

La Protección de los Datos Personales.



El próximo sábado 28 de Enero, se celebrará el Día Internacional de Protección de Datos Personales, que en este año conmemora su sexta edición.

Comenzando como una iniciativa del Consejo de Europa, por medio de la cual se ha invitado a las autoridades de distintos países alrededor del mundo, para generar un espacio de reflexión y promoción entre su población acerca de la importancia que tiene para cualquier individuo, el adecuado uso, obtención y transmisión de su información personal.

Prácticamente cualquier actividad humana requiere el tratamiento de la información personal. Todos los días de manera cotidiana y en actividades diversas, las personas transmiten o intercambian alguno de sus datos personales, ya sea para adquirir un bien o servicio en un establecimiento comercial, realizar un trámite ante alguna autoridad, o bien al acceder a Internet.

A partir de la aparición y desarrollo de las Tecnologías de la Información que permiten la recolección y transmisión de grandes bases de datos e información, la protección de los datos personales ha cobrado mayor relevancia, ya que si bien estas innovaciones ofrecen grandes ventajas en términos de eficiencia y productividad, por otra parte, permiten el almacenamiento masivo de información que concierne a los individuos y la formación de perfiles que pueden emplearse inadecuadamente para injerencias arbitrarias o ilegales a la vida privada.

¿Qué son los datos personales?

Los datos personales se refieren a toda aquella información relativa al individuo que lo identifica o lo hace identificable. Entre otras cosas, le dan identidad, lo describen, precisan su origen, edad, lugar de residencia, trayectoria académica, laboral o profesional.

Además de ello, los datos personales también describen aspectos más sensibles o delicados sobre tal individuo, como es el caso de su forma de pensar, estado de salud, sus características físicas, ideología o vida sexual, entre otros.

¿Para qué sirven los datos personales?

Los datos personales son necesarios para que un individuo pueda interactuar con otros o con una o más organizaciones sin que sea confundido con el resto de la colectividad y para que pueda cumplir con lo que disponen las leyes. Asimismo, hacen posible la oferta y obtención de bienes y servicios.

Sin embargo, el uso extensivo de las tecnologías de la información y las telecomunicaciones ha permitido que en muchas ocasiones, los datos personales sean tratados para fines distintos para los que originalmente fueron recabados, rebasando los límites de la esfera de privacidad de la persona, y lesionando en ocasiones otros derechos y libertades.

¿Por qué proteger los datos personales?

A fin de equilibrar las fuerzas entre un individuo y aquellas organizaciones –públicas o privadas– que recaban o colectan datos sobre tal individuo, surge en Europa el concepto de la protección de datos personales. Un concepto similar surgió en los Estados Unidos de América --el concepto de “privacidad”-- aunque con alcances distintos.

Bajo el concepto de protección de datos personales, el titular (o dueño) de dichos datos es el propio individuo. En naciones avanzadas, la protección de datos personales es quizá el más nuevo de los derechos que goza un ciudadano.

Se han plasmado un conjunto de principios y derechos derivados de la protección de datos personales con los que es posible precisar qué implica tanto para el titular como para la organización que recaba o colecta datos personales.

¿Qué conmemoramos el 28 de enero?

El 26 de abril del 2006 el Comité de Ministros del Consejo de Europa resolvió declarar el 28 de enero como el “Día de la protección de los Datos Personales” con motivo del aniversario de la firma del Convenio 108 sobre la protección de los datos personales.

¿Qué es el Convenio 108?

El Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, suscrito en 1981, es el primer instrumento vinculativo de carácter internacional en materia de protección de datos y es el resultado de la decisión del Consejo de Europa, ante el rápido avance en el campo del procesamiento electrónico de información y la aparición de las primeras bases de datos usadas por las grandes empresas y los gobiernos estatales, de otorgarle un marco legal con principios y normas concretos para prevenir la recolección y el tratamiento ilegal de datos personales.

Por medio del Convenio 108 los países firmantes se comprometen a realizar las reformas necesarias en su legislación nacional para implementar los principios contenidos en dicho instrumento; los cuales se refieren, en primer lugar, a que los datos personales deben recolectarse y tratarse con fines legítimos y no para otros propósitos distintos, que no deben conservarse más de lo estrictamente necesario; de acuerdo con el fin para el cual fueron recolectados, que sean verdaderos y que no sean excesivos.

