Protección de Datos Personales – Preguntas frecuentes

¿Cuál es el objeto de la Ley 25.326 de Protección de Datos Personales?
El artículo 1 de la ley 25.326 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 éstos 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 a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

¿Qué es 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 sólo a datos de personas físicas?
No; también se aplican, en cuanto resulte pertinente, a los datos relativos a las personas de existencia ideal.

¿Esta Ley sólo sirve para borrar datos negativos publicados por las empresas de informes comerciales?
No; la mayoría de la gente supone erróneamente que la Ley de Protección de Datos Personales (Hábeas Data) sólo permite controlar la información contenida en las bases de datos de las entidades financieras y de las empresas que brindan servicios de información comercial y crediticia.
No es así. También sirve para acceder, rectificar o suprimir datos personales que se encuentren almacenados en cualquier tipo de archivo, registro, base o banco de datos, ya sea público o privado.

¿Qué se entiende por archivos, registros, bases o bancos de datos privados destinados a dar informes?
El artículo 1º del Decreto 1558/2001 entiende por tales 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.

¿Cuál es el órgano de control?
La Dirección Nacional de Protección de Datos Personales (DNPDP), que funciona en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos.

¿Todas las bases de datos deben inscribirse en el Registro Nacional de Bases de Datos Privadas?
No; los archivos, registros, bancos o bases de datos formados por los particulares para uso exclusivamente personal están exentos del deber de registro.
Ellas son las que mantienen las personas físicas con fines exclusivamente particulares, como el caso de las agendas personales o las listas de teléfonos y direcciones, cuya obligación de registro supondría una intromisión ilegítima en su intimidad.

¿Qué ocurre con las fuentes de información periodística?
Este tipo de datos se encuentra excluido del régimen establecido por la Ley.

¿Qué son los datos sensibles?

No todos los datos personales requieren de idéntica intensidad protectora. La ley entiende por 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 está prohibida.

¿Qué requisitos mínimos deben cumplir las bases de datos para tener registrados datos personales de los usuarios?

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:

a) **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 creación de la base de datos. En ningún caso se puedan utilizar los datos obtenidos para finalidades distintas de aquéllas para las que se hubieran recogido.

b) **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 el que la información personal es recolectada. Los datos que se obtengan deben tratarse de manera leal y lícita, y su almacenamiento debe perseguir fines concretos y legítimos.

c) **Utilización no abusiva:** Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

d) **Exactitud:** Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. Si fueren inexactos o incompletos, deben ser suprimidos y sustituidos, o en su caso, completados.

e) **Limitación en el tiempo:** Los datos deben ser eliminados una vez que se haya cumplido la finalidad para la que fueron recabados.

f) **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.

g) **Publicidad:** Los archivos, registro, base o banco de datos alcanzados por las disposiciones legales deben inscribirse en el Registro de la Dirección Nacional de Protección de Datos Personales 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 de sus derechos.

h) **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.

i) **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.

¿Siempre debo obtener el consentimiento de los ciudadanos para registrar sus datos personales en un archivo, registro, banco o base de datos?

No; el requisito del consentimiento previo cuenta con las siguientes excepciones:

a) cuando los datos se obtienen de fuentes de acceso público irrestricto.

b) cuando lo datos se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.
c) 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.
d) cuando deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento.
e) cuando se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la ley 21.526.

¿Cuáles son los derechos que la ley le reconoce a los ciudadanos?
La ley reconoce a los ciudadanos los derechos de oposición, información, acceso, rectificación, cancelación, supresión, tutela, impugnación de valoraciones y consulta.

¿Qué es 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 de datos sensibles se trata.

¿Qué es el derecho de información?
El derecho de información 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 datos.
Consiste en la posibilidad de que tiene una persona a la que se le solicitan datos de carácter personal a ser previamente informada de modo expreso, preciso e inequívoco de las siguientes circunstancias:
a) La finalidad para la que serán tratados sus datos personales y quiénes pueden ser sus destinatarios o clase de destinatarios.
b) 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.
c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga.
d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos. Esta información deberá aparecer en los todos los formularios que se utilicen para recoger datos de carácter personal.

¿Qué es el derecho de acceso?
Entendido como la garantía de comprobación de que las informaciones que versan 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 cualquier persona pueda conocer no sólo 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:

a) Sepa si se encuentra o no en el archivo, registro, base o banco de datos.
b) Conozca todos los datos relativos a su persona que constan en el archivo.
c) Solicite información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos.
d) Solicite información acerca de la finalidad para la que sus datos fueron recabados.
e) Conozca el destino previsto para sus datos.
f) Sepa si el archivo se encuentra registrado en el Registro Nacional de Bases de Datos Privadas.

