajes cuando corresponda, la información que se muestra en el boleto, los datos financieros (número de tarjeta de crédito, fecha de caducidad, dirección del lugar de expedición, etcétera), el itinerario, información sobre el transportista que opera el vuelo (número de vuelo, etcétera), número de asiento y datos anteriores del PNR (*Passenger Name Records*). En estos últimos pueden constar no sólo los viajes completados en el pasado, sino también información de carácter religioso o étnico (elección de la comida, etcétera), afiliación a un determinado grupo, datos relativos al lugar de residencia o los medios para contactar con una persona (dirección de correo electrónico, información sobre un amigo, lugar de trabajo, etcétera), datos médicos (cualquier asistencia médica que se haya requerido, oxígeno, problemas relacionados con la vista, el oído o la movilidad, o cualquier otro problema que deba hacerse saber para garantizar un vuelo satisfactorio) y otros datos relacionados, por ejemplo, con los programas de viajeros frecuentes (*Frequent Fliers number*).[22]

Asimismo, dichos datos pueden ser transmitidos a otras autoridades federales, estatales y locales, así como a agencias extranjeras encargadas de la investigación y persecución de actos violatorios de leyes civiles y

[22] Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, aprobado el 24 de octubre de 2002 por el Grupo de Trabajo sobre Protección de Datos del Artículo 29 de la Directiva 95/46/CE. *http://ec.europa.eu/justice home/fsj/privacy/docs/wpdocs/2002/wp66 es.pdf*.

penales, en caso de que se advierta la posibilidad de una potencial violación de dichas leyes.[23]

Teniendo en cuenta el impacto que la normatividad emitida por los EUA produciría en el ámbito comunitario, se dio inicio a una serie de negociaciones entre autoridades europeas y norteamericanas, adoptándose con fecha 14 de mayo de 2004, por parte de la Comisión Europea, la Decisión sobre el carácter adecuado de la protección, en la que se determinó que la Oficina de Aduanas y Protección de Fronteras de los EUA garantizaba un nivel de protección adecuado de los datos transferidos desde la Comunidad. Por su parte, con fecha 17 de mayo de 2004, el Consejo adoptó la Decisión por la que aprobó la celebración de un Acuerdo entre la Comunidad Europea y los EUA sobre el tratamiento y la transferencia de los datos de los pasajeros y la tripulación por parte de las compañías aéreas establecidas en el territorio de los Estados miembros de la Comunidad a la Oficina de Aduanas y Protección de Fronteras de EUA.[24]

Derivado de lo anterior, el Parlamento Europeo requirió al Tribunal de Justicia de las Comunidades Europeas que anulase la Decisión del Consejo (asunto C-317/04) y la Decisión sobre el carácter adecuado de la protección (asunto C-318/04), alegando fundamentalmente que esta última Decisión se adoptó *ultra vires*, que el artículo 95 de la CE no constituye una base jurídica procedente para la Decisión por la que se aprueba la celebración del Acuerdo y que en ambos casos existe una violación de los derechos fundamentales.[25]

El Tribunal de Justicia resolvió anular las decisiones de referencia sobre la base de la Directiva 95/46/CE en el sentido de que el artículo 3o., apartado 2 de la Directiva excluye de su ámbito de aplicación el tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del derecho comunitario y, en cualquier caso, el tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal.

23 *Privacy Impact Assessment, Advance Passenger Information System (APIS)*, Department of Homeland Security, 21 de marzo de 2005, *http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbpapis.pdf*.

24 Boletín de prensa del Tribunal de Justicia de las Comunidades Europeas consultable en el sitio de Internet: *http://curia.europa.eu/es/actu/communiques/cp06/aff/cp060046es.pdf*.

25 *Idem*.

El Tribunal advirtió que, de la decisión sobre el carácter adecuado de la protección, se desprende que la exigencia de que se transfieran los datos se basa en la normativa estadounidense relativa a la intensificación de la seguridad. En consecuencia, la transferencia de los datos de los pasajeros y tripulación a la Oficina de Aduanas y Protección de Fronteras de los EUA constituye un tratamiento que tiene por objeto la seguridad pública y las actividades del Estado en materia penal.

