

**Diccionario
de
derecho mexicano
a la protección de datos personales
en posesión de los particulares**

**Jaime
Cortés González**

**Sonia del Carmen
Álvarez Cisneros**

**Diccionario
de
derecho mexicano
a la protección de datos personales
en posesión de los particulares**

**Jaime
Cortés González**

**Sonia del Carmen
Álvarez Cisneros**

**Diccionario
de
derecho mexicano
a la protección de datos personales
en posesión de los particulares**



Diccionario de derecho mexicano a la protección de datos personales en posesión de los particulares / Jaime Cortés González y Sonia del Carmen Álvarez Cisneros.- 1.ª ed., - México: Amate, 2016.

229 págs.; 21.5 x 14 cm

ISBN 978-607-507-590-7

1. Protección de datos. 2. Diccionarios. México.

I. Título. I. t.

Sistema Decimal Universal CDU: 342.738 (460)

Primera edición, 2016

La presentación y disposición en conjunto de:
Diccionario de derecho mexicano a la protección de datos
personales en posesión de los particulares

Es propiedad de los autores

Se autoriza copiar y compartir esta obra por cualquier medio, siempre y cuando no se haga con fines comerciales, no se modifique el contenido, se respete su autoría, se reconozca a los propietarios del copyright, y esta nota se mantenga. No permite obras derivadas.

Derechos reservados conforme a la ley:

© Copyright by Jaime Cortés González,

Sonia del Carmen Álvarez Cisneros

ISBN: 978-607-507-590-7

Impreso en México - *Printed in Mexico*

Dedicamos este libro a Aimée Cortés
Con amor

Índice

Abreviaturas y latinismos.....	9
Introducción.....	11
Diccionario.....	35
Bibliografía.....	223

Abreviaturas y latinismos

Cfr.

Deriva del latín confer, en español: cónfer, abreviaturas: cf., o cfr., que significa: compárese, confróntese con referencia a cotejar, como prueba de autoridad; se utiliza en notas interpretativas.

Ed.

Abreviatura, que significa: edición o editorial.

Et al.

Locución latina, deriva de et alii, en español: et álii., que significa: y otros; se utiliza, tras el nombre de un autor, para indicar que la obra intelectual ha sido realizada, además, por otras personas.

Ibídem.

Locución latina, en español: ibídem, abreviaturas: ib., o ibíd., que significa: la misma fuente, o allí mismo, o en el mismo lugar; se utiliza, cuando se repite la fuente de información anterior, cuando cambia un dato, se señalan los demás.

Íd.

Abreviatura de ídem, también se usa la abreviatura de la forma latina idem: id., sin tilde y con letra cursiva, que significa: el mismo, o lo mismo, o igual que; se utiliza, cuando se repite la fuente de información anterior, cuando no cambia algún dato.

Ob. cit.

Abreviatura, que significa: obra citada; en latín Op. cit., expresión latina, deriva de opus citatum.

Pág.

Abreviatura, que significa: página.

Págs.

Abreviatura, que significa: páginas.

[Sic]

El adverbio latino ‘sic’, deriva de sicut, en español: ‘sic’, que significa: así, o léase como está, se escribe entre corchetes; se utiliza al final de un texto transcrito que presenta error, vicio gramatical o un dato inexacto.

Introducción

Escribir es el cuento de nunca acabar y la tarea de Sísifo. Paul Valéry acertó: no hay obras terminadas, sólo obras abandonadas.

José Emilio Pacheco*

Este libro tiene dos antecedentes intelectuales, en primer lugar el *Prontuario de derecho a la protección de datos personales*¹, publicado en 2008, que fue presentado en público el 7 de junio en la XLI FERIA Municipal del Libro y la Cultura de Guadalajara 2009 Don Fernando del Pazo Morante, obra que su contenido principal trato legislación extranjera de España y de países de Hispanoamérica, asimismo de algunas entidades federativas de la República Mexicana, introduciendo al lector en forma general al área de derecho a la protección de datos personales, cuando se publicó esta área de la ciencia del Derecho,

*Pacheco, José Emilio, *Tarde o temprano*, Letras Mexicanas, México, Fondo de Cultura Económica, 1980, pág. 10.

¹Cortés González, Jaime, *Prontuario de derecho a la protección de datos personales*, México, Amate, 2008, págs. 1-173.

estaba poco transitada por los estudiosos mexicanos, el merito de esta publicación, es que hace un reconocimiento más del derecho a la protección de datos personales, como cuerpo de conocimiento, que se encuentra aún en plena fase de evolución y difusión en México.

