Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?

Cristos Velasco San Martín*

1. Introducción

La privacidad[1] y la protección de datos personales son elementos importantes en las distintas modalidades del comercio electrónico (B2B, B2C, G2B)[2], pero particularmente han tomado mayor relevancia en el área de B2C, al momento en que los consumidores llevan a cabo transacciones comerciales por medios electrónicos, compras en Internet o simplemente al intercambiar datos e información con otros usuarios, empresas y gobierno en la red.

El tema de protección de datos personales está tomando cada vez mayor importancia en otro tipo de portales de comercio electrónico como son el (G2B) y (G2C), sobre todo a medida que el gobierno mexicano implementa gradualmente el sistema E-Gobierno, por medio del cual pretende garantizar a los ciudadanos el libre acceso a una gama de servicios públicos integrales, como son sistemas de información pública y trámites en línea ante las diversas dependencias de las administraciones públicas federal, estatal y municipal.

*Miembro del Capítulo Mexicano de la Sociedad Internet (ISOC). Abogado especialista en tecnologías de la información y comercio electrónico. Su correo electrónico es: cristosuofa@yahoo.com

[1] El concepto jurídico de privacidad varia dependiendo del sistema jurídico de cada país (Sistema Common Law o Derecho Romano-Germánico), sin embargo, existen tres derechos fundamentales para la protección de los individuos que deben ser considerados bajo ambos sistemas jurídicos. El primero, el derecho a disfrutar de una vida privada libre, sin interrupciones o intrusiones indeseadas; el segundo, el derecho a comunicarse libremente con cualquier persona sin el temor a ser vigilado; y tercero, el derecho a controlar el acceso de la información personal.

[2] Nota del editor: B2B (business to business) es una abreviación acuñada en inglés para denotar la relación de comercio electrónico entre negocios; B2C (business to consumers) negocios y consumidores; G2B (government to business) gobierno y negocios; y G2C (government to citizen)

Es por ello que resulta relevante saber qué harán dichas dependencias con la información y los datos que proporcionen las empresas y personas al llevar a cabo trámites gubernamentales en Internet, ya que en un futuro no muy lejano, todos los asuntos y trámites ante gobierno se llevarán completamente en línea y toda la información que se genere estará contenida en sistemas electrónicos y bases de datos propiedad del gobierno.

El propósito de este artículo es dar a conocer al lector algunas políticas sobre privacidad y protección de datos elaboradas por los organismos internacionales más importantes, a nivel multilateral y analizar en forma general, algunos esquemas regulatorios adoptados por países de primer mundo, así como el marco jurídico nacional y las iniciativas de ley respecto a la privacidad y la protección de datos que se encuentran en el H. Congreso de la Unión. Estamos seguros que este artículo permitirá a nuestros legisladores tomar algunas ideas que los llevarán a analizar estos temas en forma más detallada con el propósito de evaluar si nuestro país debe o no contar en este momento con un marco jurídico al respecto, que por un lado tutele las garantías individuales de privacidad y el derecho a la intimidad de los ciudadanos; que no sea excesivamente sobre regulado para las empresas y el sector financiero y sobre todo que no contravenga las disposiciones de los tratados comerciales actualmente celebrados por México.

2. Marco jurídico en la Unión Europea

La privacidad y la protección de datos personales en Internet son temas que la comunidad internacional se ha enfocado a estudiar y analizar con más detenimiento, a raíz de los atentados terroristas del 11 de septiembre del 2001.

Muchos países, como por ejemplo algunos estados miembros de la Unión Europea han considerado los temas de privacidad y protección de datos personales como asuntos prioritarios en su agenda legislativa[3], con el propósito de hacer no sólo un frente comercial común a fuertes bloques comerciales regionales como son el TLCAN y el MERCOSUR, sino sobre todo como una medida proteccionista para salvaguardar y proteger los derechos y libertades de las personas físicas, en particular del derecho a la intimidad y la libre circulación de datos personales, derechos consagrados en las constituciones y leyes de los estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, buscando con base en estos ordenamientos jurídicos, proteger a los ciudadanos europeos al momento en que proporcionen información personal a empresas, filiales, sitios y organismos gubernamentales y no gubernamentales en línea que se encuentren físicamente localizados dentro del continente europeo o que tengan sus servidores fuera de países miembros de la Unión Europea.