En resumen, lo anterior significa que en virtud de la arquitectura competencial trazada en la Unión Europea (UE), los acuerdos celebrados entre ésta y los EUA son declarados nulos por haberse celebrado por autoridades incompetentes en la materia.

Más allá de la nulidad declarada por el Tribunal de Justicia de las Comunidades Europeas para este caso en particular, en razón de la competencia y atribuciones de las autoridades correspondientes, conviene analizar la razón por la cual se celebraron los acuerdos entre la UE y los EUA, que derivaron en las decisiones anuladas.

En el ámbito de la protección de datos personales, de competencia comunitaria, por lo que se refiere a transferencias internacionales de datos a países terceros, el principio que rige es que los Estados miembros de la UE sólo pueden autorizar transferencias a aquéllos que aseguren un nivel de protección adecuado.

De acuerdo con el artículo 25 de la Directiva 95/46/CE, el carácter adecuado del nivel de protección que ofrece un país tercero se evalúa atendiendo a todas las circunstancias que concurran en una transferencia en particular, de conformidad con la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

En tal sentido, la Comisión Europea puede hacer constar que un país tercero garantiza un nivel de protección adecuado, a la vista de su legislación interna o de sus compromisos internacionales suscritos.[26]

El punto de partida para llevar a cabo transferencias internacionales de datos a países terceros es la observancia de los siguientes principios generales:[27]

[26] Para mayor referencia véase el artículo 25 de la Directiva 95/46.

[27] *Idem*.

a) Limitación de objetivos. Los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia.
b) Proporcionalidad y calidad de los datos. Los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.
c) Transparencia: debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.23 y 13 de la Directiva.
d) Seguridad: el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.
e) Derechos de acceso, rectificación y oposición: el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.
f) Restricciones respecto a transferencias sucesivas a otros terceros países: únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice, asimismo, un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la Directiva.
g) En términos de lo descrito, el hecho de que los EUA no se encontrara entre los países considerados por la UE, como uno de aquéllos que cuenta con un nivel adecuado de protección de datos, según los elementos señalados, y ante la anulación de las decisiones anteriormente señaladas, se hizo necesaria la celebración de una serie de negociaciones tendentes a remediar tal situación entre ese país y la UE.

Finalmente, el 6 de octubre de 2006 se adoptó un nuevo acuerdo de carácter provisional entre los EUA y la UE, con fundamento en el cual podría continuarse con la transmisión de los datos de referencia, entre los EUA y la UE, bajo ciertos parámetros, vigente hasta el 31 de julio de 2007, salvo que se acuerde una extensión del mismo.[28]

Con el caso expuesto, queda claro que para la UE el que las transferencias internacionales de datos personales, incluso para aquellos transmitidos para la investigación del terrorismo, se llevan a cabo bajo un control mínimo de la autoridad competente representa uno de los temas de mayor relevancia dentro de su agenda internacional.

3. *México y las transferencias internacionales*

De acuerdo con lo indicado en el apartado anterior, es posible afirmar, al menos hasta el día de hoy, que existe una duda fundada de que los EUA cuenten con un marco normativo respetuoso del derecho fundamental a la protección de datos, entendido éste como el poder de disposición y de control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, sea el Estado o un particular, y que también permite al individuo saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.[29]

En el caso mexicano, el asunto de la transmisión de datos de los mexicanos a un gobierno extranjero se presenta de manera diversa a la realidad europea, debido, por una parte, a la ausencia de una disposición de carácter constitucional que reconozca expresamente el derecho a la protección de datos personales. [30]

[28] Documento consultable en el sitio de Internet *http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/er/91183.pdf*.

[29] Sentencia 292/2000 del Tribunal Constitucional de España, consultable en el sitio de Internet *https://www.agpd.es/upload/Canal_Documentacion/Sentencias/Sentencia292.pdf*.

