Artículo **Revista de Tecnologías de la Información**
Diciembre 2014 Vol.1 44-56

Privacidad de datos

VAZQUEZ- Adrian†

Universidad Iberoamericana.

Recibido 29 de Enero, 2014; Aceptado 29 de Julio, 2014

Resumen

Hablar de este tema es vasto y variado definir como nombre los datos personales, teléfono, dirección, fotografía o huellas dactilares, así como cualquier otra información que le pueda identificar, es fundamental para lo que nos importa estos datos por razones de seguridad y porque es nuestro derecho.

Los datos deben ser protegidos contra el abuso, como el robo de identidad, transmisiones indebidas o ilegales o acceso no autorizado.

La nueva legislación pone a las personas en el centro de la atención estatal mexicanos ahora tienen legislación que protege la información personal que se puede encontrar en las bases de datos de cualquier persona o empresa como compañías de seguros, bancos, grandes almacenes, teléfono, hospitales, laboratorios, universidades. Esta legislación contiene una serie de reglas claras y respetuosas de la privacidad, la dignidad y la información de los individuos, derivadas del observado internacionalmente por otros países. La ley regula la forma y condiciones en que las empresas deben utilizar su información personal.

Por ejemplo, el origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencias sexuales.

Privacidad, la Información Personal, Protección.

Abstract

To talk about this topic is vast and varied define as personal data name, phone , address, photograph or fingerprints , as well as any other information that can identify you , it is critical to what we care this data for security reasons and because it is our right .

The data must be protected against misuse such as identity theft, improper or illegal transmissions or unauthorized access.

The new legislation puts people at the center of state care Mexicans now have legislation that protects personal information that can be found in the databases of any person or company as insurance companies, banks , department stores , phone , hospitals , laboratories, universities . This legislation contains a number of clear and respectful rules of privacy, dignity and information of individuals, derived of internationally observed by other countries. The law regulates the manner and conditions under which companies must use your personal information.

For example, racial or ethnic origin , health status , genetic information, religious, philosophical and moral beliefs , trade union membership , political opinions and sexual preferences.

Privacy, Personal Information, Protection.

Citación: VAZQUEZ- Adrian. Privacidad de datos. Revista de Tecnologías de la Información 2014, 1-1:44-56

† Investigador contribuyendo como primer autor.

Artículo **Revista de Tecnologías de la Información**
Diciembre 2014 Vol.1 44-56

Introducción

Hablar de este tema es muy amplio y variado definimos como datos personales el nombre, teléfono, domicilio, fotografía, o huellas dactilares, así como cualquier otro dato que pueda identificarte, resulta crítico qué cuidemos estos datos por razones de seguridad y porque es nuestro derecho.

Los datos deben ser protegidos contra el mal uso como robo de identidad, transmisiones indebidas o ilícitas o accesos no autorizados.

La nueva legislación coloca a las personas en el centro de la tutela del Estado

Los mexicanos cuentan hoy con una legislación que protege la información personal que pueda encontrarse en las bases de datos de cualquier persona física, o empresa como, aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades.

Esta legislación contiene una serie de reglas claras y respetuosas de la privacidad, dignidad e información de las personas, derivadas de principios internacionalmente observados por otros países del mundo.

La Ley regula la forma y condiciones en que las empresas deben utilizar tus datos personales.

Por ejemplo: origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencias sexuales.

