

LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO: UNA PROPUESTA PARA DELIBERAR

Introducción

El siglo XXI comienza con un despliegue tecnológico estelar. Ya no es posible concebir la vida de los seres humanos ni su interacción, sin el uso de tecnologías informáticas *urbi et orbi*. Dicha expansión conlleva el intercambio de flujos de información de todo tipo, incluida la relativa a las personas. Hoy en día, es posible acceder a información sobre millones de seres humanos y sus actividades en prácticamente cualquier parte del planeta.

Aunque a lo largo de la historia de la humanidad se han conquistado grandes espacios en materia de libertad de información y de expresión, el hecho de que los avances tecnológicos permitan irrumpir silenciosamente en el ámbito de lo privado, vulnera la esfera de uno de los derechos fundamentales de los individuos, el de la privacidad.

En este contexto, puede afirmarse que los horizontes de la privacidad se están transformando en *terra incognita, en un terreno desconocido para quienes lo habitan*, debido a que sin que las personas se enteren, ni mucho menos otorguen su consentimiento, terceros –ya sean entes públicos o privados- recaban y transmiten información sobre sus datos personales a través de todo tipo de procedimientos que echan mano de tecnologías de punta. Entre éstos destacan la minería de datos o la geo-localización, la detección remota o la video vigilancia, dispositivos que hoy en día han madurado y están fácilmente disponibles en cualquier lugar del mundo. Además, todo lo anterior se difunde a través de las supercarreteras de información en Internet en donde los proveedores de servicios cuentan con una monumental capacidad para almacenar y analizar los datos a

través de buscadores que de manera precisa pueden conocer casi todo acerca de un individuo usuario de la red.

Es cierto que los avances tecnológicos generalmente repercuten de forma positiva en la calidad de vida del ser humano, pero sería ingenuo desconocer que también con ellos nacen nuevos conflictos e interrogantes a los que el Derecho, en su objetivo último de ordenar la convivencia social, debe dar respuesta. La tecnología no puede permanecer ajena al Derecho, ni evidentemente a la Constitución, por más que la velocidad con la que ocurren las innovaciones tecnológicas amenace con hacer obsoleto cualquier esfuerzo por regular su impacto sobre el derecho a la vida privada.¹

La probabilidad de que se susciten abusos a la vida privada aumenta hoy como consecuencia del desarrollo de la llamada "sociedad de la información". La expansión global de las redes informáticas y de comunicación hace cada vez más frecuentes los casos de robo de identidad o de discriminación a través de la obtención de perfiles que hacen identificables a las personas en sus patrones de consumo y de ahorro, o en sus inclinaciones y preferencias.

Dado que los medios tradicionales de protección de la vida privada son insuficientes en la actualidad, cada vez más países han aprobado leyes de protección de datos personales²

Los países que otorgan un mayor grado de importancia a la esfera de lo íntimo suelen tener un pasado cultural e histórico marcado por experiencias de invasión en la vida privada de las personas.³ Así por ejemplo, Alemania ha sido uno de los

⁴ GUERRERO PICÓ, María del Carmen. El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal. Estudios de Protección de Datos. Agencia de Protección de Datos de la Comunidad de Madrid. Thomson Civitas, 2006.

² El último reporte sobre Privacidad y Derechos Humanos 2006 del *Electronic Privacy Information Center (EPIC)*, da cuenta de los desarrollos constitucionales, legales y del marco regulatorio en materia de protección a la privacidad en más de 75 países alrededor del mundo. Ver www.epic.or

³ Esta afirmación corresponde, entre otros a J. DHONT y M. V. PEREZ ASINARI, "New Physics and the Law. A comparative Approach to the EU and US Privacy and Data Protection Regulation, looking for Adequate protection" en Flujos transfronterizos y extraterritorialidad: La postura

precursores del derecho a la autodeterminación informativa para cada individuo, porque sabe del riesgo que implica acumular información sobre las personas para ejercer control sobre sus destinos.

Recientemente la Cumbre Mundial de la Sociedad de la Información ha hecho un llamado para pedir normas “mundiales” para la privacidad, convocando “... a todas las partes interesadas en garantizar el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de una legislación, la aplicación de marcos de colaboración, de mejores prácticas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios”.⁴

Antecedentes históricos

Me voy a permitir delinear los antecedentes normativos que en materia de protección de datos personales existen a nivel internacional. Los primeros esfuerzos se dieron en Europa, con la Resolución 509 de la Asamblea del Consejo de Europa sobre los “derechos humanos y nuevos logros científicos y técnicos” emitida en 1967, que marcó la pauta, sin embargo, no fue sino hasta el final de la década de los setenta, cuando Alemania, Francia, Dinamarca, Austria y Luxemburgo aprobaron leyes nacionales para la protección de datos personales.