El segundo antecedente fue el *Diccionario de derecho a la protección de datos personales*², publicado en 2010, que trato legislación extranjera y local de las entidades federativas de México, y como apéndice la Ley Federal de Protección de Datos Personales en Posesión de los Particulares publicada el 5 de julio de 2010. Ambas obras intelectuales del área de conocimiento específico del derecho a la protección de datos personales, que constituyen las fuentes de inspiración de este libro.

Necesidad

Ante la necesidad de un nuevo estudio exclusivo de México, surgió éste Diccionario de derecho mexicano a la protección de datos personales en posesión de los particulares, diferente en su totalidad a los textos inspiradores descritos con anterioridad, toda vez que su contenido es de interés exclusivo para México, del área de derecho a la protección de datos personales en posición de los particulares.

En esencia, resulta una versión actualizada, breve y nueva en modo de diccionario de un “curso completo elemental del derecho en México a la protección de datos personales en posesión de los particulares”.

²Cortés González, Jaime, *et al.*, *Diccionario de derecho a la protección de datos personales*, México, Umbral, 2010, págs. 1-196.

El derecho a la protección de datos personales

El progreso tecnológico ha dado origen a la denominada ‘era digital’, o ‘sociedad de la información’, donde la información puede circular por todo el mundo, debido a las redes computacionales, que permiten un intercambio inmediato de conocimientos e información, en la especie la aplicación de las nuevas tecnologías de la información y la comunicación genera que a diario se traten e intercambien datos de carácter personal, tanto en el sector público como en el sector privado.

El equilibrio entre el derecho de las personas, a preservar el control sobre sus datos personales y, la aplicación de las tecnologías de la información y la comunicación ha generado el surgimiento de la expresión ‘derecho a la protección de datos personales’, también denominado ‘derecho a la autodeterminación informativa’ o ‘derecho a la intimidad informática’.

Para comenzar, respecto a lo que ha de entenderse por el vocablo «protección de datos», en su sentido literal, es el «sistema legal que garantiza la confidencialidad de los datos personales en poder de las Administraciones públicas u otras organizaciones»³.

A partir de la interpretación gramatical que antecede, es posible para nosotros construir un concepto del derecho a la protección de datos personales, por tanto, en la comunidad hispánica, se entiende que

³Real Academia Española, *Diccionario de la lengua española*, tomo 2 h/z, 23. ^a, Edición del Tricentenario, México, Espasa Libros S.L.U.-Editorial Planeta Mexicana, S.A., de C.V., 2014, pág. 1801.

es un derecho autónomo, que otorga a toda persona una protección contra el posible mal uso de la información de carácter personal que le concierne, que en esencia consiste en un poder de disposición y de control sobre los datos personales, que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede recabar este tercero.

El derecho a la protección de datos personales, por tanto, es parte del patrimonio de toda persona la cual tiene derecho a saber quién tiene esos datos, qué se está haciendo con ellos y para qué se están utilizando, pudiendo oponerse a esa posesión o uso.

En síntesis, se entiende que el derecho a la protección de datos personales, es el derecho que otorga a toda persona una protección contra la posible utilización de sus datos personales por parte de terceros, sin su autorización, para confeccionar una información que, identificable con él, lo afecte en su entorno personal, social o profesional, en los límites de su intimidad.

La protección de datos personales, es un derecho en evolución constante, que ha empezado a incorporarse en las legislaciones, es un derecho que, en muchas ocasiones, resulta violado sin que el ciudadano sea consciente de ello, toda vez que no siempre se puede saber quién tiene los datos personales y qué se está haciendo con ellos; surgiendo el riesgo de que sean tratados de forma indebida. Esta situación genera una indefensión de los ciudadanos que ignoran o pierden el conocimiento de ‘donde’ se encuentran sus datos de carácter personal, ‘quien’ trata dichos datos y ‘para qué’ se utilizan⁴.

Origen y evolución

¿Qué ha de entenderse por derecho a la protección de datos personales? En párrafos anteriores se proporcionó un concepto amplio de este derecho. Habría que precisar un poco más, con aportaciones recientes de juristas, exponiéndose en orden de importancia como un hilo conductor, así en respuesta más amplia a esta cuestión, primero es necesario conocer en forma breve algunos hechos importantes del extranjero, relacionados con su origen y evolución, así a manera de antecedente histórico, se ha escrito que en 1967, en el seno de la Unión Europea se constituyó una Comisión Consultiva con el objeto de efectuar un pormenorizado análisis sobre las tecnologías de la información como posible medio utilizado para vulnerar los derechos de las personas, así en 1968 surgió la resolución 509, de la Asamblea del Consejo de Europa sobre “los derechos humanos y los nuevos logros científicos y técnicos”.

La primera ley específica en la materia fue la Ley Alemana del Land de Hesse de 17 de octubre de 1970, esta norma tutela los datos que son objetos de tratamiento en organismos públicos.