¿En qué consisten los derechos de rectificación, cancelación o supresión?

Como correlato lógico a los principios de finalidad, pertinencia y exactitud que en forma de deberes la ley impone a los responsables de los archivos, registros, bancos o bases de datos que contengan datos de carácter personal, surge el derecho a exigir que cuando los mismos sean inexactos o incompletos, sean 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. Resulta importante destacar que el derecho de cancelación debe ser entendido 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 empleada diferirá de acuerdo a las circunstancias.

¿Qué es el derecho de tutela?

Es el derecho que le 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 norma.

La ley prevé dos tipos de acciones:

a) Reclamar los daños y perjuicios que pudieran habérsele ocasionado a raíz de la inobservancia de la ley; y
b) 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 públicos o privados destinados a proporcionar informes, y de su finalidad; y exigir la rectificación, supresión, confidencialidad o actualización de la información cuyo registro se encuentre prohibido o se presuma que sea falsa, inexacta o desactualizada.

¿Qué es el 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.

¿Qué es el derecho de consulta?

Este derecho permite que toda persona pueda solicitar a la Dirección Nacional de Protección de Datos Personales información relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.

El registro que debe mantener dicho organismo es de consulta pública y gratuita.

¿Cuáles son los deberes y obligaciones de los titulares de 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 sancionad.
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 la 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.

¿Qué se entiende por deber de secreto?
Definido 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 destinada, habida cuenta que sobre los archivos o bases de datos pesa una presunción de secreto.

¿En qué consiste el deber de registro?
Este deber 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 Dirección Nacional de Protección de Datos Personales.
La inscripción de archivos, registros, bases o bancos 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 que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

¿Cuáles son las excepciones al 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 Dirección Nacional de Protección de los Datos Personales 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.

¿Cuándo se habilitó el Registro Nacional de Bases de Datos Privadas?

El Registro Nacional de Bases de Datos Privadas fue habilitado el 1º de agosto de 2005. Si bien el plazo original de vencimiento de la obligación de inscribir las bases de datos privadas vencía el 31 de enero de 2006, dicho plazo fue prorrogado hasta el 31 de marzo de 2006.

¿Qué es el deber de información?

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, quienes 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.

¿Qué se entiende por 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 desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

¿En qué consiste el deber de velar por la calidad de los datos?

Este deber consiste en el necesario respeto por parte del responsable y los usuarios de los archivos, registros, bancos o bases de datos, de las reglas establecidas para la recogida, tratamiento, uso, conservación, almacenamiento y cesión de datos, conjugadas con los principios generales de protección de datos.

De esta forma, la calidad estará medida de acuerdo a los parámetros de la pertinencia, proporcionalidad, lealtad, congruencia, exactitud y accesibilidad por parte del titular de los datos.

¿Cómo se cumple con el deber de dar acceso a los datos?

El responsable de un archivo, registro, banco o base de datos que almacene datos de carácter personal debe suministrar información amplia sobre la totalidad del registro perteneciente al titular de los datos personales que solicite el acceso a 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.

La 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:

a) Visualización en pantalla.
b) Informe escrito entregado en el domicilio del requerido.
c) Informe escrito remitido al domicilio denunciado por el requirente.
d) Transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información.
e) Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario al mismo.

¿Siempre se debe cumplir con el deber de dar acceso a los datos?
No; este deber cuenta con una clara excepción que permite que los responsables o usuarios de archivos, registros, bancos o bases de datos públicas 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.

¿En qué consisten los deberes de rectificación, cancelación y supresión?
Luego de recibir un reclamo efectuado por una persona cuyos datos personales se encuentren 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 sólo pueden tratarse los datos que sean adecuados a la finalidad que lo justifica, aquellos que hayan dejado de serlo, por los motivos que fuere, no pueden seguir siendo objeto de tratamiento.

¿Existen excepciones al deber de supresión?
Si; el deber de supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
Asimismo, los responsables o usuarios de 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.

¿Qué es el 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.

¿Cómo se cumple con el deber de controlar la cesión a terceros?
El deber de controlar la cesión a terceros de los datos, constituye el requisito 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 realizarse siempre y cuando concurran los siguientes tres requisitos:

a) Consentimiento del afectado.
b) Que la cesión constituya un requisito para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario.
c) 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 permitan hacerlo.

