TÍTULO:	PROTECCIÓN DE DATOS PERSONALES
AUTOR/ES:	Sarchman, José M.
PUBLICACIÓN:	Profesional y Empresaria (D&G)
TOMO/BOLETÍN:	XX
PÁGINA:	-
MES:	Junio
AÑO:	2019
OTROS DATOS:	-

JOSÉ M. SARCHMAN

PROTECCIÓN DE DATOS PERSONALES

La Dirección Nacional de Protección de Datos Personales (DNPDP), es la autoridad de aplicación de la ley 25326 (ley de protección de datos personales). El ámbito de la competencia de la DNPDP surge de la ley citada y de la normativa que la reglamenta, principalmente el decreto 1558/2001. La protección de los datos personales se encuentra garantizada en la República Argentina a través de la acción del Habeas Data, incorporada en la Reforma Constitucional del año 1994, en el artículo 473, tercer párrafo de la mencionada Constitución Nacional. Posteriormente fue sancionada la ley 23526, norma de orden público que regula los principios aplicables en la materia y el procedimiento de la acción de Habeas Data.

Es decir, entonces que el objeto de la ley 25326 es la protección integral de los datos personales, asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados.

En este artículo, trataremos de analizar pormenorizadamente la ley 25326 y al finalizar señalaremos algunas normas ISO sobre el tema.

I - INTRODUCCIÓN

El artículo 1 de la ley 25326 de protección de datos personales señala que la misma tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados, destinados a dar informes para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad con lo establecido en el artículo 43, tercer párrafo, de la Constitución Nacional.

Un dato de carácter personal es toda información referida a personas físicas o de existencia ideal determinadas o determinables.

Las disposiciones de la ley se aplican, en cuanto resulte pertinente, a los datos relativos a las personas de existencia ideal, así como a los datos de las personas físicas.

Mucha gente supone erróneamente que esta ley sirve solo para borrar datos negativos publicados por empresas de informes comerciales (Habeas Data), es decir que solo permite controlar la información contenida en las bases de datos de las entidades financieras y de las empresas que brindan informes comerciales y crediticios. También sirve para acceder, rectificar o suprimir datos personales que se encuentran almacenados en cualquier tipo de archivo, registro, base o banco de datos, ya sea público o privado.

El artículo 1 del decreto 1558/2001 entiende por archivos, registros, bases o bancos de datos privados destinados a brindar informes a aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

El órgano de control es la Dirección Nacional de Protección de Datos Personales, que funciona en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos.

Los archivos, registros, bancos o bases de datos formados por los particulares para su uso exclusivamente personal están exentos del deber de registrarse. Ellos son los que mantienen las personas físicas con fines exclusivamente particulares, como es el caso de las agendas personales o las listas de teléfonos y direcciones, cuya obligación de registro supondría una intromisión ilegítima en su intimidad.

Las fuentes de información periodística se encuentran excluidas del régimen establecido por la ley.

No todos los datos personales requieren una idéntica intensidad protectora. La ley comprende que los datos sensibles a aquellos datos personales que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual, y, como regla general sujeta a excepciones, la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele este tipo de datos, están totalmente prohibidos.

Los requisitos generales que deben cumplir los titulares de archivos, registros, bancos o bases de datos que contengan información relativa a personas para garantizar la veracidad de la información contenida, la congruencia y la racionalidad de la utilización de los mismos, pueden resumirse enumerando los siguientes principios rectores:

- Pertinencia: los datos que se recaben y almacenen deben ser pertinentes y adecuados, es decir, estar relacionados con el fin perseguido en el momento de la creación de la base de datos. En ningún caso se pueden utilizar los datos obtenidos para finalidades diferentes de aquellas para las que se hubieran recogido.

- Finalidad: los datos deben tratarse con un objetivo específico que debe conocerse antes de la creación de la base misma e informarse en el momento en que la información personal es recolectada. Los datos que se obtengan deben tratarse de manera leal y lícita.

- Utilización no abusiva: los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

- Exactitud: los datos deben ser exactos y actualizarse en el caso de que ello fuera necesario. Si fueren inexactos o incompletos, deben ser suprimidos y sustituidos, o en su caso, completados.

- Limitación en el tiempo: los datos deben ser eliminados una vez que se haya cumplido la finalidad para la que fueron recabados.

- Legalidad: el procedimiento de recogida de datos no debe ser realizado en forma ilícita o desleal, no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley.