Marco teórico

La ley federal de Protección de Datos Personales en Posesión de Particulares, también referenciada como LFPDPPP fue publicada en el Diario Oficial de la Federación el 5 de Julio de 2010 con entrada en vigor un año después es la primera ley de este tipo aprobada en México, existen antecedentes sobre leyes de protección de datos sin embargo es la primera que abarca en un sentido amplio con reglas estándar, posee ciertas similitudes con las leyes de protección de datos existentes en la Unión Europea, principalmente España y también con las leyes existentes en Argentina quien lidera el cambio dentro de América Latina.[1]

Esta ley aplica únicamente al tratamiento de la información realizada por particulares, por lo que Gobierno instituciones de reportes crediticios y empresas que recaban información sin fines de lucro están exentas de su cumplimiento. Por otra parte, el cumplimiento es obligatorio para personas y empresas que residan en territorio mexicano independientemente del lugar en que resida la persona objeto de la información, lo que implica que las compañías de internet residentes en México deben de cumplir con la regulación aún si sus clientes no son mexicanos, sin embargo empresas de internet extranjeras no están obligadas a cumplir con los estatus de la ley para sus clientes Mexicanos.

El modelo de esta ley incluye el uso de definiciones generales, permitiendo control sobre la obtención, uso, incluyendo acceso, administración, transferencia o eliminación, publicación o almacenamiento de información personal a través de cualquier medio perteneciente a un individuo que pueda ser identificable, prohibiendo por defecto todo tipo de procesamiento sin el consentimiento del mismo.

ISSN-2410-4000

Respecto a la información existente en fuentes públicas, la ley es mucho más permisiva que la existente en la Unión Europea al permitir, el uso de esta información sin ningún tipo de notificación o justificación expresa.

Los principios generales de esta ley siguen la inspiración de la OCDE delimitando los siguientes:

- Notificación: Toda persona debe ser notificada cuando se están recabando sus datos personales

- Propósito: En la notificación se debe dará viso del propósito para el que serán recabados sus datos y los mismo únicamente deberán ser usados para el mismo.

- Consentimiento: Los datos personales no podrán ser publicados sin el consentimiento explícito del titular

- Seguridad: La información recabada deberá ser resguardada de abusos potenciales

- Transparencia: Los titulares de la información deben ser informados sobre la identidad de la persona que se encarga de recabar los datos.

- Responsabilidad: Los titulares deben de contar con un método para responsabilizar al recolector de los datos personales por cualquier incumplimiento de los principios anteriores

Las notificaciones realizadas por las entidades que recolectan datos personales deben de contener los siguientes puntos [2]:

- Identidad y dirección de la entidad que recolecta los datos

- El propósito para el cual serán recabados los datos personales

- Las opciones y métodos disponibles por la entidad recolectora para limitar la divulgación y uso de la información recolectada

- Los mecanismos que pueden utilizar los titulares de la información para solicitar acceso, corrección, cancelación y oposición al procedimiento de acuerdo a lo establecido en la ley

- El procedimiento a través del cual la entidad recolectora comunicará a los titulares sobre algún cambio en las disposiciones

Ley de protección de datos personales

Principios de Protección de Datos Personales, Derechos ARCO y su ejercicio [3].

De los Principios de Protección de Datos Personales

La ley está basada en principios internacionalmente reconocidos desde hace muchos años en el ámbito de la privacidad y la protección de datos personales. Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

Algunos puntos importantes en relación a la adopción obligatoria de estos principios son los siguientes [4]:

- Los datos personales deberán recabarse y tratarse de manera lícita.

La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos-

En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad.

- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la Ley.

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

- Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

- El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos.

Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones previstas en la ley.

Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.
- El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades previstas en el aviso de privacidad.

El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.

- El responsable velará por el cumplimiento de los principios de protección de datos personales establecidos por la Ley, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable.
- El responsable tendrá la obligación de informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través del aviso de privacidad.

El multicitado “aviso de privacidad”, que es documento clave sobre el cual gira buena parte de las “responsabilidades” de esta ley, debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología.

ISSN-2410-4000

Dicho aviso debe contener al menos la siguiente información:

- La identidad y domicilio del responsable que los recaba; Las finalidades del tratamiento de datos;
- Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
- Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en la Ley;

En su caso, las transferencias de datos que se efectúen; procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en la Ley; y En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Dentro del "catálogo" de obligaciones que marca esta ley, sin duda una de las más importantes es la que establece el artículo 19: "Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado."