---

gobierno y ciudadanos.

[3] Ver la Directiva 95/46 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 a la libre circulación de estos datos, disponible en la siguiente dirección: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=es&numdoc=31995L0046&model=guichett

La "Directiva 95/46 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 a la libre circulación de estos datos" (mejor conocida como la Directiva sobre Privacidad y Protección de Datos), entró en vigor el 25 de octubre de 1998 y su objeto es proporcionar un marco general de referencia para los países miembros. Esta Directiva establece reglas muy estrictas para la protección de los derechos y garantías de libertad de los ciudadanos europeos y en particular la protección del derecho a la privacidad con relación a la obtención y procesamiento de datos personales.

Una de las disposiciones más controvertidas que contiene esta Directiva es el artículo 25, que establece la prohibición a sus estados miembros de transferir datos personales e información a terceros países que no proporcionen una suficiente y adecuada protección a la privacidad. Aun cuando algunos países puedan proporcionar o satisfacer un adecuado nivel de seguridad y protección de los datos personales, dicha Directiva impone obligaciones adicionales bastante restrictivas para llevar a cabo la transferencia de datos a terceros países.

Esta Directiva, si bien ha sido adoptada por la mayoría de los países miembros, también ha encontrado algunas dificultades de implementación por parte de algunos otros estados miembros. Cabe señalar que en enero de 2000, la Comisión Europea decidió llevar a cabo procedimientos administrativos de sanción en contra de Francia, Alemania, Holanda, Irlanda y Luxemburgo por no haber comunicado a tiempo las medidas que tomaron para implementar esta Directiva en cada una de sus legislaciones internas.

En mayo de 2002, la Comisión Europea elaboró un cuestionario dirigido a los estados miembros con el objeto de poder implementar efectivamente la Directiva. La mayoría de los gobiernos enviaron la primera parte de sus respuestas a la Comisión Europea en junio de 2002.

Recientemente, el Gobierno del Reino Unido envió parte de sus respuestas a este cuestionario a la Comisión Europea y entre otros puntos propone revisar no sólo algunas reglas para poder implementar esta Directiva en su país debido a la rapidez y cambios que ha habido en los desarrollos tecnológicos, sino sobre todo con el propósito de darle mayor flexibilidad y efectividad a sus organismos de vigilancia, al mismo tiempo que le permita salvaguardar la protección de los datos personales de los ciudadanos ingleses.

Entre las propuestas del gobierno inglés se encuentran: (i) revisar las definiciones de "datos personales", "sistema de aplicación de datos personales" y "datos sensibles" con el objeto de mejorarlas y hacerlas más consistentes al momento de ponerlas en práctica; (ii) mejorar las reglas sobre procesamiento de datos personales; (iii) establecer reglas especiales de algunas definiciones como "datos sensibles" para que tengan una aplicación más práctica; (iv) revisar los arreglos de acceso en la materia para encontrar un balance entre los intereses de los sujetos que proporcionan datos personales y los intereses de los organismos

controladores de datos, sin reducir la efectiva protección de los datos personales; (v) revisar las reglas relacionadas con la transferencia de datos personales a terceros países y establecer criterios más simples y flexibles.

Recientemente, Finlandia, Suecia y Austria solicitaron cambios a la Directiva con el objeto de remover obstáculos burocráticos costosos e innecesarios.

A nivel internacional, esta Directiva también ha tenido serios problemas de aceptación en países que han adoptado políticas de regulación distintas a los países miembros de la Unión Europea, como es el caso de los Estados Unidos y algunos países asiáticos.

El artículo 25 de la Directiva sobre Privacidad y Protección de Datos contiene una clara restricción comercial que ha tenido un grave impacto a nivel mundial, sin embargo, en el caso de países latinoamericanos como Argentina, Chile y Paraguay han introducido legislación sobre protección de datos consistente con esta Directiva, con el objeto de estrechar sus lazos comerciales y diplomáticos con el continente europeo, sin tomar en cuenta que la prohibición del libre flujo transfronterizo de datos e información podría ocasionarles graves distorsiones comerciales con terceros países como los Estados Unidos y Canadá que eventualmente los podrían llevar a tener que sustanciar una controversia en el ámbito de la Organización Mundial del Comercio (OMC).