[30] A pesar de que se han presentado diversas iniciativas de ley para regular la protección de los datos personales, es importante destacar que éstas no han sido aprobadas, entre otras razones de índole técnico-jurídico, porque no existe un fundamento expreso en la Constitución para que el Congreso legisle en la materia, de modo que será muy importante el impulso que se dé en lo particular, a dos iniciativas de Reforma Constitucional que podrán dar cauce al ejercicio de este derecho. La primera de las iniciativas de referencia fue presentada el 5 de abril de 2006, por parte del senador Antonio García Torres del grupo parlamentario del Partido Revolucionario Institucional, ante la Cámara de Se-

Como se apuntó en apartados anteriores, únicamente se cuenta con una regulación básica a nivel federal en torno al derecho a la protección de datos en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y desarrollos administrativos posteriores (Lineamientos de Protección de Datos Personales), que permiten proteger aquellos datos de carácter personal objeto de tratamiento por parte de los entes gubernamentales, así como las leyes estatales, tal como la de Colima, que cumplen con funciones similares dentro de su ámbito competencial.

Es evidente que no resulta suficiente el esquema regulatorio en materia de protección de datos personales con que se cuenta actualmente, por

nadores. Dicha iniciativa fue formulada como una adición al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos —en adelante la Constitución Federal— para reconocer al derecho a la protección de datos personales, como un derecho fundamental, en los siguientes términos

"PROYECTO DE DECRETO POR EL CUAL SE ADICIONAN DOS PÁRRAFOS AL ARTÍCULO 16 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.

ARTÍCULO ÚNICO. Se adicionan tres párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que se insertan luego del primer párrafo y se recorren los subsecuentes, para quedar en los siguientes términos:

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos y, en su caso, obtener su rectificación, cancelación o destrucción en los términos que fijen las leyes.

La ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden público, seguridad, salud o para proteger los derechos de tercero.

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado cuando menos con pena privativa de libertad y existan datos que acrediten el cuerpo del delito y que hagan probable la responsabilidad del indiciado".

Un aspecto de la mayor relevancia en cuanto a este proyecto es que el mismo fue aprobado en la anterior legislatura, con 77 votos a favor y 5 abstenciones, en la Cámara de Senadores y fue enviado a la Cámara de Diputados para los efectos constitucionales correspondientes, estando aún pendiente su discusión y aprobación en ésta última.

La segunda iniciativa de reforma constitucional se presentó el pasado 27 de marzo de 2007 de abril, por el diputado Gustavo Parra del Partido Acción Nacional, que vendría a reforzar la señalada anteriormente, ya que dota al Congreso de facultades expresas para expedir la ley de la materia, esgrimiendo que es relevante no sólo por tratarse de un tema de protección de derechos humanos y libertades fundamentales, sino por los efectos esenciales que estos tienen sobre la economía nacional.

el simple hecho de que hay sectores que carecen de una normatividad mínima que reconozca dicho derecho, esto es, se ha avanzado por el camino correcto, al haberse expedido ya una normatividad "sectorial" a través de la cual los particulares pueden exigir la tutela de ciertas prerrogativas, es necesario irradiarlo a toda la sociedad mexicana, en la que con independencia de las particularidades que deba observar este derecho en sus distintos campos de aplicación (gubernamental, mercantil, en Internet) debe existir un umbral mínimo de principios aplicables a todos los gobernados.

Ahora bien, en relación con los datos de pasajeros y tripulación que se transfieren a los EUA mediante el APIS, es de señalar que, si bien las transmisiones que se han mencionado son hechas directamente por aerolíneas privadas, lo cierto es que el gobierno mexicano requiere verificar que dichas transmisiones sean acordes con una política respetuosa de los derechos fundamentales.

En específico, no se advierte que se esté cumpliendo con el principio de información ni con el principio de finalidad. Es decir, no se ha demostrado la necesidad de realizar dicha transferencia y no parece aceptable que una decisión unilateral, tomada por un tercer país por motivos que obedecen a sus propios intereses públicos, lleve a efectuar de manera periódica y sistemática las transferencias de datos antes señalados.