- Publicidad: los archivos, registros, bases o bancos de datos alcanzados por las disposiciones legales deben inscribirse en el Registro habilitado a tal efecto para permitir que, a través de su consulta, los ciudadanos pueden tomar conocimiento de los archivos en los cuales pueden existir datos referidos a su persona y de la identidad de los responsables de su tratamiento para poder ejercer una defensa adecuada a sus derechos.

- Seguridad: la información personal referida a los ciudadanos debe almacenarse en archivos, registros, bancos o bases de datos que reúnan condiciones técnicas de integridad y seguridad.

- Consentimiento: como regla general, el tratamiento de datos de carácter personal requiere el consentimiento libre, expreso e informado del titular de los datos. Ello, para permitir que cada persona pueda elegir qué datos referidos a su persona pueden ser sujetos a tratamiento. En principio, el consentimiento debe constar por escrito o por medio equiparable que deberá ser establecido por la DNPDP.

II - REQUISITO DE CONSENTIMIENTO PREVIO

El requisito del consentimiento previo cuenta con las siguientes excepciones:

- Cuando los datos se obtienen de fuentes de acceso público irrestricto.

- Cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

- Cuando se trate de listados cuyos datos se limiten a nombre, Documento Nacional de Identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.

- Cuando deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento.

- Cuando se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes, conforme a las disposiciones del artículo 39 de la ley 21526.

III - DERECHOS DE LOS CIUDADANOS

La ley reconoce a los ciudadanos el derecho de oposición, información, acceso, rectificación, cancelación, supresión, tutela, impugnación de valoraciones y consulta.

Derecho de oposición

El derecho de oposición es el derecho que le permite al titular de los datos personales negarse a facilitar un dato de carácter personal en el caso de que no sea obligatorio hacerlo, especialmente si se trata de datos sensibles.

Derecho de información

El derecho de información, en cambio, es el derecho básico del afectado para poder ejercitar, con ciertas garantías, los controles que la ley articula en los diversos momentos del tratamiento de los datos. Consiste en la posibilidad que tiene una persona a la que le solicitan datos de carácter personal a ser previamente informada de modo expreso, preciso e inequívoco de las siguientes circunstancias:

- La finalidad para la que serán tratados sus datos personales y quiénes pueden ser sus destinatarios o clase de destinatarios.

- La existencia del archivo, registro, banco o base de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.

- El carácter obligatorio o facultativo de las respuestas al cuestionario que se proponga.

- Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos.

- La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

- Esta información deberá aparecer en todos los formularios que se utilicen para recoger datos de carácter personal.

Derecho de acceso

El derecho de acceso se entiende como la garantía de comprobación de que las informaciones que versen sobre las personas son veraces, actualizadas y delimitadas al fin para el cual fueron registradas; este derecho es la médula de lo que comúnmente se conoce como *habeas data* o *habeas scriptum*. Se complementa con la obligación que tienen los responsables de los archivos, registros, bancos o bases de datos de almacenar la información de modo tal que permita que cualquier persona pueda conocer no solo si sus datos personales figuran en una base de datos, sino también cuáles son. En síntesis, consiste en el derecho que tienen los ciudadanos a obtener en intervalos razonables y sin demoras o gastos excesivos la confirmación de la existencia o inexistencia de información relativa a su persona que existe en un archivo, registro, banco o base de datos, así como la comunicación de tales datos en forma inteligible. Este derecho puede ser ejercido en forma gratuita por quien acredite previamente su identidad con una frecuencia no inferior a seis meses. Si se acredita un interés legítimo, este derecho puede ejercerse a intervalos menores. La solicitud de información no requiere de fórmulas específicas y la respuesta debe permitir que el titular de los datos:

- Sepa si se encuentra o no en el archivo, registro, base o banco de datos.

- Conozca todos los datos relativos a su persona que constan en el archivo, registro, base o banco de datos.

- Solicite información acerca de la finalidad para la cual sus datos fueron recabados.

- Sepa si el archivo se encuentra registrado en el Registro Nacional de Bases de Datos Privadas.

- Conozca el destino previsto para sus datos.

Derechos de rectificación, cancelación o supresión

Para los responsables de los archivos, registros, bancos o bases de datos que contengan datos de carácter personal, surge para los ciudadanos el derecho a exigir que, cuando los mismos sean inexactos e incompletos, deben ser rectificados o actualizados y cuando corresponda, suprimidos o sometidos a confidencialidad. El derecho de cancelación permite eliminar del archivo o base de datos a aquellos datos personales que por diversas circunstancias no deben figurar en el mismo.