Dentro del Consejo de Europa en 1973, apareció la Resolución 22/1973, de 20 de noviembre, del Consejo de Europa sobre regulación jurídica de los ficheros electrónicos en el sector privado, en 1974 apareció la Resolución 29/1974 de 29 de noviembre de 1974,

⁴Apuntes recabados por Jaime Cortés González en febrero de 2006, del curso «Acceso a la información, transparencia y protección de datos», impartido por el profesor José Luis Piñar Mañas, del programa de Doctorado en Derecho “Cuestiones actuales de la ciencia jurídica” de la Universidad San Pablo CEU Madrid en colaboración con la Universidad de Guadalajara.

para establecer pautas ordenadoras del sector público de la informática, mismas resoluciones que han sido consideradas por la doctrina como el punto de partida de la proliferación legislativa que se irá produciendo en el continente europeo, así los principios que fueron establecidos en ambas resoluciones están vigentes en la actualidad.

Apareció el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, texto decisivo en el ámbito legal de la protección de datos de carácter personal.

El 31 de diciembre de 1983 se hizo pública la sentencia dictada por el Tribunal Constitucional Alemán de 15 de diciembre del mismo año, aprobada por el parlamento alemán el 4 de marzo de 1983, hecho relevante para evolución histórica de este derecho, hasta la actualidad en constante evolución, esta sentencia sienta precedente toda vez que establece las bases de la autodeterminación informativa o consentimiento⁵.

El jurista español José Luis Piñar Mañas, afirma:

El derecho fundamental a la protección de datos personales es uno de los más importantes en la sociedad actual. El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, aprobada en Niza en 2000, reconoce expresamente el derecho a la protección de datos de carácter personal, lo que ha producido un cambio sustancial en la consideración sobre ese derecho fundamental. Éste es el punto de partida⁶.

En línea con lo que acaba de indicarse, se transcribe el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea

Artículo 8

Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

En palabras del Tribunal Constitucional Español, en lo que aquí interesa, publicó:

De todo lo dicho resulta que el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.⁷

En concepción del escritor argentino Juan Antonio Travieso:

La protección de los datos personales constituye un nuevo aspecto de los derechos humanos aplicados en el mundo de la tecnología. La sociedad de la información en un mundo que se ha tornado esencialmente digital es el escenario donde se desenvuelve esta disciplina. La protección de datos personales en general, garantiza el derecho al honor y a la privacidad de las personas y las defiende del uso indebido de sus datos, por eso ha sido consagrada por normas constitucionales, leyes y reglamentos⁸.

De lo anterior se afirma que el derecho a la protección de datos personales es un derecho humano de tercera generación.

⁵Al respecto, véase Almuzara Almaila, Cristina, *et al.*, *Estudio práctico sobre la protección de datos de carácter personal*, 2.ª ed., España, Lex Nova, 2007, págs. 33-34.

⁶Piñar Mañas, José Luis, “La mirada europea. Protección de datos personales”, en *Revista Nexos*, México, D. F., año 29 volumen XXIX número 353 mayo de 2007, pág. 29. Se ha respetado, en cada caso, la ortografía del texto transcrito.

⁷Boletín Oficial del Estado, número 4. Suplemento. Publicado el jueves 4 de enero de 2001, pág. 112. Sentencia pronunciada por el Pleno del Tribunal Constitucional Español, en el recurso de inconstitucionalidad número 1463-2000, parte II, fundamentos jurídicos, apartado 7. Reino de España.

⁸Así ha sido advertido por Travieso, Juan Antonio, “La protección de datos personales en la Argentina: De la teoría a la práctica”, en García Torres, Antonio, *La protección de datos personales en México*, México, publicado por el Senado de la República, 2006, págs. 95-96.

En este sentido, ha escrito el jurista mexicano Antonio García Torres:

En términos generales se puede considerar que el derecho a la protección de datos personales consiste en el poder de disposición sobre los datos personales, el cual se desenvuelve en el previo consentimiento para la recogida y uso de los datos, en el derecho a ser informado sobre el destino y uso de ellos, y en el derecho de acceder, rectificar y cancelar los datos⁹.

Por parte de los juristas mexicanos Alonso Gómez-Robledo Verduzco y Lina Ornelas Núñez, afirman:

De manera que el derecho a la protección de datos se traduce en el reconocimiento y establecimiento de prerrogativas, principios y procedimientos para el tratamiento por parte del Estado o de terceros, de la información concerniente a personas físicas.

Las prerrogativas son el derecho a ser informado de la existencia de bases de datos que contengan su información, a otorgar su consentimiento libre, expreso e informado para la transmisión de dicha información, así como el derecho a oponerse a que sean utilizados y finalmente, a solicitar que se corrijan o cancelen (derecho al olvido) cuando así resulte procedente[sic]¹⁰.