Cabe señalar, a manera de referencia, que en leyes como LOPD, si bien exceptúa de su ámbito de aplicación a los datos personales relacionados con los sistemas de datos personales establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada, prevé para los responsables de este tipo de sistemas, la obligación de comunicar de manera previa a la Agencia Española de Protección de Datos lo siguiente:

1. La existencia del sistema.
2. Las características generales del sistema.
3. La finalidad para la que será utilizado el sistema.

Se considera por tanto que, si bien como se ha dicho, las transmisiones son hechas por aerolíneas privadas, sean los gobiernos quienes determinen, a través de normatividad que emitan ambos, los datos que deben transmitirse y la protección adecuada a los mismos.

Ahora bien, cabe señalar que en el ámbito continental, existe la Alianza para la Seguridad y la Prosperidad de América del Norte, la cual es un

proceso trilateral, permanente, para una mayor integración de América del Norte, a través de la cual México, Estados Unidos y Canadá comparten una agenda en materia de prosperidad y seguridad.

De los dos Informes que se han presentado a los Mandatarios, en junio de 2005 y agosto de 2006, se desprende claramente que se han iniciado acciones para el intercambio de información de diversa índole entre los tres países. Dentro de los puntos a destacar, contenidos en la Agenda de Seguridad cuyo desarrollo se encuentra ya en proceso se encuentran los siguientes:

> Trabajaremos para desarrollar sistemas que impidan que los viajeros de alto riesgo ingresen a América del Norte, que a la vez faciliten el tránsito legal de personas hacia y dentro de la región, a través de mejoras a nuestra capacidad para verificar la identidad de los mismos… probaremos tecnología y realizaremos recomendaciones para mejorar el uso de la biométrica en la inspección de viajeros con destino a América del Norte, con miras a desarrollar sistemas biométricos fronterizos y de migración compatibles. Desarrollaremos estándares seguros para documentos de status migratorio y de nacionalidad con un menor costo, que faciliten el cruce transfronterizo, con el fin de obtener una producción óptima antes del 1o. de enero de 2008. Dentro de los próximos 36 meses, diseñaremos un *sistema de registro único e integral de los programas de viajeros confiables en América del Norte.*
>
> …
>
> Dentro de un período de 36 meses, diseñar un programa único e integrado de inscripción global para viajeros de confianza de América del Norte (por ejemplo NEXUS, FAST, SENTRI) para el viaje por aire, tierra y mar.
>
> …
>
> Mejorar la cooperación de *intercambio de información y aplicación de la ley entre investigadores y fiscales*, para dirigirse a actividades ilegales entre puertos de entrada y crimen organizado transfronterizo, contrabando de bienes, crímenes económicos, y el trafico de alcohol, armas de fuego, drogas ilegales y explosivos.
>
> …
>
> Mejorar nuestras capacidades para combatir el terrorismo a través del *intercambio apropiado de listas de terroristas* (*terrorist wathclists*) y el establecimiento de vínculos entre las autoridades de Canadá, Estados Unidos y México.
>
> …

> A fin de fortalecer la integridad y seguridad de los sistemas de determinación de asilo y refugiados, Estados Unidos y Canadá lanzaron un proyecto piloto para compartir información de solicitantes de refugio y de asilo con base en la comparación de registros de huellas digitales.[31]

A partir de lo anterior, se advierte que México está coadyuvando en el ámbito de América del Norte de diversas formas en términos de lo antes apuntado, intercambiando, entre otros datos información relativa a la comisión de delitos.