La parte más importante de esta obligación de seguridad no termina ahí, pues a su vez el artículo 20 [4] establece que: Las vulneraciones de seguridad ocurridas en cualquier fase del tratamiento que afecten de forma significativa los derechos patrimoniales o morales de los titulares, serán informadas de forma inmediata por el responsable al titular, a fin de que este último pueda tomar las medidas correspondientes a la defensa de sus derechos.

Al final de este capítulo se determina una obligación genérica de confidencialidad de la información, concretamente en el artículo 21:

El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de estos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable.

Ley y privacidad de datos opiniones

La presencia del IFAI en todas estas ciudades tiene como objetivo difundir el ejercicio del derecho a la protección de datos personales en sus dos vertientes: la primera, desde la perspectiva de los titulares, como una garantía fundamental, y la segunda, desde el punto de vista de los responsables, en cuanto al cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de los particulares.

De acuerdo con el Instituto, la intención es generar conciencia entre los titulares y responsables sobre la importancia y el impacto del valor cuantitativo y cualitativo de los datos personales dentro de un contexto global y digital, y sensibilizar a la población sobre la responsabilidad que implica compartir los datos personales con terceros, entre otros objetivos.

También se pretende difundir las herramientas que ha desarrollado el Instituto para facilitar a los responsables el cumplimiento de sus obligaciones y a los titulares la promoción de los procedimientos, y dar a conocer las sanciones impuestas en sectores estratégicos.

ISSN-2410-4000

En cuanto a dichas herramientas, el IFAI pone a disposición de todos los responsables el Generador de Avisos de Privacidad (GAP), para que en forma gratuita elaboren su aviso de privacidad.

Según el estudio Termómetro: De la Privacidad de datos, realizado por la empresa Deloitte México, a pesar de la entrada en vigor de la Ley de Protección de Datos Personales en Protección de los Particulares, los lineamientos de regulación y protección de datos en México, así como la cultura de privacidad es rudimentaria. [5]

El análisis reúne la opinión de ejecutivos de la industria mexicana, arroja que 74% de los encuestados conoce la ley aunque sea de manera parcial. Sin embargo, 54% de los empleados no tienen el conocimiento de la responsabilidad que deben cumplir en el proceso.

De igual manera el reporte dio a conocer que el 77% de los entrevistados tiene como objetivo principal incrementar o ganarse la confianza de los clientes, seguido por el aseguramiento del cumplimiento regulatorio con 74%.

Esto hace evidente que más allá del cumplimiento, las empresas buscan mantener o incrementar la confianza y la lealtad de los clientes; lo que cobrará mayor relevancia conforme a la cultura de protección de datos en el país se vaya fortaleciendo", dijo Eduardo Cocina, socio de riesgos de tecnología de la información de Deloitte México.

Por otra parte, el estudio reveló que el principal riesgo que las organizaciones enfrentan ante el mal uso de la información personal es la pérdida que se da vía dispositivos móviles o de memoria.

Para que las empresas puedan llevar a cabo una correcta adopción de la ley, resulta prioritario implementar una serie de acciones que contemplan, de inicio, el desarrollo de un modelo de privacidad aplicado a la realidad de la organización; asignar roles y responsabilidades para el manejo de la información; establecer mecanismos de medición y aseguramiento y, finalmente, exhibir los resultados obtenidos ante las audiencias involucradas.

Las empresas mexicanas han identificado ser vulnerables y necesitan hacer ciertos cambios en su forma de proteger y tratar la información", dijo el especialista.

De acuerdo con el estudio de Deloitte, más de la mitad de los entrevistados aseguró que su organización sí cuenta con los recursos internos necesarios para cumplir con la ley.

Consideran que los procesos y las prácticas internas, políticas y estándares, así como el conocimiento y la cantidad de gente son los factores claves para poder llegar al cumplimiento que establece la ley.

Mientras más sensibles estén las compañías ante la relevancia de los procesos y avancen en su autoanálisis, podrán determinar el nivel de esfuerzo requerido y comenzar a actuar para obtener diversos beneficios.