¿Qué es el 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 dicha rectificación o supresión al cesionario.

¿Cuáles son las sanciones que pueden aplicarse al titular de una base de datos que no cumple con la Ley?
Sin perjuicio de las responsabilidades administrativas que pudieran corresponder en los casos de incumplimiento o violación a la ley por parte de responsables o usuarios de archivos, registros, bancos o bases de datos públicos, la Ley 25.326 establece dos tipos de sanciones: administrativas y penales.

¿Qué tipo de sanciones administrativas pueden aplicarse a quienes no cumplan con las disposiciones de la Ley de Protección de Datos Personales?
Las sanciones que podrá aplicar la Dirección Nacional de Protección de Datos pueden ser desde un simple apercibimiento, hasta una suspensión, o bien la aplicación de multas de $ 1.000 a $ 100.000, la clausura o cancelación del archivo, registro, banco o base de datos.

¿Cuáles son las sanciones penales?
Para quien inserte o hiciere 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 2 años. Para quien proporcione a un tercero, 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 aplicársele la accesoria de inhabilitación para el desempeño de cargos públicos por el doble de 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 un pena de 1 mes a 2 años de prisión.
La misma pena se establece para quien revelare a otro información registrada en un archivo, registro, banco o base de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley, y si se trata de un funcionario público, podrá aplicársele, además, pena de inhabilitación especial de 1 a 4 años.

¿Cómo se clasifican las infracciones?
Las infracciones se clasifican en las siguientes categorías: "Leves", "Graves" y "Muy Graves".

¿Cómo se determina qué tipo de sanción corresponde aplicar?
El Decreto 1558/2001 establece que la cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, el volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceros, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

¿Cuáles son las infracciones leves?

Sin perjuicio de otras que a juicio de la Dirección Nacional de Protección de Datos Personales también las constituyan, las siguientes conductas serán consideradas infracciones leves:

a) 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.

b) No proporcionar la información que solicite la Dirección Nacional de Protección de Datos Personales en el ejercicio de las competencias que tiene atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción de una base de datos personales pública o privada que exceda el uso personal.

d) Recoger datos de carácter personal de los propios titulares sin proporcionarles la información que señala el artículo 6° de Ley N° 25.326.

e) Incumplir el deber de secreto establecido en el artículo 10 de la Ley N° 25.326, salvo que constituya infracción grave.

¿Cuáles son las infracciones graves?

Sin perjuicio de otras que a juicio de la Dirección Nacional de Protección de Datos Personales también las constituyan, las siguientes conductas serán consideradas infracciones graves:

a) 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 los requisitos del artículo 22 de la Ley N° 25.326.

b) Proceder al tratamiento de datos de carácter personal que no reúnan las calidades de ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

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

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en Ley N° 25.326 o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

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

f) 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 la Ley N° 25.326 ampara.

g) 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 aquellos otros bases de datos que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) 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.

i) No proporcionar en plazo a la Dirección Nacional de Protección de Datos Personales cuantos documentos e informaciones sean requeridos, conforme las previsiones de la Ley 25.326 o sus disposiciones reglamentarias.

j) La obstrucción al ejercicio de la función de inspección y fiscalización a cargo de la Dirección Nacional de Protección de Datos Personales.
k) 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 Dirección Nacional de Protección de Datos Personales.
l) Incumplir el deber de información que se establece en los artículos 6 y 26 de la Ley N° 25.326, cuando los datos hayan sido recabados de persona distinta del afectado.

¿Cuáles son las infracciones muy graves?
Sin perjuicio de otras que a juicio de la Dirección Nacional de Protección de Datos Personales también las constituyan, las siguientes conductas serán consideradas infracciones muy graves:
a) Recoger datos de carácter personal en forma engañosa y fraudulenta.
b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
c) Recolectar y tratar los datos sensibles vulnerando los principios y garantías de la Ley N° 25.326.
d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por la Dirección Nacional de Protección de Datos Personales o por las personas titulares del derecho de acceso.
e) 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.
f) 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.
g) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, actualización, supresión o bloqueo.
h) 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 N° 25.326.

¿A cuánto ascienden las multas que pueden aplicarse de acuerdo al tipo de infracción cometida?
a) **Infracciones leves:** De $ 1.000 a $ 3.000.
b) **Infracciones graves:** De $ 3.001 a $ 50.000.
c) **Infracciones muy graves:** De $ 50.001 a $ 100.000.