Es importante destacar que el derecho de cancelación debe comprenderse en forma amplia, como la acción tendiente a hacer irreconocibles los datos archivados, ya sea anulando, destruyendo, borrando, tornando ilegible o declarando su nulidad. La metodología adecuada variará según las circunstancias.

Derecho de tutela

Es el derecho que les asiste a todos los titulares de datos en ejercicio de los demás derechos conferidos por la ley para hacer frente a los incumplimientos de la misma. La ley prevé dos tipos de acciones: reclamar los datos y prejuicios que pudieran habérsele ocasionado a raíz de la inobservancia de la ley; e iniciar la denominada "acción de protección de los datos personales", que tiene como fin tomar conocimiento de los datos personales almacenados en archivos, registros, bancos o bases de datos públicas o privadas destinados a proporcionar informes y de su finalidad, y exigir la rectificación, supresión, confidencialidad o actualización de la información cuyo registro se encuentra prohibido o se presuma que sea falsa, inexacta o desactualizada.

Derecho de impugnación de valoraciones

Además de declarar su insanable nulidad, la ley legitima a los ciudadanos a impugnar, entendiéndose por ello recurrir, demandando su invalidez, todo acto administrativo o decisión privada que implique una apreciación o valoración de su comportamiento fundada únicamente en el tratamiento de datos de carácter personal que permita obtener un determinado perfil de su personalidad.

Derecho de consulta

Este derecho permite que toda persona pueda solicitar a la DNPDP información relativa a la existencia de archivos, registros, bancos y bases de datos personales sin finalidades y la identidad de sus responsables. El registro que debe mantener dicho organismo es de consulta pública y gratuita.

IV - DEBERES Y OBLIGACIONES DE LOS TITULARES DE LOS ARCHIVOS, REGISTROS, BANCOS O BASES DE DATOS QUE CONTENGAN INFORMACIÓN PERSONAL DE LOS CIUDADANOS

Además de los derechos de defensa legalmente reconocidos a los titulares de los datos de carácter personal, la ley establece una serie de garantías específicas tendientes a asegurar su respeto, cuyo incumplimiento puede ser sancionado. Estas garantías constituyen otros tantos deberes que pesan sobre la persona del responsable del archivo, registro, banco o base de datos, entre los que se destacan los de secreto, registro, información, seguridad, velar por una calidad de los datos, dar acceso a los datos, rectificación, cancelación y supresión, bloqueo, controlar la cesión de datos a terceros y de información al cesionario.

Deber de secreto

Definido también como "deber de confidencialidad", obliga al responsable del archivo, registro, banco o base de datos y a las personas que intervengan en cualquier fase del tratamiento de datos a respetar el secreto profesional respecto de los mismos, exigencia que debe subsistir aun después de finalizada la relación con el titular del archivo de datos. Tiene como objetivo evitar que la información salga del círculo de personas a quienes está dirigida, habida cuenta de que sobre los archivos o bases de datos pesa una presunción de secreto.

Deber de registro

Pone en cabeza de los usuarios y responsables de los archivos, registros, bases o bancos de datos que contienen información personal, la exigencia de inscribirlos en el Registro Nacional de Bases de Datos Privadas habilitado por la DNPDP. La inscripción de archivos, registros, bancos y bases de datos debe comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales

contenidos en cada archivo; d) Forma de recolección y actualización de datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en las que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación y actualización de los datos.

Excepciones del deber de registro

Todos aquellos archivos, registros, bancos o bases de datos con fines de publicidad que se encuentren adheridos a alguna cámara, asociación y/o colegio profesional del sector que disponga de un Código de Conducta homologado por la DNPDP están exceptuados de este deber. En estos casos, serán dichas cámaras, asociaciones y/o colegios profesionales quienes deberán inscribirse, acompañando una nómina con el nombre, apellido y domicilio de sus asociados, quienes, por estatuto, deberán estar obligatoriamente adheridos a dicho Código de Conducta.

El RNBDP se habilitó el 1/8/2005. Si bien el plazo original de vencimiento de la obligación de inscribir las bases de datos privadas vencía el 31/1/2006, el mismo fue prorrogándose.