La protección de datos personales se remonta a 1948, cuando la Asamblea General de las Naciones Unidas adopta el documento conocido como Declaración Universal de Derechos Humanos, en este documento se expresan los derechos humanos conocidos como básicos. En el artículo 12 se señala lo siguiente:

ISSN-2410-4000

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Actualmente, una gran cantidad de datos personales, incluyendo aquellos conocidos como datos biométricos, son almacenados en sistemas computacionales, factor que los hace susceptibles de sufrir ataques informáticos.

En varios países del mundo hay esfuerzos por crear legislaciones que establezcan los límites, permisos y castigos entorno al manejo adecuado de los datos contenidos en los sistemas de información, sobre todo de aquellos definidos como datos personales. Esta investigación busca un precedente legal de cómo son considerados los datos biométricos por las leyes de protección de datos personales de distintos países en el mundo.

A continuación, se describen algunos conceptos relevantes en este tema:

Dato personal. Se refiere a toda aquella información asociada a una persona o individuo que lo hace identificable del resto de las personas y/o como parte de un grupo determinado de individuos, por ejemplo: nombre, domicilio, teléfono, fotografía, huellas dactilares, sexo, nacionalidad, edad, lugar de nacimiento, raza, filiación, preferencias políticas, fecha de nacimiento, imagen del iris del ojo, patrón de la voz, etc.

La idea central de este concepto es común en las legislaciones de protección de datos que distintos países han redactado.

Datos personales sensibles. Comúnmente se refiere a todos aquellos datos que se relacionan con el nivel más íntimo de su titular y cuya divulgación pueda ser causa de discriminación o generar un severo riesgo para su titular. De manera general, se consideran datos sensibles aquellos que revelen características como origen étnico o racial, estado de salud, creencias religiosas, opiniones políticas, preferencia sexual, pertenencia a sindicatos, creencias filosóficas y morales, entre otras. Esta clase de información debe ser tratada con mayor responsabilidad y establecer medidas de protección más estrictas.

Datos biométricos. Por definición común, los datos biométricos son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población. Aquellos sistemas informáticos en los que se mide algún dato biométrico, como parte del proceso de identificación y/o autentificación de un sujeto, son conocidos como sistemas de seguridad biométrica o simplemente sistemas biométricos. [6]
La siguiente lista son algunos ejemplos de datos biométricos:

- Huellas dactilares
- Geometría de la mano
- Análisis del iris
- Análisis de retina
- Venas del dorso de la mano
- Rasgos faciales
- Patrón de voz
- Firma manuscrita

ISSN-2410-4000

- Dinámica de tecleo
- Cadencia del paso al caminar
- Análisis gestual
- Análisis del ADN

Leyes de protección de datos en el mundo

En el mundo existen dos vertientes principales entorno a la protección de los datos personales: El modelo europeo busca proteger la información y la propiedad de la misma, en aras de conservar la honorabilidad de la persona aun cuando ésta hubiese fallecido, la motivación de este modelo tiene base en los derechos humanos de los individuos. El modelo estadounidense pretende proteger la información de las personas con el concepto de derecho a la privacidad, el cual puede extinguirse con la muerte del sujeto, el modelo surge derivado de motivos comerciales ya que las empresas utilizaban de manera indiscriminada esa información.

Diversos países han promulgado leyes de protección de datos personales y en cada país se ha buscado adaptar, a sus propias condiciones culturales, económicas y políticas, las bases de alguno de los dos modelos de protección de datos personales existentes.

A continuación, se mencionan algunos casos relevantes sobre las leyes de protección de datos personales de distintos países, organizaciones y regiones del mundo:

1. **Organización de Naciones Unidas (ONU)**. En 1948, adopta el documento conocido como Declaración Universal de Derechos Humanos, en la que el artículo 12 señala que las personas tienen derecho a la protección de la ley de sus datos personales.