¿Qué son las cookies?
Las cookies constituyen una potente herramienta utilizada por la gran 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 esa computadora con el fin de recolectar información acerca de lo que el usuario ha estado haciendo 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 desean arriesgar 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.

¿Qué es el SPAM?

El SPAM integra el grupo de los llamados "Abusos en el Correo Electrónico" y consiste en la técnica de enviar indiscriminadamente mensajes de correo electrónico a usuarios que no pidieron recibirlos. Su práctica trasciende los objetivos habituales del servicio y perjudica a proveedores y usuarios. Si bien generalmente se lo utiliza con fines comerciales o publicitarios, no son pocos los casos en que se lo utiliza con el fin de paralizar el servicio por saturación de las líneas, del espacio en disco o de la capacidad de procesamiento de un servidor. En la mayoría de los casos el spammer -así se denomina a quienes practican esta actividad- es desconocido y la dirección de correo que aparece en el remitente es falsa, lo que impide identificar una dirección de retorno correcta para responder el mensaje.

Cada mensaje enviado por un spammer es transportado por varios sistemas hasta que llega al lugar de destino, generando costos a lo largo de la cadena. El bolsillo de los usuarios es quien paga los pulsos de su cuenta telefónica por el tiempo que ocupan en descargar estos mensajes, además de los recursos de espacio de almacenamiento y tiempo para su lectura y eliminación.

Por su parte, los proveedores de servicio consumen ancho de banda para procesarlos y, por ende, la velocidad y calidad de sus servicios disminuye. Finalmente, los costos se transfieren al usuario final, repercutiendo negativamente en la satisfacción de los clientes y en los ingresos económicos de las empresas.

El Spam ha sido condenado desde los albores de Internet, especialmente por la Netiquette y las RFCs 2505 y 2635, pero también por las asociaciones que nuclean a los proveedores de servicios de Internet y por diversos pronunciamientos judiciales extranjeros. No obstante, son pocas las voces que se alzan a favor de la prohibición total. Varios de los proyectos existentes sobre la materia, sobre todo los elaborados en la Unión Europea, consideran apropiado el sistema de opt-out que permite a los usuarios solicitar que sus datos sean excluidos de las bases de datos utilizadas por los spammers.

Ese es el criterio que, en concordancia con la Ley 25.326 de Protección de los Datos Personales, sostienen los escasos proyectos de Ley existentes sobre la materia, que en líneas generales consideran que las comunicaciones comerciales no solicitadas deben ser claramente identificadas como tales e incluir una opción automática de exclusión voluntaria de la lista de destinatarios.

Entendiendo que el método mencionado no impide que las víctimas del SPAM puedan evitar totalmente la invasión a su privacidad, valiéndose de la técnica del "marketing permission", las organizaciones protectoras de los usuarios y consumidores prefieren el sistema opt-in, según el cual quien pretenda enviar mensajes comerciales deberá contar con la autorización expresa del destinatario. Más allá de estas propuestas, aún no existe legislación nacional ni internacional que condene el SPAM.

Ni siquiera el famoso y nunca sancionado Decreto S.1618 del 105 Congreso que los spammers suelen mencionar al pie de sus mensajes de correo electrónico, que no fue más que un proyecto de enmienda para el Acta de Telecomunicaciones estadounidense presentado en el año 1998, pero que nunca fue sancionada. Evidentemente, el mundo sin fronteras creado por Internet impide que intentos de soluciones locales puedan aplicarse a problemas globales.

Por el momento la Netiquette y las condiciones de uso de los servicios de correo electrónico surgen como las mejores alternativas para intentar controlar el spam. Los programas utilizados para filtrar automáticamente dichos mensajes disminuyen los problemas, pero no son totalmente eficientes.

Los proveedores de servicios de Internet deben adoptar políticas de "tolerancia cero" respecto a los mensajes spam que envíen sus clientes y exigir el cumplimiento de las condiciones de contratación del servicio. Debe alentarse la aprobación de códigos de conducta que obliguen a las partes involucradas en el negocio a comportarse éticamente.

También es recomendable que se prohíba el desarrollo de software que permita enviar mensajes engañosos, que se impida que los remailers anónimos sean utilizados con fines publicitarios y que se concientice a las empresas que enviar e-mails inconsentidos perjudica su imagen comercial.
Finalmente, debe decirse que la Ley 25.326 de Protección de Datos Personales es hoy por hoy la herramienta jurídica más importante que los usuarios argentinos de Internet que reciben mensajes de correo electrónico no solicitado tienen a su alcance para protegerse del SPAM.