⁹García Torres, Antonio, op. cit., pág. 53.

¹⁰Véase con amplitud Gómez-Robledo Verduzco, Alonso y Ornelas Núñez, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2006, págs. 17-18.

La jurisprudencia mexicana, ha establecido que el derecho a la protección de los datos personales está previsto, con la finalidad de proteger al titular de la información para que pueda manifestar su oposición a la divulgación, no sólo de sus propios datos personales, sino también de los concernientes a su persona, esto es, los que ponen en riesgo su vida, seguridad o salud, los secretos industriales, fiscales, bancarios, fiduciarios o cualquier otro considerado como tal por una disposición jurídica.

De tal modo que una resolución que permite el acceso a la información perteneciente a un tercero, transgrede en el derecho de su titular a que se proteja, e incluso a oponerse a su divulgación, esto es, a intervenir en la delimitación o determinación de la parte que puede divulgarse.

En consecuencia, el titular de la información tendrá interés jurídico para reclamar en un juicio de amparo una determinación del Instituto Federal de Acceso a la Información y Protección de Datos por la cual se ordene la elaboración de la versión pública para entregarla al solicitante de la misma; lo anterior en atención de que el titular de la información al ser propietario de la información, tiene el derecho a que ésta sea protegida, lo cual, a su vez, le otorga el derecho de oposición, el cual involucra la facultad de intervenir en la delimitación o determinación de la parte que puede ser del conocimiento del solicitante, antes de que se ordene la elaboración de la versión pública correspondiente, como un mecanismo para que no se trastoquen sus derechos públicos subjetivos, sin afectar el derecho de acceso a la información de los peticionarios.

Principios del derecho a la protección de datos personales

Una vez expuesto con amplitud lo que ha de entenderse por el derecho a la protección de los datos personales, surge otra cuestión medular que su respuesta todo lector debe saber.

¿Cuáles son los principios del derecho a la protección de los datos personales? Son los principios que configuran el contenido esencial de éste derecho, que en coherencia a la dogmática de la materia, todo ordenamiento jurídico que reconozca este derecho debe contener.

Se comienza con el principio de tutela del derecho a la protección de datos personales a través de un organismo independiente o, un Ente público independiente, es decir, una ‘autoridad de control independiente’¹², descrito bajo la expresión:

o Autoridad de control.

¹¹En este sentido, cfr. Jurisprudencia (común), tesis: PC.I.A. J/12 K (10a.) Registro No. 2 006 753, el Pleno en Materia Administrativa del Primer Circuito, en *Gaceta del Semanario Judicial de la Federación*, México, Décima Época, Libro 7, junio de 2014, Tomo II, pág. 1127, rubro: “DERECHO A LA INFORMACIÓN. EL TITULAR DE ÉSTA TIENE INTERÉS JURÍDICO PARA RECLAMAR EN AMPARO LA DETERMINACIÓN DEL INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS QUE ORDENA LA ELABORACIÓN DE LA VERSIÓN PÚBLICA QUE CONTIENE DATOS PERSONALES O QUE LE CONCIERNEN COMO PERSONA”.

¹²Puntualizado en el artículo 28.1 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La ley española en materia de protección de datos personales, establece los principios de la protección de datos, que son los postulados fundamentales que constituyen las características propias de este derecho y que se detallan en sus artículos 4 al 12, que denominó:

- o Calidad de los datos.
- o Derecho de información en la recogida de datos.
- o Consentimiento del afectado.
- o Datos especialmente protegidos.
- o Datos relativos a la salud.
- o Seguridad de los datos.
- o Deber de secreto.
- o Comunicación de datos.
- o Acceso a los datos por cuenta de terceros.

Los derechos de las personas titulares de datos concretan esos principios generales, derechos que se conocen bajo las locuciones siguientes:

- o Impugnación de valoraciones.
- o Derecho de consulta al Registro General de Protección de Datos.
- o Derecho de acceso.
- o Derecho de rectificación y cancelación.
- o Derecho de oposición del interesado.
- o Tutela de los derechos.
- o Derecho a indemnización.

Derecho mexicano a la protección de datos personales

En relación con la incorporación del derecho a la protección de datos personales en nuestro país, desde hace varios años, empezaron a presentarse iniciativas legislativas en el congreso, algunas de reforma

en la Constitución Política de los Estados Unidos Mexicanos, otras para una ley federal, otras para reformar el Código Penal Federal, y además algunas entidades federativas promulgaron su propia ley en esta materia, constituyendo los prototipos jurídicos mexicanos en materia de protección de datos personales; para no desviar el rumbo de este texto no se entró al análisis de dichas iniciativas legislativas, ni de legislaciones de entidades federativas de la República Mexicana, en razón de que en el transitorio quinto de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, se dispuso que las disposiciones locales en materia de protección de datos personales en posesión de los particulares se abrogan, y se derogan¹³ las demás disposiciones que se opongan a dicha ley.