Se considera que dicho intercambio es importante para lograr los diversos objetivos de seguridad y prosperidad de los Estados. No obstante, es de vital importancia que dicho intercambio cuente con la base jurídica adecuada, y que los datos que se transfieran cumplan de manera estricta con los principios de protección de datos personales internacionalmente reconocidos, incluyendo específicamente el principio de finalidad y las medidas de seguridad adecuadas en la transmisión.[32]

IV. Conclusiones

El derecho a la protección de datos puede definirse como el poder de disposición y de control que faculta a su titular a decidir cuáles de sus datos

31 Primer Reporte a Mandatarios, *http://web2.senasica.sagarpa.gob.mx/xportal/sen/qesen/Doc1914/SPP062705Report.pdf*.

32 Cabe mencionar que con fecha 28 de mayo de 2007 se publicó el "Acuerdo del Consejo de Seguridad Nacional por el que se establece un Comité Especializado de Alto Nivel para coordinar las acciones del Poder Ejecutivo Federal" a efecto de dar cumplimiento a las obligaciones internacionales del Estado mexicano en el ámbito nacional en materia de desarme, terrorismo y/o seguridad internacionales, por el cual se crea el Comité Especializado de Alto Nivel en materia de Desarme, Terrorismo y Seguridad Internacionales, integrado por representantes de las secretarías de Relaciones Exteriores; Defensa Nacional; Marina; Seguridad Pública; Hacienda y Crédito Público; Comunicaciones y Transportes; de la Procuraduría General de la República; así como del Centro de Investigación y Seguridad Nacional, el cual ostentará la Secretaría General del Comité. Entre las facultades a destacar del citado Comité se encuentran las siguientes:

Establecer las reglas para el intercambio de informes, datos o cooperación técnica entre las dependencias, relacionados con las obligaciones del Estado mexicano frente a la comunidad internacional en materia de desarme, terrorismo y/o seguridad internacionales;

Solicitar, a través de su Secretaría General, la información exigida por los organismos y mecanismos establecidos por virtud de los tratados e instrumentos internacionales, a las personas físicas o jurídicas afectadas por los mismos.

proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso.

En el actual contexto de internacionalización económica y desarrollo tecnológico, la existencia de un régimen que regule el flujo transfronterizo de datos constituye un elemento a través del cual es posible garantizar la libre circulación de datos personales, así como el respecto a derechos fundamentales.

En ese sentido, al establecerse un régimen que regule las transferencias internacionales de datos el legislador debe tener en todo momento en cuenta los intereses en presencia, de manera tal que, por una parte, los controles que el Estado establezca no se traduzcan en obstáculos o barreras que entorpezcan injustificadamente la actividad comercial, y por la otra, que la política a seguir al respecto no resulte tan laxa que el derecho a la protección de datos quede vaciado de contenido, una vez que los datos hayan salido del territorio nacional.

De esta forma, el primer paso que el gobierno mexicano debe dar en aras de alcanzar la meta apuntada es el promover una reforma constitucional que reconozca el derecho fundamental a la protección de datos personales, para que a partir de ella, en un esfuerzo conjunto entre gobierno y sociedad, se continúe con el proceso para la emisión de una ley de protección de datos personales, que permita el ejercicio efectivo de este derecho en todos los ámbitos en los que son recabados dichos datos.

Considerando que las reformas constitucional y legislativa constituyen objetivos que, en el mejor de los escenarios se alcanzarían en el mediano plazo, se hace necesario que el gobierno federal adopte medidas de manera inmediata tendentes a mejorar la situación que actualmente subsiste en ámbitos como el de la seguridad nacional. Dichas medidas se pueden traducir en la celebración de convenios internacionales, en los que el Estado mexicano, empiece a preparar el camino sobre el que se transitará en los próximos años.

El contar con una regulación equilibrada en materia de protección de datos, y en consecuencia tratándose de transferencias internacionales, puede llegar a erigirse en un factor que fortalezca la integración económica en bloques comerciales de los que México ya es parte.

Es importante hacer notar que la existencia de una normatividad en materia de protección de datos, en la que se encuentren debidamente ponderados los intereses en presencia, no constituye un freno a la activi-

dad económica sino más bien representa una herramienta eficaz para potenciar las transacciones económicas, así como para proteger los derechos de las personas vinculadas a dichas transacciones, por lo que a esta materia se refiere.