Es por estas razones, que nuestros legisladores deben ser muy cautelosos al tratar de adoptar un esquema de regulación europeo que pudiera inhibir no solamente el comercio transfronterizo de bienes y la prestación de servicios con terceros países, sino particularmente las actividades de comercio electrónico, el flujo transfronterizo de datos personales y las inversiones que se están realizando en México en el sector de las tecnologías de la información y los empleos que éstas generan.

3. Estados Unidos

En cambio, países como los Estados Unidos, si bien cuentan con un marco jurídico bastante amplio en materia de privacidad[4], también ha adoptado una política de autorregulación que ha estado a cargo en gran medida del sector privado, respondiendo satisfactoriamente a las demandas y necesidades de sus grandes corporaciones y protegiendo en la medida de lo posible los derechos básicos de los consumidores y de los ciudadanos con base en la primera enmienda de su Constitución[5].

---

[4] Como ejemplo de ello, podemos citar la Ley de Privacidad de 1974 (Privacy Act of 1974) cuyo objeto es regular la obtención y el uso de la información personal dentro del sector público.

[5] La primera enmienda de la Constitución de los Estados Unidos de América del Norte señala textualmente: “Amendment I Religious and Political Freedom.
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peacebly to assemble, and to petition the Government for a redress of grievances”.

Por otro lado, cabe destacar que la política de regulación de los Estados Unidos ha evolucionado de tal forma que hoy en día se ha ocupado más de legislar aquellos sectores que se consideran más sensibles y vulnerables para la sociedad, como son el sector salud[6] y la protección y confidencialidad de la información que proporcionen niños menores de edad a sitios en Internet[7].

En este orden de ideas, podemos decir que los Estados Unidos han adoptado una política mucho más flexible sobre privacidad y protección de datos que la Unión Europea, cuyo objetivo es proteger y tutelar los derechos de consumidores, la población vulnerable y más aún que se caracteriza por la adopción de un esquema más liberal para el sector empresarial. Los Estados Unidos han confiado sus políticas de regulación y privacidad a sus empresas porque saben que el gobierno está consciente de que estas acciones y mecanismos fomentan y reactivan el comercio electrónico, no sólo a nivel interno sino también a nivel mundial, promueven las inversiones del sector de las tecnologías de información y sobre todo permiten que las pequeñas y medianas empresas puedan realizar actividades de comercio electrónico en todos los niveles.

4. Canadá

Otros países, como Canadá por ejemplo, han seguido políticas de regulación sobre privacidad y protección de datos caracterizadas por la adopción de la llamada "Tercera Vía" (The Third Way), es decir, han tratado de adoptar un marco regulatorio que no sea ni excesivamente sobre regulado por el gobierno ni tampoco que sea libremente autorregulado por las empresas, sino que combine legislación y políticas de autorregulación eficientes que respondan específicamente a las necesidades individuales de sus nacionales, buscando con ello proteger los derechos de los ciudadanos y consumidores, sin menoscabar los intereses patrimoniales de las medianas y grandes empresas, estableciendo reglas claras y organismos gubernamentales ad-hoc eficientes para su debida vigilancia.

El 13 de mayo de 2002, el gobierno de la provincia de la Columbia Británica, convocó a una consulta pública con el objeto de crear una Iniciativa de Ley sobre Protección de la Privacidad para el Sector Privado como respuesta a los requerimientos de la Ley Federal denominada *"The Personal Information Protection and Electronic Documents Act (PIPED Act)"*[8].

[6] Como ejemplo de ello podemos destacar el "Health Insurance Portability and Accountability Act de 1996 (HIPPA)" que es una ley de carácter federal que protege la confidencialidad de los antecedentes y datos médicos de las personas.

[7] Como ejemplo de esto podemos citar el "Children's Online Privacy Protection Act de 1998" cuyo propósito es limitar la obtención, utilización y divulgación de información personal de niños menores de 12 años de edad por parte de los operadores de portales y sitios web que vayan dirigidos a la población infantil.