En la actualidad cada entidad federativa tiene en forma similar su organismo público autónomo especializado en materia de información pública y protección de datos personales¹⁴.

¹³La palabra ‘abrogación’, se refiere a la abolición, revocación y anulación de una ley, un código, un reglamento o un precepto, es decir, la supresión total de la vigencia y por lo tanto de la obligatoriedad de una ley, código o reglamento; en cambio, la palabra ‘derogar’, se refiere a la revocación de sólo alguno de los preceptos de la ley, código o reglamento, mientras que la abrogación implica la anulación total de la eficacia jurídica de un mandato legal en su conjunto. Con amplitud cfr. Berlín Valenzuela, Francisco, (Coordinador), *et al.*, *Diccionario universal de términos parlamentarios*, 2.ª ed., México, Cámara de Diputados del H. Congreso de la Unión Comité del Instituto de Investigaciones Legislativas LVII Legislatura, Miguel Angel Porrúa, 1998, págs. 17-18.

El derecho a la protección de datos personales es una garantía individual constitucional al establecerse en la Ley Suprema mexicana en su artículo 16 párrafo segundo, que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los datos personales, asimismo a manifestar su oposición en la forma que fije la ley

En la nación mexicana, se encuentra como antecedente la reforma realizada el 20 de julio de 2007 al artículo 6º de la Carta Magna mexicana, en la que se adicionó un párrafo segundo, sentando el derecho a la información o transparencia, y la protección de datos personales por parte de las entidades públicas, reconociendo los derechos de acceso y rectificación¹⁴; son dos derechos independientes entre sí y autónomos, uno se trata de acceso a la información o transparencia y el otro, se trata de protección de datos personales.

La Cámara de Senadores, el 4 de diciembre de 2008, aprobó una reforma constitucional a los artículos 16 y 73 que son la base para contar con una ley federal en materia de protección de datos en posesión de los particulares en México.

El 30 de abril de 2009, se publicó en el Diario Oficial de la Federación el Decreto en el que el Congreso

¹⁴Véase en este diccionario: México; entidades federativas de la República Mexicana, leyes estatales vigentes en materia de protección de datos personales u organismos públicos autónomos especializados en materia de información pública y protección de datos personales.

¹⁵Véase con amplitud, el texto vigente del artículo 6º de la Constitución Política de los Estados Unidos Mexicanos.

General de los Estados Unidos Mexicanos, previa la aprobación de la mayoría de las Legislaturas de los Estados, declara adicionada la fracción XXIX-O al artículo 73 de la Constitución Mexicana, otorgando facultades al Congreso mexicano para legislar en materia de protección de datos en posesión de los particulares.

El 1º de junio de 2009, se publicó en el Diario Oficial de la Federación, el Decreto por el que se adiciona un segundo párrafo, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, otorgando una nueva garantía individual de seguridad jurídica:

Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

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 terceros¹⁶.

¹⁶Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 5 de febrero de 1917, artículo 16 párrafos primero y segundo.

El 27 de abril de 2010, la Cámara de Senadores, expidió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en forma simultánea a las reformas a los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II, del título segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en que se establece que el Instituto Federal de Acceso a la Información y Protección de Datos, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia¹⁷.

Decreto que entró en vigor el 6 de julio de 2010, día siguiente de su publicación, en el Diario Oficial de la Federación; de ahí se afirma, que es la fecha en que comenzó la dogmática propia de la República Mexicana del derecho a la protección de datos personales, en otras palabras, se inició el ahora denominado derecho mexicano a la protección de datos personales.

Lo anterior, toda vez que las normas legales vigentes se consideran dogmas, en otras palabras, declaraciones de la voluntad legal, con pretensión de validez general que en consecuencia deben tenerse por verdad firme y cierta.

En el Diario Oficial de la Federación, el 21 de diciembre de 2011, se publicó el reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares que complemento dicha ley.

¹⁷Dictamen de la Cámara de Senadores del martes, 27 de abril de 2010, publicado en la Gaceta del Senado No. 127.

El 7 de febrero de 2014, se publicó en el Diario Oficial de la Federación el Decreto en el que el Congreso General de los Estados Unidos Mexicanos, declara adicionada la fracción XXIX-S al artículo 73 de la Constitución Federal mexicana, otorgándole facultades al Congreso mexicano para expedir las leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada el 11 de junio de 2002, se abrogó al expedirse la vigente Ley Federal de Transparencia y Acceso a la Información Pública, publicada el 9 de mayo de 2016, que garantiza el derecho de acceso a la Información Pública en posesión de cualquier autoridad, entidad y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerzca recursos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerzca recursos públicos federales o realice actos de autoridad.