Asimismo prevé que deberá garantizarse la confidencialidad de los datos sensibles y reconoce el derecho de los individuos para tener acceso y en su caso solicitar la corrección de sus datos.

¿Existe en México el derecho a la protección de datos personales?

En México, desde el año 2000, se han promovido diversos proyectos legislativos en torno a la protección de datos personales en el Congreso de la Unión, sin que ninguno de ellos fructificara dada la ausencia de una disposición constitucional que les diera sustento. Si bien la reciente reforma constitucional en 2007 al artículo 6º establece en sus fracciones II y III que los datos personales y la información relativa a la vida privada será protegida, así como el derecho de acceder y corregir sus datos que obren en archivos públicos, el legislador quiso establecer límites al ejercicio del derecho de acceso a la información pública en los tres órdenes de gobierno (federal, estatal y municipal), pero no creó un derecho fundamental independiente.

No es sino hasta la aprobación en 2008 de las reformas a los artículos 16 y 73 constitucionales que se introduce al más alto nivel de nuestra Constitución, el derecho de toda persona a la protección de su información. Lo anterior es relevante dado que los datos personales se encuentran en manos tanto de gobiernos como de particulares (empresas, organizaciones y profesionistas) y, porque con el uso indiscriminado de la tecnología, éstos pueden utilizarse para fines distintos de aquellos para los que fueron recabados, pudiendo causar afectaciones en las esferas de otros derechos de los titulares de dichos datos.

¿Qué logra la reforma al artículo 16?

El artículo 16 constitucional reconoce y da contenido al derecho a la protección de datos personales. En ese sentido, en la reforma se plasman los derechos con los que cuentan los titulares de los datos como lo son aquellos de acceso, rectificación, cancelación y oposición (denominados por su acrónimo como derechos ARCO).

Por otra parte, se hace referencia a la existencia de principios a los que se debe sujetar todo tratamiento de datos personales, así como los supuestos en los que excepcionalmente dejarían de aplicarse dichos principios.

La reforma consistió en añadir un segundo párrafo que a la letra dice:

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

El proyecto fue aprobado por el pleno del Senado en sesión del 4 de diciembre de 2008 y por el de la Cámara de Diputados el 11 de diciembre. Se envió a las legislaturas locales para continuar el trámite de aprobación a reformas constitucionales y actualmente se cuenta con el voto aprobatorio de Chiapas y Aguascalientes.

¿Qué aporta la reforma al artículo 73?

Por virtud de las leyes de transparencia y acceso a la información gubernamental, únicamente los sujetos obligados de las mismas en todo el país, están obligados a proteger la información personal que poseen en sus archivos. Sin embargo, dado que los particulares también tratan grandes cúmulos de información, resultaba indispensable dotar de facultades expresas al Congreso Federal para que regulara a escala nacional, la forma en que los particulares (bancos,

hospitales, universidades, profesionistas, entre otros) pueden utilizar y transmitir la información relativa a las personas.

Por lo anterior, la reforma al artículo 73 consistió en añadir la fracción

“O” que a la letra dice:

“Artículo 73. El Congreso tiene facultad:

I. a XXIX-N. ...

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

XXX. ...”

Al igual que con la Reforma al artículo 16, queda pendiente la aprobación por parte de las legislaturas locales de la reforma aprobada al artículo 73. A la fecha, únicamente se tiene registrada la aprobación por parte de Chiapas.

El consentimiento.

A diferencia de algunos países europeos, la nueva legislación mexicana no obliga a que las empresas registren sus bases ante la autoridad, de manera que cualquier privado puede recopilar datos personales sin una firma del titular de los mismos, siempre y cuando avise para qué lo utilizará. Este esquema es conocido como Opt-out.

El aviso de privacidad debe explicar lo que se hará con la información y manifestar quién es el responsable, así como dar a conocer los derechos de acceso, rectificación o cancelación.

Según el artículo 8 de la ley recién aprobada, se entenderá que el “titular de los datos consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición. Sin embargo, este consentimiento podrá ser revocado en cualquier momento, sin que se le atribuyan efectos retroactivos”.

El IFAI, como ente garante.

Las primeras iniciativas proponían crear un nuevo organismo, pero esto resultaría muy caro y se consideró que el Instituto Federal de Acceso a la Información Pública (IFAI) tiene las condiciones para ser la institución garante de la protección de datos.