Deber de información

Es la contracara del derecho de información que tienen los titulares de los datos personales. La ley exige que cuando se recolecten datos de carácter personal que requieran el consentimiento de sus titulares, el responsable del tratamiento ponga a disposición de los mismos una serie de informaciones que le permitan decidir en forma libre la conveniencia de proporcionar datos referidos a su persona. Dicha información deberá indicar qué se va a hacer con los datos, quiénes serán los destinatarios de la información y la identidad y dirección del responsable del archivo o base de datos. Este deber también es exigido en los casos de cesión de datos a terceros, oportunidad en la que el titular de los datos debe ser informado sobre la finalidad de la cesión, la identidad del cesionario y los elementos que permiten realizar dicha cesión.

Deber de seguridad

El responsable del tratamiento de datos de carácter personal debe adoptar las medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado que permitan detectar desvíos, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Deber de velar por la seguridad de los datos

Consiste en el respeto necesario por parte del responsable y los usuarios de los archivos, registros, bancos o bases de datos, de las reglas establecidas para la recepción, tratamiento, uso, conservación, almacenamiento y cesión de datos, conjugadas con los principios generales de protección de datos. De esta manera, la calidad estará medida de acuerdo a los parámetros de pertinencia, proporcionalidad, lealtad, congruencia, exactitud y accesibilidad por parte del titular de los datos.

Cumplimiento del deber de dar acceso a los datos

El responsable de un archivo, registro, banco o base de datos que almacenan datos de carácter personal debe suministrar información amplia sobre la totalidad del registro perteneciente al titular de los datos personales que solicite el acceso de los mismos. El informe debe ser claro, exento de codificaciones y, en caso de ser necesario, debe entregarse acompañado de una explicación escrita en lenguaje accesible al conocimiento medio de la población.

Esta información puede suministrarse por escrito, por medios electrónicos, telefónicos, de imagen u otro medio idóneo a tal fin, a opción del titular de los datos personales, no obstante lo cual, pueden, además, ofrecerse los siguientes medios alternativos de información: visualizarse en la pantalla; informe escrito entregado en el domicilio del requerido; informe escrito remitido al domicilio denunciado por el requirente; transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información; cualquier otro procedimiento que sea adecuado a la configuración e implementación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario al mismo.

No siempre se debe cumplir con el deber de dar acceso a los datos; este deber cuenta con una clara excepción que permite que los responsables o usuarios de archivos, registros, bancos o bases de datos públicos puedan denegar, mediante resolución fundada, la información solicitada por los titulares de datos de carácter personal, cuando por intermedio de ello se pudieran obstaculizar actuaciones judiciales o administrativas en curso, vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas.

Deberes de rectificación, cancelación y supresión

Después de recibir un reclamo realizado por una persona cuyos datos personales se encuentran registrados en un archivo, registro, banco o base de datos, o al advertir un error o falsedad en la información, el responsable o usuario del mismo debe proceder a la rectificación, supresión o actualización de la información registrada. Este deber es la consecuencia lógica del principio de pertinencia, pues si solo pueden tratarse los datos que sean a la finalidad que lo justifica, aquellos que hayan dejado de serlo por los motivos que fueren no pueden seguir siendo objeto de tratamiento.

Existen excepciones al deber de supresión, pues este no procede cuando pudiese causar perjuicios o derechos o intereses legítimos de terceros o cuando existiera una obligación legal de conservar los datos. De la misma forma, los responsables o usuarios de los archivos, registros, bancos o bases de datos públicos pueden, mediante decisión fundada, denegar la rectificación o la supresión de los datos de carácter personal solicitada por el titular de los mismos en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

Deber de bloqueo

Es el deber que tienen los titulares de archivos, registros, bancos o bases de datos de bloquear el registro referido a una persona durante el transcurso del proceso de verificación y rectificación de los errores o falsedades que pudieran haberse denunciado, período durante el cual, en caso de proveerse información relativa al titular de los datos personales analizados, se deberá aclarar que dichos datos se encuentran sometidos a revisión.

Deber de controlar la cesión a terceros

Este deber constituye el registro último y fundamental de la pretensión legal de preservar la intimidad de los datos incorporados en archivos o bases de datos. Si bien la regla general impide ceder tales datos, la cesión puede efectuarse, siempre y cuando concurran los siguientes requisitos: consentimiento del afectado; que la cesión constituya un requisito para

el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y el cesionario; que la cesión le sea informada al titular de los datos, indicándose además la finalidad de la cesión, la identidad del cesionario y los elementos que permiten hacerlo.