Durante los años ochenta, justo cuando hace su aparición la computadora personal o PC, el Consejo de Europa se pronunció sobre la protección de la intimidad frente a la potencial agresividad de las tecnologías, a través de la promulgación del Convenio No. 108 para proteger a las personas frente al tratamiento automatizado de sus datos. El, propósito era garantizar a los ciudadanos de los Estados contratantes el respeto de sus derechos y libertades, en particular, el derecho a la vida privada, conciliándolo con la libre circulación de la información entre los Estados miembros.

europa, PUOLET, Ives, Revista Española de Protección de Datos p.112. Julio-Diciembre 2006. Thomson Civitas.

⁴Idem.

Finalmente, en el año 2000, se aprobó la Carta de Derechos Fundamentales de la Unión Europea en la que se elevó la protección de los datos personales al rango de derecho fundamental. Actualmente el Tratado de Lisboa mantiene este reconocimiento al derecho a la intimidad y a la privacidad de las personas como derecho autónomo.

Por otra parte, en 1980 en el marco de la Organización para la Cooperación y el Desarrollo Económico -OCDE- se emitió una recomendación que contiene las “Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales”, que constituyó el primer instrumento supranacional que analiza a profundidad el derecho a la protección de estos datos.

Su adopción se funda en la constatación por parte del Consejo de la OCDE de la inexistencia de una regulación uniforme en esta materia en los distintos Estados miembros, **lo cual dificultaba el flujo de los datos personales entre ellos mismos.**

Igualmente, en el Foro de Cooperación Economía Asia Pacífico -APEC-, en vísperas del cambio de siglo, se estableció un Grupo de Manejo del Comercio Electrónico que tiene dentro de sus principales actividades el desarrollo de legislaciones y políticas compatibles entre las economías participantes en el campo de la privacidad. Por ello, APEC ha emitido lineamientos generales en la materia con el fin de que éstos se establezcan en los cuerpos legales correspondientes para lograr un flujo de datos seguro, pero al mismo tiempo, sin obstáculos para fomentar el comercio.

Finalmente, la Organización de las Naciones Unidas emitió en 1990 la Resolución 45/95 que contiene una lista básica de principios para la protección de datos personales de aplicación mundial, como el de exactitud de los mismos, la determinación de su finalidad, su acceso y la no discriminación.

En resumen, los desarrollos normativos en el ámbito internacional han buscado **proteger a la persona y no al dato *per se***. Estas disposiciones establecen los principios y derechos que tiene un individuo para exigirle tanto al Estado como a los particulares quien, cuándo y para qué pueden utilizar sus datos personales.

Los ejes rectores pueden resumirse en el principio de licitud o trato leal de los datos, de finalidad, de proporcionalidad, de calidad y de seguridad. Los derechos se resumen en el acrónimo ARCO, es decir el derecho de acceder a su información y en caso de ser inexacta de rectificarla, el derecho a cancelar el dato cuando ya no es pertinente o ha perdido vigencia y el derecho a oponerse a su utilización por parte de un tercero.

Vale la pena anotar que esta normativa aunque con diferentes enfoques y diseños institucionales, abarca tanto al sector público como al privado y en el caso de la Directiva Comunitaria, a efecto de que puedan fluir datos desde Europa al resto del mundo, se prevé la necesidad de otorgar un reconocimiento a terceros países que cuenten con un nivel adecuado de protección a la privacidad, entre los que se encuentra por cierto, Argentina. Este “nivel de adecuación” se ha visto como una barrera encubierta al comercio, pero tiene sustento en lo que la doctrina ha denominado el “principio de continuidad de la protección”, pues asegura al individuo que si su dato está protegido en el espacio europeo, también lo estará en otras latitudes.

¿Qué está en juego cuando hablamos de datos personales?

¿cuál es la relevancia de contar con una ley que regule la protección de estos datos?

Para contestar a la pregunta me voy a permitir mencionarles algunos ejemplos internacionales que nos ayudan a dimensionar la importancia de regular el derecho a la protección de datos y la complejidad que ello entraña.

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 dichas medidas, el gobierno norteamericano expidió en octubre de 2001 la *Ley Patriota (Patriot Act)* cuya finalidad, en términos generales, era salvaguardar la seguridad nacional de los Estados Unidos de América y sus ciudadanos.

A raíz de la *Ley Patriota*, el vecino del norte emitió disposiciones⁵ que obligan a las compañías aéreas o marítimas que operen en su territorio a facilitarles los datos de sus pasajeros y la tripulación.