2. **Alemania**. En 1970 fue aprobada la primera ley de protección de datos (Datenschutz). En 1977, el Parlamento Federal Alemán aprueba la Ley Federal Bundesdatenschutzgesetz. Estas leyes impiden la transmisión de cualquier dato personal sin la autorización de la persona interesada.

3. **Suecia**. En 1973 fue publicada la que fue una de las primeras leyes de protección de datos en el mundo.

4. **Estados Unidos de Norteamérica**. La protección de datos tiene base en la Privacy Act de 1974.

5. **Unión Europea**. El primer convenio internacional de protección de datos fue firmado en 1981 por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocido como "Convenio 108" o "Convenio de Estrasburgo". En los 90's, se establece una norma común que se denominó Directiva 95/46/CE. La directiva es referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

6. **España**. La ley Orgánica 15 de 1999, establece la Protección de Datos de Carácter Personal. Está ley ha sido importante para Latinoamérica porque se ha utilizado como firme referente del modelo europeo.

7. **Latinoamérica**. En América Latina, las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las tecnologías de la información y el aumento de las vulnerabilidades asociadas. En su mayoría, estas leyes se asemejan al modelo europeo: En Argentina la Ley 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), Uruguay (2008).

8. **Rusia**. En el año 2006 fue aprobada una exhaustiva ley de protección de datos personales.

9. **Perú**. La ley 29.733 del 2 de julio de 2011 es la más reciente ley de protección de datos personales en el mundo.

10. **México**. La Ley Federal de Protección de Datos Personales en Posesión de Particulares fue publicada en el Diario Oficial de la Federación el 5 de julio de 2010, entró en vigor un día después y tiene efecto a partir de enero del año 2012.

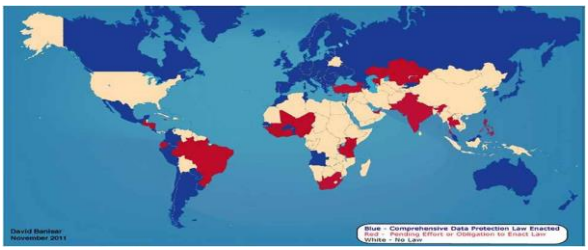
Esta ley pretende salvaguardar el respeto a la privacidad, dignidad e información de las personas, en ella se establecen cuatro derechos fundamentales que tienen los individuos sobre su información en posesión de cualquier persona física o empresa particular (aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades, etc.), son los denominados derechos ARCO: Acceso, Rectificación, Corrección y Oposición.

La ley también indica que los particulares deberán avisar, a cada persona de la que obtengan información personal, sobre el tratamiento que planean dar a sus datos. Lo anterior se debe hacer mediante un aviso de privacidad, el cual deberá ser respetado por el particular, y cada persona notificada tendrá la libertad de otorgar o no su consentimiento respecto al procesamiento de su información.

Mapa de protección de datos personales

Se ha publicado un mapa con las leyes de protección de datos personales aplicadas en el mundo

La clasificación parece evaluar únicamente el modelo europeo de protección de datos personales, ya que no incluye a los Estados Unidos como parte de los países con legislación sobre protección de datos personales [5].



Finalmente, tras dos meses de espera, ha sido publicada en el Diario Oficial de la Federación, la Ley federal de protección de datos en posesión de particulares. En México sólo existía protección de datos, para aquella información personal que aparecía en los archivos estatales o de la Administración, a través de la Ley federal de transparencia y acceso a la información.

Con la nueva ley, las empresas privadas tendrán un periodo de un año para nombrar al encargado del tratamiento de los datos.

Asimismo, también se estipuló el plazo de un año para la emisión del Reglamento de la ley, que contendrá las disposiciones específicas. Esperamos que éste, tenga las características del RD 1720/2007 de España, con las medidas de seguridad de los ficheros que contengan datos personales.