Deber de información al cesionario

El responsable o usuario de un archivo, registro, banco o base de datos que proceda a rectificar, cancelar o suprimir información de carácter personal relativa a una persona que hubiera sido previamente cedida a terceros, debe notificar de esta rectificación o supresión al cesionario.

V - SANCIONES

Sin perjuicio de las responsabilidades administrativas que pudieran caberle en los casos de incumplimiento o violación a la ley por parte de los responsables o usuarios de los archivos, registros, bancos o bases de datos públicos, la ley 25326 establece dos tipos de sanciones: administrativas y penales.

Sanciones administrativas

Las sanciones que se pudieran aplicar van desde un simple apercibimiento hasta una suspensión o bien la aplicación de multas pecuniarias, la clausura o cancelación del archivo, registro, banco o base de datos.

Sanciones penales

Para aquel que inserte o hiciera insertar, a sabiendas, datos falsos en un archivo, registro, banco o base de datos personales, se establece una pena de prisión de 1 mes a dos años. Para quien proporcione a terceros, a sabiendas, información falsa contenida en un archivo, registro, banco o base de datos personales, se establece una pena de prisión de entre 6 meses a 3 años. Si de alguno de estos delitos se derivara un perjuicio a alguna persona, la escala podrá aumentarse en la mitad del mínimo y del máximo, y si el autor o responsable del ilícito es un funcionario público en ejercicio de sus funciones, podrá aplicarse la accesoria de inhabilitación en el desempeño de cargos públicos por el doble del tiempo de la condena.

Para quien, a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un archivo, registro, banco o base de datos personales, se establece una pena de 1 mes a 2 años de prisión. La misma pena se establece para quien revelare información registrada a otro, en un archivo, registro, banco o base de datos personales, cuyo secreto estuviese obligado a preservar por disposición de una ley y, si además se trata de un funcionario público, podrá aplicársele, además, una pena de inhabilitación especial de 1 a 4 años.

VI - INFRACCIONES

La ley también habla de infracciones a las que clasifica en las categorías de leves, graves y muy graves.

Infracciones leves

Sin perjuicio de otras que a juicio de la DNPDP también las constituyan, las siguientes conductas serán consideradas infracciones leves: no atender, por motivos formales, la solicitud del interesado de acceso, rectificación, confidencialidad o cancelación de los datos personales, objeto de tratamiento cuando legalmente proceda; no proporcionar la información que solicite la Dirección antes mencionada en el ejercicio de las competencias que tiene atribuidas, en relación con los aspectos no sustantivos de la protección de datos; no solicitar la inscripción de una base de datos personales pública o privada que exceda el uso personal; recoger datos de carácter personal de los propios titulares sin proporcionales la información que señala el artículo 6 de la ley 25326; incumplir el deber de secreto, establecido en el artículo 10 de la ley 25326, salvo que constituya una infracción grave.

Infracciones graves

Sin perjuicio de otras que a juicio de la DNPDP también las constituyan, las siguientes conductas serán consideradas infracciones graves:

- Proceder a la creación de bases de datos de titularidad pública o recoger datos de carácter personal para las mismas sin autorización de disposición general publicada en el Boletín Oficial o diario oficial correspondiente y cumpliendo con los requisitos del artículo 22 de la ley 25326.

- Proceder al tratamiento de datos de carácter personal que no reúnan las calidades de ciertos, adecuados, pertinentes y no excesivos en relación con el ámbito y la finalidad para los que se hubieran obtenido.

- Recoger datos de carácter personal sin recabar el consentimiento libre, expreso e informado de su titular, en los casos que este sea exigible.

- Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la ley 25326 o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya una infracción muy grave.

- El impedimento o la obstaculización del ejercicio de los derechos de acceso y la negativa a facilitar la información que le sea solicitada.

- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones, actualizaciones o supresiones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que ampara la ley 25326.

- La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a bases de datos que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellas otras bases de datos que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

- Mantener las bases de datos, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

- No proporcionar en plazo a la DNPDP cuantos documentos e informaciones sean requeridas, conforme a las previsiones de

la ley 25326 o sus disposiciones reglamentarias.

- La obstrucción al ejercicio de la función de inspección y fiscalización a cargo de la DNPDP.

- No inscribir la base de datos de carácter personal en el Registro Nacional de Protección de Datos Personales, cuando haya sido requerido para ello por la DNPDP.