[8] El *PIPED Act*, contiene entre otras disposiciones, los estándares mínimos de protección a la privacidad en el ámbito del sector privado. Si una ley sobre privacidad de alguna provincia canadiense no cumple con los requisitos del PIPED Act, el gobierno federal podría desconocer

Para este fin, el Gobierno de esta provincia (The Corporate Privacy and Information Access Branch, Ministry of Management Services) distribuyó dos documentos de consulta; el primero contiene 10 preguntas básicas y sus respectivas respuestas en relación a la necesidad de contar con una legislación de privacidad para el sector privado; y el segundo documento contiene nueve puntos fundamentales a considerarse para esta legislación y que son: (1) Introducción y justificación; (2) Objetivos; (3) Ámbito de aplicación; (4) Derechos y obligaciones de los individuos, (5) Recolección de información personal; (6) Utilización y divulgación de la información; (7) Veracidad de la información; (8) Seguridad de la información y; (9) Vigilancia y protección de la privacidad en el sector privado.

Hasta donde tenemos conocimiento, esta Ley de la provincia de la Columbia Británica para el sector privado ya se encuentra vigente y fue el resultado de un consenso entre empresas, grupos de consumidores, ONG, órganos de gobierno, académicos y ciudadanos de esta provincia.[9]

5. Normatividad internacional

Ahora bien, en el ámbito internacional, cabe destacar la labor de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), organismo multilateral que ha elaborado importantes lineamientos y políticas sobre privacidad y protección de datos y protección al consumidor en el contexto del comercio electrónico, entre los más importantes. Aun cuando las guías o lineamientos que emite la OCDE no son obligatorios para muchos países en el ámbito del derecho internacional público, éstos son principios generalmente aceptados como recomendaciones de carácter voluntario comúnmente adoptadas por gobiernos, empresas, organizaciones y usuarios individuales de países miembros de la OCDE, como es el caso de México.

dicha ley y no considerarla como “sustancialmente similar”. A nivel internacional, el *PIPED Act* fue una de las primeras leyes reconocidas por el Parlamento y el Consejo de la Unión Europea como suficientemente “adecuada” para propósitos comerciales. Su entrada en vigor se encuentra dividida en tres fases distintas. La primera fase, en vigor desde el primero de enero de 2001, aplica a la regulación de organismos federales, específicamente a la información personal que utilicen organismos en actividades comerciales, así como información que las organizaciones recolecten, utilicen o proporcionen sobre sus empleados en relación con actividades laborales, de compromiso o de negocios a nivel federal. El 1o. de enero de 2002 entró en vigor la segunda fase de esta ley que regula específicamente la información sobre salud de los individuos. La tercera fase entrará en vigor el 1o. de enero de 2004 y regulará a organizaciones bajo la jurisdicción de cada una de las provincias canadienses, a menos que cada provincia implemente una legislación específica para el sector privado sustancialmente similar al *PIPED Act*.
Antes de la entrada en vigor del *PIPED Act*, Quebec era la única provincia en Canadá que contaba con una amplia legislación sobre privacidad para el sector privado. El *PIPED Act* se encuentra disponible en la siguiente página:
http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp

[9] The *Freedom of Information and Protection of Privacy Act de la Provincia de British Columbia* se encuentra disponible en la siguiente dirección:
http://www.legis.gov.bc.ca/37th3rd/3rd_read/gov07-3.htm

Las guías de la OCDE que regulan la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales del 23 de septiembre de 1980[10] contienen ocho principios complementarios de aplicación nacional y cuatro de aplicación internacional que son considerados como los estándares mínimos a seguir para la obtención, el procesamiento de datos y el libre flujo transfronterizo de datos para los sectores público y privado.

Los ocho principios de aplicación a nivel nacional son los siguientes:

1. El principio de "Límite de obtención", consistente en la imposición de límites para la obtención de datos personales a través de medios apropiados y legales haciéndolo del conocimiento y obteniendo el consentimiento;

2. El principio de "Calidad de los datos", consistente en la importancia de asegurar la exactitud, totalidad y actualización de los datos;

3. El principio del "Propósito de descripción", consistente en especificar el propósito de recabar información en el momento en el que se lleva a cabo la recolección y el subsecuente uso limitado del cumplimiento de dichos propósitos u otros que no sean incompatibles con aquellos propósitos especificados en cada ocasión;

4. El principio del "Límite de uso", consistente en no divulgar los datos personales o aquellos utilizados para propósitos distintos a los contemplados en el principio anterior, excepto:

- el consentimiento sobre la materia de datos;
- mediante una autoridad contemplada en ley.