La ley, por supuesto, contempla las figuras de encargado, responsable y tercero; así como el concepto de datos sensibles, que tendrán que tener un tratamiento especial.

ISSN-2410-4000

En posteriores entregas, hablaremos más ampliamente de esta ley, de sus aspectos positivos y de aquellos que son susceptibles de mejora.

Es difícil dar una definición de la "privacidad" puesto que es un asunto subjetivo. Por razones personales, algunas personas prefieren vivir en sociedad de forma anónima sin que nada interfiera en sus asuntos. Otras no son reacias a dar a conocer sus detalles personales a cambio de poder acceder a información, bienes o servicios. Para la mayoría, la privacidad constituye un simple asunto de seguridad.

Las personas muestran preferencia por acceder a servicios sin tener que rellenar complicados formularios ni someterse a comprobaciones de referencia. Para ello, pueden mostrarse de acuerdo en permitir que los sistemas de información rastreen sus movimientos y sus compras

La seguridad está íntimamente ligada a la privacidad. Los sistemas de información seguros nunca deben revelar datos de manera inapropiada. No podemos afirmar que la revelación de cualquier información sea un acto sin segundas intenciones. La información es recopilada y procesada siempre con un propósito determinado.

La intención de quienes recogen información personal o hacen negocio con ella y la almacenan en una base de datos es la de crear perfiles individuales con un objetivo concreto. Los modos en que los datos personales son revelados, usados y almacenados nos ayudarán a determinar si las tecnologías de la información están siendo utilizadas para el empoderamiento o para la represión.

Al considerar las formas de medir la privacidad y la seguridad, debemos distinguir entre distintas clases de privacidad:

La privacidad significa para la mayoría "intimidad" o el derecho de la persona a que nada ni nadie interfiera en su hogar, su propiedad o su vida privada. Esta puede ser considerada como una privacidad del "mundo real".

El derecho de las personas a protegerse de las pruebas médicas o genéticas constituye la base de su intimidad corporal; también comprende el derecho a que la información sobre su salud y bienestar personal sea protegida por el personal que tiene acceso a ella (médicos, empleadores, aseguradoras, etc.).

La "privacidad en las comunicaciones" se refiere a la protección contra la interferencia de las comunicaciones telefónicas o de Internet. El respeto a la privacidad en las comunicaciones constituye un requisito indispensable para el mantenimiento de las relaciones humanas por medios de comunicación tecnológica.

La "confidencialidad de la información" es probablemente el aspecto más debatido en el uso de las computadoras y los sistemas de información.

Los sistemas de información tienen la capacidad de almacenar y procesar con rapidez los datos de un gran número de personas.

Es importante garantizar que dicha información será utilizada únicamente para los fines con que fue recogida y que ésta no será revelada a terceros sin el consentimiento de los interesados.

ISSN-2410-4000

Amenazas a la privacidad en la Web

Al navegar por la Web no somos completamente anónimos; existen varias maneras de recoger información sobre los usuarios o sus actividades sin contar con su consentimiento [7]: Cookies (mini archivo de identificación de usuario de páginas Web) HTTP Navegadores. Es probable que ya exista información sobre su persona publicada en la Web. Descarga de software libre y de uso compartido Motores de búsqueda Comercio electrónico Correo electrónico Correo electrónico y criptografía Correo basura (Spam) Peligros en el Chat IRC.

En México, el derecho fundamental a la protección de datos personales está garantizado por la Constitución (artículo 16) y la correspondiente Ley de desarrollo, denominada de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) y su reglamento. La primera aparece en 2010 y a finales del año pasado, la norma reglamentaria. Así, este derecho humano se convierte en fundamental desde su inclusión en la carta magna y, entre otros aspectos, implica garantías derivadas de éste como los preceptos acerca de los derechos de acceso, rectificación, cancelación u oposición (derechos Arco) al tratamiento de los datos personales. Como particulares, como individuos, como titulares de esos datos personales, pero sobre todo como sujetos de derechos fundamentales, es necesario y cuasi obligatorio informarse sobre la manera en que está protegido el que estamos analizando, pero también la forma en que podemos llevar a efecto su auténtico ejercicio.