- Incumplir el deber de información que se establece en los artículos 6 y 26 de la ley 25326 cuando los datos hayan sido recabados por persona distinta del afectado.

Infracciones muy graves

Sin perjuicio de otras que a juicio de la DNPDP también las constituyan, las siguientes conductas serán consideradas infracciones muy graves:

- Recoger datos de carácter personal en forma fraudulenta.

- La comunicación o cesión de los datos de carácter personal fuera de los casos en que estén permitidas.

- Recolectar y tratar los datos sensibles vulnerando los principios y garantías de la ley 25326.

- No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por la DNPDP o por las personas titulares del derecho de acceso.

- Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

- La vulneración del deber de guardar secreto sobre los datos sensibles, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

- No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, actualización, supresión o bloqueo.

- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en una base de datos, de conformidad con los artículos 5 y 6 de la ley 25326.

VII - *COOKIES*

Las *cookies* constituyen una potente herramienta utilizada por la mayoría de los sitios web y consisten en pequeños archivos de datos de texto que el servidor entrega al programa navegador que lo visita para que lo guarde en el disco rígido de la computadora con el fin de recolectar información acerca de lo que ha estado haciendo el usuario por sus páginas. Si un sitio web utiliza *cookies*, su titular debe explicar claramente qué son las *cookies*, qué tipo de información recopilan, cuál es su objeto y cómo pueden desactivarse. De esta manera, los usuarios tienen la libertad de elegir si prefieren la navegación sin *cookies*, de decidir si arriesgan una porción de su intimidad a cambio de una navegación más personalizada, o si aceptan la intromisión luego de comprobar que quienes las utilizan se ajustan a los límites impuestos por la ley.

VIII - NORMA ISO 17779

La norma ISO 17779 es un estándar de seguridad internacionalmente reconocido que contiene una serie de controles que contemplan las mejores prácticas en seguridad de la información. Probablemente, la DNPDP utilizará esta norma para exigir distintos niveles de seguridad a los responsables de archivos, registros, bancos o bases de datos personales, de acuerdo al tipo de datos que las mismas contengan.

IX - NORMA ISO 27001

El Reglamento General de Protección de Datos es cada vez más severo. Las organizaciones que manejan datos personales deben adaptar sus operaciones a los nuevos requisitos para evitar problemas con los clientes y las autoridades pueden hacerlo con la norma ISO 27001.

En lo que respecta a los servicios de infraestructura de la nube, el esfuerzo puede ayudar a los proveedores y los clientes.

En resumen, la Norma ISO 27001 es un estándar internacional que permite el aseguramiento, la confidencialidad y la integridad de los datos y de la información, así como de los sistemas que la procesan. La Gestión de Seguridad de la Información se complementa con las buenas prácticas o controles establecidos en la Norma ISO 27002.

X - CONCLUSIONES

La entrada en vigor de la ley 25326 de protección de datos personales ilustra un escenario lleno de nuevos requisitos que las organizaciones deben cumplir. Aunque se vienen realizando esfuerzos de adaptación a este entorno, las organizaciones afrontan el reto de mantener ese nivel de cumplimiento de manera continuada, planteándose establecer sistemas de gestión que les ayuden a conseguirlo.

En la actualidad, existen cada vez más países que desvían la mirada a estándares de conformidad más modernos e internacionales para ayudar a la gestión de este nuevo entorno, donde entra en juego la norma ISO 19600.

La reciente regulación en materia de datos personales adopta una evidente aproximación basada en el riesgo, muy alineada con el enfoque que también siguen los estándares internacionales basados en la estructura de alto nivel de ISO/IEC. Además, el responsable del tratamiento de los datos personales debe ser capaz de demostrar el correcto cumplimiento de sus obligaciones, lo que conlleva la trazabilidad documental de actividades, asignación de roles, responsables, criterios, etc., que son aspectos igualmente tratados en estos sistemas de gestión. Como sucede en otras áreas de conformidad, la diligencia debida de las organizaciones y sus responsables se medirá según hayan organizado el cumplimiento de sus obligaciones en

materia de datos personales. Y como en otros ámbitos también avalará su conducta el recurrir a prácticas reconocidas internacionalmente.

XI - BIBLIOGRAFÍA

- Decreto 1558/2001 de la República Argentina.
- Ley 25326 de la República Argentina.
- Norma ISO 19600.
- Norma ISO 27001.

Cita digital: EOLDC099607A