En cambio, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, garantiza el derecho a proteger los datos personales en poder de personas físicas, empresas y organizaciones privadas, ambas son leyes vigentes, de orden público y de observancia general en toda la República Mexicana.

Justificación y finalidad

Se presenta este *Diccionario de derecho mexicano a la protección de datos personales en posesión de los particulares*, libro, básico, especializado, pensado, como herramienta de autodidactismo, consulta y de divulgación en México de la información básica de esta área del conocimiento, para el dominio público.

Busca contribuir al desarrollo del área del derecho a la protección de datos personales en México, al presentar esta selección de los términos y vocablos que consideramos representativos sobre esta área de conocimiento.

Destinatarios

Este libro es útil para el lector que se instruye por sí mismo, toda vez que este diccionario es actualizado, autodidáctico, completo y objetivo, elemental de referencia para éste derecho, útil para el ciudadano común, asimismo para profesionistas e investigadores de diferentes áreas.

Sin duda alguna servirá de guía para posteriores lecturas e investigaciones por lo que será de interés general.

Método y proceso

Este diccionario se formó de la compilación básica de conceptos¹⁸ y definiciones¹⁹ respecto de palabras, locuciones o vocablos utilizados en el ámbito del derecho en México a la protección de datos personales en posesión de los particulares, de ahí la razón de su título.

En este diccionario los autores seleccionamos los conceptos y definiciones que en su mayoría fueron acuñados por legisladores expertos, respetando las palabras precisas que ellos utilizaron.

Cabe señalar que por regla general las citas de leyes no requieren de nota que identifique su origen, pues se sabe que su autor fue el poder legislativo, la editorial el boletín, diario o periódico oficial respectivo.

Distinguido lector, en este diccionario hallarás información de utilidad, por ejemplo la concerniente a la expresión: «Algunas formas de ataque a los datos personales en internet», asimismo respecto al tema de la «Suplantación de identidad», también denominado robo de identidad, estafa, fraude, *phishing*, hurto, plagio, suplantación o usurpación de identidad.

Forma

En cuanto a forma, es un diccionario especializado de índole monográfico, es monolingüe de lengua española de un subconjunto de categorías léxicas, específico del vocabulario usual o relacionadas en el contexto del área de derecho a la protección de datos

¹⁸La palabra ‘concepto’, significa la imagen racional que representa a una cosa existente o determinada mediante algún razonamiento, o bien, creada por la misma imaginación. Con amplitud cfr. De Gortari De Gortari, Eli Eduardo, *Diccionario de la lógica*, México, Plaza y Valdés Editores, reimpresión 1988, pág. 86.

¹⁹La palabra ‘definición’, significa la manifestación del empleo específico de un concepto o término. Al respecto con amplitud cfr. Tamayo y Tamayo, Mario, *Diccionario de la investigación científica*, 2.ª ed., México, Limusa Noriega Editores, 2004, pág. 36. A partir de lo anterior, se colige que las definiciones resultan exactas, en cambio, los conceptos resul-

personales en posesión de los particulares, que trata en especial de legislación mexicana vigente, y que sólo para mayor abundamiento de la materia trata alguna legislación extranjera hispánica, marco dentro del cual se desarrolló el registro léxico.

En suma, es un repertorio que recoge en orden alfabético entradas o unidades léxicas, expresiones, frases, locuciones, palabras, términos, vocabulario o voces, de las cuales se proporciona su acepción, concepto, definición jurídica o su significado utilizado en el ámbito del derecho a la protección de datos personales en México.

Bibliografía

En la parte final de este libro se enlista la bibliografía y las fuentes de información utilizadas, sustento de donde emanaron las palabras, las voces así como sus respectivos significados o acepciones recabados. Se proporcionan los datos exactos de cada fuente de consulta utilizada, dando crédito y respetando a todos los autores respectivos.

En los diccionarios los textos se forman con las conceptualizaciones o las palabras precisas de quienes las formularon con anterioridad, en otras palabras, se redactan con los modos de recoger e interpretar la realidad, que en esta obra los autores en su mayoría fueron los legisladores respectivos.

²⁰La palabra ‘conceptualizar’, es un verbo que significa forjar conceptos acerca de algo. Al respecto con amplitud cfr. Fernández Fernández, Antonio, *Diccionario de dudas: A-H*, España, Ediciones Nobel, Ediciones de la Universidad de Oviedo, 2007, pág. 165.