Es el Instituto Federal de Acceso a la Información y Protección de Datos el órgano garante.

Esto es, la institución a la cual podemos acudir para conocer los dos aspectos antes mencionados y también la que nos apoyará en caso de ver vulnerados nuestros derechos. Por otro lado, y como contraparte, el órgano regulador de cara al sector empresarial es la Secretaría de Economía, la cual tiene atribuciones en la materia para crear conciencia entre las organizaciones sobre sus obligaciones en cuanto a la protección de datos personales (entre las que destacan la puesta a disposición de sus usuarios o clientes del aviso de privacidad –en donde deben señalarse las categorías de datos personales que se recopilarán, así como el objetivo para el cual serán tratados y la duración de dicho tratamiento– y el nombramiento de un encargado de las bases de datos personales –que dependiendo del tamaño de las empresas puede ser una persona o un departamento-) y fomentar la cultura de adopción de esquemas de autorregulación vinculante, tal y como dispone la normativa mencionada.

La adopción de medidas de autorregulación, que se compone de inclusión de códigos éticos que, por parte de las empresas, complementen las medidas para cumplir con la legislación, disminuyan las brechas o agujeros de seguridad y, asimismo, reduzcan los montos de las sanciones a las que una persona física o jurídica puede hacerse acreedora por la inobservancia de las disposiciones de la LFPDPPP y su reglamento, como por cualquier ataque a sus bases de datos personales, que además de hacerle acreedor a dicha penalidad, pueden suponer un enorme riesgo en la pérdida de información de gran valor (teniendo en consideración que los datos personales son uno de los principales activos de las empresas), así como un enorme desprestigio, falta de fidelidad de los clientes, o incluso finalización de contrataciones con los mismos.

ISSN-2410-4000

Ahora bien, uno de los aspectos que debe tomarse en consideración con relación en el tratamiento de bases de datos personales que hacen prácticamente todas las empresas (la Ley obliga a la totalidad de las mismas siempre que tengan en su haber esos datos y los utilicen para fines de difusión y/o comercialización), es el uso de Tecnologías de la Información y la Comunicación (TIC) en dicho tratamiento. Son muchos los retos a los que se enfrentan tanto las empresas como las personas en cuanto al uso de la tecnología, e incluso las propias TIC son la razón por la cual en diversos países inició la preocupación por regular estos aspectos. Esto es, la tecnología que cada vez más proliferaba en los años ochenta y que supuso inclusive que se desarrollaran muchos análisis teóricos para analizar los fenómenos que planteaba ésta, desde el punto de vista sociológico o comunicacional, también supuso estudios y enmiendas en el plano jurídico, toda vez que se consideraba el potencial que podría tener de vulnerar las esferas de derechos humanos ya protegidos, como el de la intimidad y el del honor y la propia imagen.

Los instrumentos internacionales que destacan en este sentido, aun cuando el auge de las TIC apenas o incluso no iniciaba, son la Declaración Universal de los Derechos Humanos de 1948 y el Pacto Internacional de los Derechos Civiles y Políticos de 1966. En diversos países europeos se inició el debate en torno a los derechos ahí establecidos, pero con la consecuente agravante que podría suponer la tecnología. Alemania, por ejemplo, es uno de los primeros países en brindar protección a los derechos vinculados con la privacidad. En España, tempranamente inician también esos desarrollos legales, de tal forma que ya en su Constitución de 1978 se establecía un derecho a la intimidad personal y familiar y se estipulaba que la Ley limitaría el uso de la informática para protegerla.

Esto es, una alusión clara a los inicios del desarrollo de las TIC, que parten de la mencionada informática, pero que luego entraron en convergencia con los sectores de telecomunicaciones y audiovisual.