En cuanto al intercambio que entre Estados se llegue a generar en el ámbito de la seguridad nacional, la normativa relativa a la protección de datos tampoco representa un límite para los gobiernos en el intercambio institucional que se deba llevar a cabo, ni para lograr acciones eficaces en contra de la delincuencia organizada, ya que sólo se observarán aquellos principios de protección esenciales para que el flujo que de los datos se produzca.

De modo que es imprescindible que los gobiernos adopten medidas eficaces en la lucha contra el terrorismo y que de igual forma, al aplicarlas se respeten los derechos fundamentales, ya que de lo contrario, como han afirmado las autoridades de protección de datos personales en el ámbito internacional, se estaría produciendo ya la primera y capital victoria de los terroristas: restringir el marco de las libertades y derechos que, afortunadamente caracterizan a las democracias en el mundo. Por lo anterior, es indispensable contar con la regulación adecuada que dote al gobernado de un blindaje especial, en el que a nivel gubernamental se garantice una protección a su información de carácter personal, con la que actualmente no se cuenta.

V. Bibliografía

Arenas Ramiro, Mónica, *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, 2005.

Ballesteros Moffa, Luis Ángel, *La privacidad electrónica*, Valencia, Tirant lo Blanch, 2005.

Corropio Gil-Delgado, María de los Reyes, *Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet*, Madrid, Arellano, 2000.

———, *El tratamiento de los datos de carácter personal y la protección de la intimidad en el sector de las telecomunicaciones*, Madrid, De Arellano, 2001.

Craig, Paul y Burga, Gráinne de, *EU Law text, Cases and Materials*, 3a. ed., Oxford, 2003.

DAVARA RODRÍGUEZ, Miguel Ángel, *Manual de protección de datos para abogados*, Navarra, Aranzadi, 2006.

———, *La seguridad en las transacciones electrónicas*, Madrid, Universidad Pontificia Comillas, 2005.

———, *La transposición de la Directiva sobre la privacidad y las comunicaciones electrónicas*, Madrid, Universidad Pontificia Comillas, 2005.

FERNÁNDEZ SALMERÓN, Manuel, *La protección de los datos personales en las administraciones públicas*, Madrid, Thomson-Civitas, 2003.

GÓMEZ ROBLEDO, Alonso y ORNELAS NÚÑEZ, Lina, *La protección de datos personales en México: el caso del Poder Ejecutivo Federal*, UNAM, 2006.

MANGAS MARTÍN, Araceli y LIÑÁN NOGUERAS, Diego J., *Instituciones y derecho de la Unión Europea*, 5a. ed., Madrid, Tecnos, 2005.

PIÑAR MAÑAS, José Luis, "El derecho fundamental a la protección de datos personales", *Protección de Datos de Carácter Personal en Iberoamérica* (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003), Valencia, Tirant lo Blanch, 2005.

———, *La Red Iberoamericana de Protección de Datos (Declaraciones y Documentos)*, Valencia, Tirant lo Blanch, 2006.

SANCHO VILLA, Diana, *Transferencia internacional de datos*, Madrid, De Arellano, 2003.

UNIVERSIDAD DE NAVARRA Y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Jornadas sobre la Protección de la Privacidad (Telecomunicaciones e Internet)*, Pamplona, Universidad de Navarra, 2000.

Direcciones electrónicas

http://www.un.org/spanish/aboutun/hrights.htm.
http://www.derechos.org/nizkor/espana/doc/conveudh50.html.
http://www.derechos.org/nizkor/ley/pdcp.html.
http://www.oas.org/juridico/spanish/Tratados/b-32.html.
http://www.oas.org/juridico/spanish/Tratados/b-32.html.
http://www.oecd.org/dataoecd/16/51/15590267.pdf.
http://www.unhchr.ch/spanish/html/menu3/b/71_sp.htm.
http://www.ifai.org.mx.
https://www.agpd.es/upload/Canal_Documentacion/Sentencias/Sentencia 292.pdf.