Contenido

En cuanto a contenido central de la obra, el material que aporta es actual, se omiten conjeturas, críticas e interpretaciones propias, de hermenéutica, jurisprudencia o de exégesis respecto a los textos legales que les dan origen, con el fin de proporcionar al apreciado lector una seguridad fiable de la información aportada, con la finalidad de que el propio lector formule sus propias reflexiones, en torno a este derecho.

Se omitió la utilización de abreviaturas, acrónimos y siglas para dar mejor comprensión al lector del contenido; se prescinde de significados etimológicos, así como ámbito o contexto histórico y teórico, se recogió en orden alfabético a manera de diccionario sólo las frases y términos básicos más significativos.

Guía de uso

Se prescindió de un índice de las entradas léxicas o voces, reúne en forma alfabética sólo las unidades léxicas que se utilizan en la actualidad en ésta área del Derecho mexicano, resaltadas con letras mayúsculas en negritas permite su ubicación con comodidad, facilidad y rapidez, enseguida se proporciona al lector una acepción dogmática y su referencia de origen escrita con letras cursivas.

Las referencias cruzadas, están escritas en mayúscula al final del concepto o definición, sin ser sinónimos, se recogen algunas de las variantes principales de un término similar con una referencia cruzada que dirige al estimado lector a la entrada principal; se han incluido para facilitar la aclaración o comparación de conceptos o definiciones legales, también para contrastar vocablos.

Invitación

Por el diseño del libro, la redacción propia, en su mayoría se ofrece en esta exposición. A partir de la lectura de esta introducción se invita para leerlo con libertad en partes, eligiendo en forma indistinta la página, toda vez que la lectura de una locución en particular atrae otras expresiones y así puede leerse o releerse en cualquier orden por partes, familiarizándose por completo con el derecho a la protección de datos personales en posesión de los particulares en México. De esta manera, el lector se apropiará del conocimiento de este derecho.

Recomendaciones

Amigo lector, la mejor manera de proteger tus datos personales es absteniéndose o negándose a dar, informar, proporcionar, publicar o suministrar tu información personal, en forma indiscriminada.

Para prevenir el mal uso de tus datos personales, evita completar formularios de datos al azar, que se ofrecen en vía pública, vía telefónica y a través de las nuevas tecnologías, al usar el internet y las redes sociales asimismo en el consumo de datos en la web, o red informática, en estas últimas existen diferentes formas de ataque a los datos personales, que en su mayoría tienen por finalidad robar información, para después usarla con fines publicitarios o con fines delictivos, en el ámbito de la informática a estos se les ha denominado *phishing*, virus informático, *pharming*, troyanos, *keyloggers*, *sidejacking*, gusanos (*worm*), etc., por lo que se deben tomar precauciones para cuidarse.

Estimado lector, si te solicitan tu información personal, exige la justificación para obtenerla, y el destino

que se dará a esa información, niégate a entregar la información si no te satisface la explicación.

Adultos y niños deben respetar el derecho a la protección de datos personales de los demás, absteniéndose u omitiendo dar, informar, proporcionar, publicar, suministrar, o tratar información personal de terceros, sin su consentimiento.

Recuerda cuidar tus datos personales, antes de facilitar algún dato personal lee en forma cuidadosa la información sobre privacidad.

Orientación

En nuestro país, para ampliar la información o recibir cualquier asesoría relacionada con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares o su reglamento, se solicita ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), vía postal a Av. Insurgentes Sur #3211, Colonia Insurgentes Cuicuilco, Delegación Coyoacán, en la Ciudad de México, Código Postal 04530, o vía correo electrónico a la dirección «atención@ifai.org.mx», o vía web en la dirección de Internet «inicio.ifai.org.mx/», dirigiéndose a su Centro de Atención a la Sociedad (CAS), o también, vía telefónica dentro del horario de 09:00 a 18:00 horas de lunes a jueves, viernes de 09:00 a 15:00 horas, marcando al 01 800 8354324.

Agradecimiento

Finalizamos esta introducción expresando nuestra gratitud a los estimados lectores interesados en este libro.

Jaime Cortés González

Sonia del Carmen Álvarez Cisneros

Diccionario de derecho mexicano a la protección de datos personales en posesión de los particulares

A

Acceso a los datos por cuenta de terceros; España

Es uno de los principios de la protección de datos personales, en la ley de referencia, que consiste en lo siguiente:

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta ley que el encargado del tratamiento está obligado a implementar.

3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

Referencia: artículo 12, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Acceso a los datos personales en sitio

Cuando el acceso a los datos personales sea en sitio, el responsable deberá determinar el periodo durante el cual el titular podrá presentarse a consultarlos, mismo que no podrá ser menor a quince días. Transcurrido ese plazo, sin que el titular haya acudido a tener acceso a sus datos personales, será necesaria la presentación de una nueva solicitud.