Es por todo esto que las legislaciones en materia de privacidad y protección de datos personales han considerado desde sus inicios, pero lo hacen con mucho más énfasis y frecuencia en la actualidad, las implicaciones de la tecnología en la intimidad de las personas. Por ejemplo, en el Reglamento de la LFPDPPP de México ya se considera el tema del cómputo en la nube (cloudcomputing), por ser una de las posibles amenazas en el manejo de los datos de personas titulares de derechos fundamentales.

Como se dijo, además de las medidas que la legislación impulsa, se tiene la posibilidad de adoptar medidas adicionales de seguridad y códigos de conducta y éticos, que aúnen las mejores prácticas, con el fin de proteger las bases de datos personales por varios motivos. Uno de ellos es la integridad de dichas bases, finalmente, por la importancia que tienen para la organización. Una de las más importantes es que se evitan penalizaciones derivadas del incumplimiento legal, toda vez que el régimen de sanciones de la LFPDPPP es sumamente fuerte.

Entre las medidas adicionales de seguridad y los esquemas de autorregulación vinculante se encuentran aquellas relacionadas con el uso de la tecnología para combatir la tecnología.

Es decir, si las TIC pueden ser potencialmente vulneradoras de la privacidad y los datos personales, con otras TIC este proceso se puede combatir, revertir o minimizar.

ISSN-2410-4000

"Ése es el caso de las PET (Privacy Enhancing Techonologies) en las que ya se trabaja en distintos países y que, por nuestra parte, ya estamos diseñando, con un fundamento teórico y doctrinal, en Infotec."[8]

Conclusiones

La protección de los datos personales son un importante avance para la ejercer nuestro derecho en cuanto al uso de ellos, en mi opinión personal y por experiencia propia muchas veces me hablaban y no sabía cómo es que estos datos llegan a ellos, creo que es muy importante debido a que es un tema muy delicado pues al no tener un control sobre nuestros datos cualquier empresa o persona tenia uso de ellos.

Creo que México dio un gran paso en cuanto al derecho que tenemos los ciudadanos para cuidar nuestros datos creo que lo único que falta es el fortalecimiento de las instituciones para poner multas más fuertes a las organizaciones o empresas que hagan un mal uso de nuestros datos un ejemplo la multa para BANAMEX se me hace poco comparado al tamaño de la empresa, debería de ver leyes que sean más fuertes que castiguen a este tipo de organizaciones.

Referencias

[1] J. T. Eustice y M. A. Bohri, «NAVIGATING THE GAUNTLET: A SURVEY OF DATA PRIVACY LAWS IN THREE KEY LATIN AMERICAN COUNTRIES,» Sedona Conference Journal, pp. 137-153, 2013.

[2] L. Determann y S. Legorreta, «New Data Privacy Law in Mexico.,» Computer & Internet Lawyer. , pp. 8-11, 2010.

[3] F. Solares Valdes, «Ley Federal de Protección de Datos Personales,» de Ley Federal de Protección de Datos Personales, Distrito Federal.

[4] Cámara de Diputados, «Ley Federal de Protección de Datos Personales en Posesión de los Particulares,» Diario Oficial de la Federación, Distrito Federal, 2010.

[5] b:Secure, «México aún no está preparado para la ley de protección de datos: Deloitte,» 15 Febrero 2012. [En línea]. Available: http://www.bsecure.com.mx/featured/mexico-aun-no-esta-preparado-para-la-proteccion-de-datos/.

[6] UNAM, «Leyes de protección de datos personales en el mundo y la protección de datos biométricos,» [En línea]. Available: http://revista.seguridad.unam.mx/numero-13/leyes-de-protecci%C3%B3n-de-datos-personales-en-el-mundo-y-la-protecci%C3%B3n-de-datos-biom%C3%A9tricos-%E2%80%93.

[7] Asociación para el progreso de las comunicaciones, «Aspectos específicos relativos a las políticas sobre internet y su regulación,» [En línea]. Available: http://derechos.apc.org/handbook/ICT_21.shtml.