El medio electrónico para facilitar estos datos es el Sistema de Información Avanzada sobre Pasajeros (APIS) y se compone de los datos sobre cada persona física que viaja de y a los Estados Unidos. En general, los datos que se transfieren son: nombre, fecha de nacimiento, nacionalidad, sexo, número de pasaporte y lugar de expedición, país de residencia, número de visado en los Estados Unidos, lugar y fecha de expedición,, domicilio en los Estados Unidos durante la estancia, así como fecha de reservación, la agencia de viajes contratada, la información que se muestra en el boleto, los datos financieros (número de tarjeta de crédito, fecha de caducidad, dirección del lugar de expedición, etc.), el itinerario, información sobre el transportista que opera el vuelo (número de vuelo, etc.), número de asiento y datos anteriores del PNR (*Passenger Name Records*). En estos últimos pueden constarse no sólo los viajes realizados en el pasado, sino también información de carácter religioso o étnico (elección de la comida), afiliación a un determinado grupo, los medios para contactar a una persona (dirección de correo electrónico, información sobre un amigo, lugar de trabajo, etc.), datos médicos (cualquier asistencia médica que se haya requerido, oxígeno,

⁵ La Aviation and Transportation Security Act (noviembre de 2001) y la Enhanced Border Security and Visa Entry Reform Act (mayo 2002)

problemas relacionados con la vista, el oído o la movilidad y datos relacionados, por ejemplo, con los programas de viajeros frecuentes.⁶

Esta auténtica invasión en la vida privada de los viajeros produjo reacciones en diversos puntos del orbe. La más enérgica provino de la Unión Europea, toda vez que bajo la perspectiva de esta última los Estados Unidos no garantizaban un nivel de protección acorde al estándar europeo, debido a que no contaban con una legislación general en la materia, ni poseían una autoridad nacional que garantizara el debido ejercicio del mencionado derecho.

El 21 de noviembre de 2007, el gobierno del Reino Unido reconoció que había perdido dos discos con información confidencial de casi la mitad de la población del país. Los discos, que contenían los **datos bancarios y de seguridad social de cerca de 25 millones de personas**, "se extraviaron" (cito) mientras eran trasladados de un departamento del gobierno a otro.

La oposición dijo que había sido un error "catastrófico" del gobierno y algunos especialistas señalaron que se podría tratar de **la mayor falla de seguridad que hubiera tenido lugar en Europa**.

El líder interino del Partido Liberal Demócrata, Vince Cable preguntó ¿Por qué el departamento de hacienda y aduanas todavía usa discos compactos para la transmisión de datos? y añadió que después de este desastre, ¿cómo podía el público tener confianza en las enormes bases de datos centralizadas para el programa de células de identidad obligatorias que se estaban elaborando?

El 11 de mayo de 2008, se tuvo conocimiento del mayor jaqueo de la historia en Chile. Los datos personales de seis millones de chilenos (más del 30% de la población de ese país que asciende a 16 millones) quedaron públicamente

⁶ 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.

disponibles en Internet durante la madrugada y la mañana del 10 de mayo, luego de que fueran sustraídos desde los servidores de diferentes entidades públicas y privadas.

Seguramente ustedes se preguntarán qué tan importante es para el ciudadano contar con una norma que reconozca el derecho a la protección de datos personales en un país como el nuestro en donde no hemos tenido o no hemos conocido de experiencias como las que he reseñado. (aunque en 2003 se supo de una venta de los datos del padrón electoral a la empresa Choicepoint) La respuesta puede resumirse en una palabra “certeza”, certeza para saber qué datos personales son transmitidos y para qué fin, y cómo garantizar que éstos sean transmitidos única y exclusivamente a autoridades previamente determinadas y no de manera discrecional.

Pero el tema no se queda en cuestiones internacionales, también guarda estrecha relación con otros ámbitos de la vida de los gobernados, por ejemplo, tenemos el caso del expediente clínico. En los países que cuentan con normas en la materia se establecen una serie de derechos a favor de los pacientes que van desde cuestiones básicas como el acceso al citado expediente por parte de su titular, hasta cuestiones de legitimación para el tratamiento de datos de salud cuando el titular se encuentra imposibilitado para otorgar su consentimiento.

Otro caso interesante es el de los expedientes crediticios, que con una adecuada regulación en materia de protección de datos, permitiría que los particulares contaran con instrumentos efectivos para exigir a las instituciones bancarias o al buró de crédito que se actualice su situación crediticia, particularmente en los casos en los que el deudor ha liquidado su crédito con el banco y tiene derecho a que sea borrado de la lista.