5. El principio de "Protección a la seguridad", consistente en proteger los datos personales e información, mediante mecanismos razonables de seguridad en contra de riesgos tales como pérdida, acceso no autorizado, destrucción, utilización, modificación o divulgación de datos;

6. El principio de "Imparcialidad", consistente en establecer políticas generales de imparcialidad sobre desarrollos, prácticas y políticas con respecto a los datos personales, asegurando la transparencia en el proceso de obtención de información y estableciendo los propósitos para su utilización;

7. El principio de "Participación individual", consistente en el derecho que tiene un individuo de: obtener del controlador de datos la confirmación de tener o no los datos del individuo; que el controlador de datos se lo haya comunicado en un tiempo y forma

[10] Estas guías se encuentran disponibles en idioma inglés en la página de la OCDE en la siguiente dirección:
http://www.oecd.org/EN/document/0,,EN-document-29-nodirectorate-no-24-10255-29,00.html

razonable; obtener respuesta del controlador de datos si una solicitud le ha sido negada y tener la posibilidad de impugnarla; tener la posibilidad de impugnar datos personales y si la impugnación resulta exitosa solicitar que los datos sean eliminados, modificados, rectificados o complementados; y

8. El principio de "Responsabilidad", consistente en la responsabilidad del controlador de datos de cumplir efectivamente con medidas suficientes para implementar los siete principios anteriores.

Los cuatro principios de aplicación internacional son los siguientes:

1. Que los países miembros tomen en cuenta las implicaciones que tiene el procesamiento doméstico y la reexportación de datos personales para otros países miembros;

2. Que los países miembros tomen las medidas apropiadas y razonables para asegurar que los flujos transfronterizos de datos personales incluyendo el tránsito a través de un país miembro sea ininterrumpido y seguro;

3. Que un país miembro se abstenga de restringir los flujos transfronterizos de datos personales entre sí mismo y otros países miembros, excepto cuando este último no haya observado sustancialmente estos lineamientos o cuando la reexportación de dichos datos contravenga su legislación interna de privacidad. Un país miembro podrá imponer restricciones en relación a ciertas categorías de datos personales para las cuales su legislación doméstica de privacidad incluya regulaciones específicas en vista de la naturaleza de aquellos datos y para los cuales el otro país miembro no proporcione protección equivalente.

4. Los países miembros deberán evitar el desarrollo de leyes, políticas y prácticas en nombre de la protección de la privacidad y las libertades individuales que pudieran crear obstáculos a los flujos transfronterizos de datos personales que pudieran exceder requisitos para dicha protección.

En términos generales, podemos señalar que el contenido de estas guías sobre privacidad y protección de datos, proporcionan principios y reglas específicas a seguir para que los gobiernos adopten políticas de regulación efectivas sobre privacidad y protección de datos y sobre todo sirven como fundamento para uniformar legislaciones en materia de privacidad que permitan, simultáneamente, evitar distorsiones al libre flujo transfronterizo de la información y los datos personales a nivel internacional.

6. Legislación mexicana

A) El marco constitucional

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos representa el marco jurídico de la privacidad en nuestro país. El primer párrafo de este artículo consagra una de las garantías individuales más importantes que es el derecho que tenemos a no ser molestados en nuestra 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.

Asimismo, el penúltimo párrafo de este artículo contempla que la correspondencia que bajo cubierta circule por las estafetas, deberá estar libre de todo registro y su violación será penada por la ley.

B) El marco jurídico aplicable en el B2C

El marco jurídico del comercio electrónico en México es relativamente reciente[11], sin embargo la protección de datos personales en el área de B2C ya se encuentra regulada en la Ley Federal de Protección al Consumidor (LFPC) y actualmente dicha legislación contempla la posibilidad de que los proveedores y consumidores puedan celebrar transacciones a través de medios electrónicos.