Aunque hasta ahora sus regulados han sido dependencias gubernamentales, el tipo de datos es el mismo, y ya se les otorga acceso a los ciudadanos para corregir sus datos personales.

Con este cambio, el nuevo nombre de la institución será Instituto Federal de Acceso a la Información y Protección de Datos y recibirá los recursos humanos, financieros y materiales estrictamente necesarios para adecuar las estructuras a las nuevas atribuciones.

Para la Comisión Dictaminadora de esta ley, es una ventaja que el IFAI sea la responsable porque habrá unicidad de criterios y se evitarán conflictos potenciales al decidir qué información es pública y cuál está protegida como dato personal. Esta problemática ha sido común en países donde dos instituciones diferentes se encargan de tales asuntos.

Por otra parte, el IFAI ya tiene un cúmulo de conocimiento y especialización en materia de datos personales, incluida la implementación de regulación secundaria –lineamientos y recomendaciones–, solución de controversias para la protección de derechos de acceso y rectificación, así como los que sobrevendrían de cancelación y oposición, supervisión del cumplimiento regulatorio –verificaciones–, promoción de la cultura y capacitación en la sociedad.

Las sanciones.

La ley prevé sanciones que van desde el apercibimiento, que es el equivalente a una llamada de atención, hasta la imposición de multas desde 100 hasta 320 mil días de salario mínimo vigente en el Distrito Federal, que equivalen a más de 18 millones de pesos. Además, según la gravedad del delito, podrían existir responsabilidades civiles y penales.

En la nueva legislación, los delitos están tipificados en tres artículos:

Artículo 67. Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Artículo 68. Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Artículo 69. Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Procedimientos.

Para la protección de derechos: El artículo 45 explica lo que procederá si una persona está inconforme con el tratamiento a sus datos para su rectificación, cancelación u oposición. En este caso, el titular o su representante legal deberán presentar su solicitud de protección de datos ante el IFAI dentro de los 15 días siguientes a la fecha en que se le comunique una respuesta por parte del responsable, o que haya vencido el plazo previsto si es que el responsable respondió.

Recibida la solicitud de protección de datos ante el Instituto, se dará traslado de la misma al responsable, para que, en un plazo de quince días, emita respuesta, ofrezca las pruebas que estime pertinentes y manifieste por escrito lo que a su derecho convenga.

El Instituto admitirá las pruebas que estime pertinentes y procederá a su desahogo. Concluido el desahogo de pruebas, el Instituto notificará al responsable el derecho que le asiste para que, de considerarlo necesario, presente sus alegatos dentro de los cinco días siguientes a su notificación. El IFAI resolverá sobre la solicitud de protección de datos formulada, una vez analizadas las pruebas y demás elementos de convicción que estime pertinentes, como pueden serlo aquéllos que deriven de la o las audiencias que se celebren con las partes.

De verificación: El Artículo 59 indica que el IFAI podrá dar inicio a una verificación de oficio o a petición de parte. La de oficio procederá cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos o se presuma fundada y motivadamente la existencia de violaciones a la Ley.

En el artículo 60 se establece que durante el procedimiento de verificación, el IFAI tendrá acceso a la información y documentación que considere necesarias, de acuerdo con la resolución que lo motive.

Los servidores públicos federales estarán obligados a guardar confidencialidad sobre la información que conozcan derivada de la verificación correspondiente.

De la imposición de sanciones: Los artículos 61 y 62 señalan que si se descubre el incumplimiento de algunos de los principios o disposiciones de la Ley, el IFAI notificará al infractor para que en un plazo de 15 días presente pruebas y manifieste por escrito lo que a su derecho convenga. A partir

de ahí comenzará un proceso de desahogo de pruebas hasta llegar a una resolución. Sin embargo, el detalle de todo este procedimiento se reflejará en el reglamento de operación.

Glosario de Protección de Datos Personales.

La Ley de Protección de Datos Personales en Posesión de Particulares define así los conceptos más relevantes a esta ley:

Aviso de Privacidad: Es el documento físico, electrónico o en cualquier otro formato generado por el responsable, que es puesto a disposición del titular previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de esta Ley.

Bases de datos: Se le llama así al conjunto ordenado de datos personales referentes a una persona identificada o identificable.