Con estos ejemplos, me referiré ahora a la situación normativa de los datos personales en México.

Situación normativa de los datos personales en México

Como ustedes saben, el 11 de julio de 2002, fue publicada en el Diario Oficial de la Federación la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental⁷. Los límites al derecho de acceso a la información están señalados de manera expresa en la propia Ley y ahí se establece que los datos personales constituyen información confidencial y requieren del consentimiento de los individuos para su difusión, distribución o comercialización. También se establecen disposiciones sobre los derechos de acceso y corrección de los datos personales, así como algunas reglas en torno a los procedimientos para hacerlos efectivos.

La reforma al artículo 6° constitucional de junio de 2007 que significó un salto cualitativo en nuestra evolución normativa en materia de acceso a la información, sólo tiene una breve referencia a la privacidad: “la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes”. Es decir, sólo aparece en función del derecho a la información y carece de un desarrollo propio, pues éste se remite a la norma secundaria.

No obstante, la inquietud ya está sembrada y existen diversos proyectos legislativos en torno al tema en el Congreso de la Unión, aunque ninguno de ellos ha fructificado porque no existe una disposición constitucional que sustente la protección de datos personales como un derecho fundamental autónomo, o la posibilidad de que el Congreso legisle en la materia.

Existe ya un Proyecto de Decreto por el que se adicionan dos párrafos al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos que establece por una parte que toda persona tiene derecho a la protección de sus datos personales,

⁷ http://www.diputados.gob.mx/LeyesBiblio/decre/LFTAIPG_06jun06.doc.

a acceder a los mismos, y en su caso, a obtener su rectificación, o cancelación y a manifestar su oposición en los términos que fijen las leyes.

En congruencia con el proyecto de reforma constitucional aludido, está el correspondiente a la reforma del artículo 73 constitucional. que tiene por objeto dotar de facultades al Congreso Federal para legislar en materia de protección de datos en posesión de los particulares.

Hay varias razones importantes para impulsar que la ley que regule los datos personales en posesión de los particulares sea federal: 1) por el comercio internacional, pues el Estado Mexicano debe contar con una legislación uniforme para normar sus relaciones internacionales, independientemente del área del territorio nacional en donde materialmente se estén utilizando los datos personales.

2) El Poder Ejecutivo Federal administra grandes bases de datos con información muy variada de las personas, ya que para el ejercicio de sus atribuciones, o para la adecuada aplicación de las leyes.

Es el caso por ejemplo de la Base Nacional de Datos de la clave única del registro de población -CURP-, la base de datos del Servicio de Administración Tributaria sobre contribuyentes, los sistemas de expedientes clínicos del sector salud en el que se alojan millones de expedientes de derechohabientes e incluso las bases de datos generados en materia de seguridad pública que utilizan herramientas tecnológicas que permiten renovar y modernizar la acción policial como la Plataforma México, que incluye el fortalecimiento de la Red Nacional de Telecomunicaciones y el Sistema Único de Información Criminal.

Al esfuerzo realizado en torno a la protección de datos, también se ha sumado la Suprema Corte de Justicia de la Nación con las reformas del 12 de diciembre de 2007 al Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo

de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en virtud de las cuales se establece que en los documentos contenidos en los expedientes que no sean reservados o confidenciales, se suprimirán los datos personales de las partes. También establecen que las sentencias ejecutorias y demás resoluciones públicas dictadas en expedientes de cualquier materia que por su naturaleza puedan afectar de algún modo la dignidad personal o causar un daño irreparable, se difundirán en una versión impresa o electrónica de la que se supriman los datos personales de las partes, en la medida en que no impidan conocer el criterio sustentado por el juzgador.

Conclusiones

Han pasado ya 7 años, desde que se presentó la primera iniciativa de Ley de protección de datos personales. A partir de entonces, la discusión legislativa entró en un *impasse*. Parece que el tema no es prioritario en la agenda nacional, pero en cambio cada vez hay más conciencia de la mala utilización que se hace de algunas bases de datos para fines comerciales. Quién no ha sido perturbado en su hogar para ofrecerle tarjetas de crédito a partir del conocimiento que se tiene de sus niveles de consumo., o para invitarle a votar por algún candidato, utilizando los datos en bases de datos públicas o privadas?

Estoy convencida de que existen ya las condiciones para que la sociedad entable un diálogo maduro con los legisladores encaminado a diseñar una ley moderna que recoja las mejores prácticas y los mecanismos mas adecuados de tutela para garantizar que no se viole nuestra preciada intimidad