La fracción I del artículo 76 bis[12] de la LFPC le impone la obligación a los proveedores de mantener la confidencialidad de la información y la prohibición de difundirla o transmitirla a otros proveedores, a menos que el consumidor lo haya autorizado por escrito (*opt in*) o que exista un requerimiento de alguna autoridad, asimismo, la fracción II de este mismo artículo impone al proveedor la obligación de mantener segura y confidencial la información e informar al consumidor sobre las características generales de los elementos técnicos disponibles antes de la celebración de una transacción.

---

[11] La primera legislación en comercio electrónico fue el Decreto publicado en el Diario Oficial de la Federación del 29 de mayo del 2000, por medio del cual se reformaron y adicionaron diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor.

[12] El artículo 76 bis se incluyó dentro del Capítulo VIII BIS de la Ley Federal de Protección al Consumidor, tomando en cuenta los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico de la Organización para la Cooperación y el Desarrollo Económico (OCDE). Estos lineamientos se encuentran disponibles en su versión en español en la página de la OCDE en la siguiente dirección:
http://www.oecd.org/EN/document/0,,EN-document-44-1-no-24-320-44,00.html

Adicionalmente, algunas disposiciones sobre privacidad se encuentran contempladas en otros ordenamientos jurídicos como son la Ley de Imprenta, la Ley Federal del Derecho de Autor, la Ley del Instituto Nacional de Estadística, Geografía e Informática, el Código Penal Federal, entre otros.

C) Iniciativas de Ley sobre Protección de Datos Personales y Privacidad

a) Iniciativa de Decreto que expide la Ley Federal de Protección de Datos Personales[13]
Esta fue la primera Iniciativa en relación con el tema de privacidad y protección de datos personales que se originó en la Cámara de Diputados del H. Congreso de la Unión. Dicha Iniciativa fue presentada el día 6 de septiembre del 2001, por el Diputado Miguel Barbosa Huerta del Grupo Parlamentario del Partido de la Revolución Democrática (PRD) ante la LVIII Legislatura del H. Congreso de la Unión y publicada en la Gaceta Parlamentaria el 7 de septiembre de 2001. Está basada en gran medida en la Directiva 95/46 sobre Privacidad y Protección de Datos de la Unión Europea y la Ley Orgánica Española de Protección de Datos de Carácter Personal del 13 de diciembre de 1999.

Hasta donde se tiene conocimiento, esta Iniciativa de Ley fue turnada a la Comisión de Gobernación y Seguridad Pública, contiene una opinión de la Comisión de Comercio y Fomento Industrial de la Cámara de Diputados y actualmente se encuentra detenida por no contar con el aval y visto bueno de los sectores público, privado y académico.

b) Iniciativa de Ley Federal de Protección de Datos Personales[14]

Esta Iniciativa fue presentada por el senador Antonio García Torres y firmada por los senadores Manuel Bartlett Díaz en su carácter de Presidente de la Comisión de Puntos Constitucionales y el Senador Fidel Herrera Beltrán en su carácter de Presidente de la Comisión de Estudios Legislativos. Esta Iniciativa fue aprobada en el Senado el 30 de abril del 2002 y publicada en la Gaceta Parlamentaria del 5 de septiembre del 2002; posteriormente fue turnada para su respectivo dictamen a las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos, y subsecuentemente a la Cámara de Diputados. Esta iniciativa es la que tiene mayores probabilidades de ser aprobada y la que en los últimos meses ha causado mucha polémica entre los sectores más vulnerables de la sociedad sobre servicios de información. Al igual que la Iniciativa de Decreto que expide la Ley Federal de Protección de Datos Personales, esta Iniciativa no cuenta con el aval y visto bueno de la sociedad, además de que tiene un serio problema de inconstitucionalidad por haberse originado directamente en la Cámara de Senadores.

---

[13] Esta Iniciativa se encuentra disponible en la página del Congreso de la Unión en la siguiente dirección: http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm

[14] Esta Iniciativa se encuentra disponible en la página del Congreso de la Unión en la siguiente dirección: http://gaceta.cddhcu.gob.mx/

Esta Iniciativa está basada en la Directiva 95/46 sobre Privacidad y Protección de Datos de la Unión Europea. El contenido y ámbito de aplicación de esta Iniciativa son poco claros y demasiado ambiguos en cuanto al registro de bases de datos; contiene reglas bastante estrictas para la transferencia de datos personales a terceros países y establece órganos de vigilancia en la esfera de la administración pública federal que no se han implementado aún y que seguramente impondrán cargas burocráticas excesivas para empresas de tecnologías de la información, de mercadotecnia y publicidad y en general de servicios de información. Esta Iniciativa, de ser aprobada por el Poder Ejecutivo, podría traer consigo un grave impacto económico en la sociedad mexicana en cuanto a generación de empleos e inversiones que posiblemente podría guiar a algunas empresas a operar clandestinamente o prestar sus servicios en terceros países, inhibiendo en forma considerable el desarrollo del comercio electrónico, las inversiones y la creación de empleos en territorio nacional.

Consideramos urgente, que el H. Congreso de la Unión organice una Mesa de Trabajo sobre Privacidad y Protección de Datos Personales, tal y como lo hizo la Comisión de Comercio y Fomento Industrial de la Cámara de Diputados desde principios de este año en las Mesas de Trabajo que organizó sobre comercio electrónico, nombres de dominio, firma electrónica y delitos informáticos. Estamos seguros que de organizarse una mesa de trabajo de esta naturaleza, se contará con la participación de los sectores interesados de la sociedad como son cámaras empresariales, empresas del sector de la TI, publicidad y mercadotecnia, entidades financieras, asociaciones, fedatarios públicos, representantes de la administración pública federal, grupos académicos, entre otros. Mediante un foro de este tipo, tendremos la oportunidad de analizar las aplicaciones tecnológicas más avanzadas de la industria para la protección de la privacidad y la protección de datos (*Privacy Enhancement Technologies*), escuchar puntos de vista, analizar propuestas y revisar las disposiciones más controvertidas de la última Iniciativa en comento. Estamos seguros que lo anterior nos llevará a encontrar un balance apropiado para la adopción de un esquema regulatorio bien estructurado, que por un lado, combine programas de regulación del sector privado y propuestas de los sectores público y académico, protegiendo en la medida de lo posible las garantías constitucionales de los individuos de libertad y privacidad, sin inhibir el desarrollo del comercio electrónico en México.

7. Conclusión

La regulación de la privacidad y protección de datos personales ha sido abordada a nivel mundial en forma muy particular por cada país. Ello se debe, en gran medida, a los intereses económicos, políticos y sobre todo responde a las estrategias comerciales de cada país. Actualmente el continente europeo es el más regulado en cuanto a protección personal de datos se refiere y el flujo transfronterizo de los mismos, inhibiendo en forma considerable sus relaciones comerciales con otros países como Estados Unidos, Canadá y algunos otros del continente asiático.

En México, la privacidad y los datos de las personas en las relaciones entre empresas y consumidores ya se encuentra regulada en la Ley Federal de Protección al Consumidor. Asimismo, existen otras disposiciones sobre privacidad que se encuentran contenidas en otros ordenamientos jurídicos a nivel federal. En la medida en la que exista una mayor penetración y uso del Internet en México, se deberá evaluar la posibilidad de crear un marco jurídico más amplio y eficiente que proteja los datos e información que proporcionen los ciudadanos no sólo a los sitios web de las empresas, sino sobre todo a los órganos gubernamentales cuyos servicios se ofrecerán completamente en línea en un futuro no muy lejano.

Resulta conveniente que en sectores altamente sensibles en donde la información de las personas es considerada primordial, como son el sector salud o el laboral, se contemple la posibilidad de incluir aspectos de privacidad y protección de datos en el ámbito de sus respectivas leyes y reglamentos, esto por supuesto, en la medida en que se vaya incrementando el uso del Internet en México y de acuerdo a las necesidades específicas que la sociedad vaya requiriendo.

Por último, insistimos una vez más en la urgente necesidad de que el H. Congreso de la Unión organice una Mesa de Trabajo sobre Privacidad y Protección de Datos Personales, con el objeto de que nuestros legisladores conozcan las opiniones de los sectores interesados de la sociedad, el uso de las tecnologías más avanzadas sobre privacidad, las políticas sobre privacidad aprobadas a nivel multilateral y el impacto que ha tenido la regulación de la privacidad y protección de datos en otros países para que, de esa forma, puedan evaluar junto con todos los partícipes e interesados en el tema, si será conveniente o no contar con una legislación específica en México.