Referencia: artículo 99, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Acciones para la seguridad de los datos personales

A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:

I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;

II. Determinar las funciones y obligaciones de las personas que traten datos personales;

III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;

IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;

V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;

VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;

VII. Llevar a cabo revisiones o auditorías;

VIII. Capacitar al personal que efectúe el tratamiento, y

IX. Realizar un registro de los medios de almacenamiento de los datos personales.

El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.

Referencia: artículo 61, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Acta de verificación

Las visitas de verificación concluirán con el levantamiento del acta correspondiente, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de verificación. Dicha acta se levantará en presencia de dos testigos propuestos por la persona con quien se hubiera entendido la diligencia o por quien la practique si aquélla se hubiera negado a proponerlos.

El acta que se emita por duplicado será firmada por el personal verificador actuante y por el responsable,

encargado o con quien se haya entendido la actuación, quien podrá manifestar lo que a su derecho convenga.

En caso de que el verificado se niegue a firmar el acta, se hará constar expresamente esta circunstancia en la misma. Dicha negativa no afectará la validez de las actuaciones o de la propia acta. La firma del verificado no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al verificado uno de los originales del acta de verificación, incorporándose el otro a las actuaciones.

Referencia: artículo 135, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Actualizaciones de las medidas de seguridad

Los responsables deberán actualizar la relación de las medidas de seguridad, cuando ocurran los siguientes eventos:

I. Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable;

II. Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo;

III. Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 del presente Reglamento, o

IV. Exista una afectación a los datos personales distinta a las anteriores.

En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes una vez al año.

Referencia: artículo 62, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Acuerdo de admisión

En su caso, el Instituto deberá acordar la admisión de la solicitud de protección de derechos en un plazo no mayor a diez días a partir de su recepción.

Acordada la admisión, el Instituto notificará la misma al promovente y correrá traslado al responsable, en un plazo no mayor a diez días, anexando copia de todos los documentos que el titular hubiere aportado, a efecto de que manifieste lo que a su derecho convenga en un plazo de quince días a partir de la notificación, debiendo ofrecer las pruebas que considere pertinentes.

Referencia: artículo 117, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Admisión o desechamiento de las pruebas

El Instituto dictará un acuerdo de admisión o desechamiento de las pruebas, y de ser necesario éstas serán desahogadas en una audiencia, de la cual se notificará el lugar o medio, la fecha y hora a las partes.

Referencia: artículo 118, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Admisión o desechamiento de las pruebas

Al ofrecimiento de pruebas del presunto infractor, deberá recaer un acuerdo de admisión o desechamiento de las mismas, y se procederá a su desahogo.

De ser necesario, se determinará lugar, fecha y hora para el desahogo de pruebas, que por su naturaleza así lo requieran. Se levantará un acta de la celebración de la audiencia y del desahogo de las pruebas.

Referencia: artículo 142, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Alcance. (De las medidas de seguridad en el tratamiento de datos personales)

El responsable y, en su caso, el encargado deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales, con arreglo a lo dispuesto en la Ley y el presente Capítulo, con independencia del sistema de tratamiento. Se entenderá por medidas de seguridad para los efectos del presente Capítulo, el control o grupo de controles de seguridad para proteger los datos personales.

Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes en materia de seguridad emitidas por las autoridades competentes al sector que corresponda, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.

Referencia: artículo 57, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Alcance. (De las transferencias de datos personales)

La transferencia implica la comunicación de datos personales dentro o fuera del territorio nacional, realizada a persona distinta del titular, del responsable o del encargado.

Referencia: artículo 67, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Algunas formas de ataque a los datos personales en internet

A través de las nuevas tecnologías, al usar internet y las redes sociales asimismo en el consumo de datos en la web o red informática, en la actualidad existen diferentes formas de ataque a los datos personales, que

en su mayoría tienen por objetivo robar información, para después usarla con fines publicitarios o con fines delictivos, destacan las formas de ataque a los datos personales con las denominaciones siguientes:

- o *Phishing*
- o Virus
- o *Pharming*
- o Troyanos
- o *Keyloggers*
- o *Sidejacking*
- o Gusanos(*worm*)

El *phishing*, es un término del ámbito de la informática que se usa para denominar un tipo de ilícito dentro del área de los fraudes o estafas. En el *phishing*, la finalidad del atacante es conseguir una contraseña o información sobre tarjetas de crédito u otros datos bancarios o financieros. El estafador o *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, mediante un correo electrónico o algún sistema de mensajería instantánea o a través de llamadas telefónicas, por lo común este tipo de engaño se realiza mediante un correo electrónico, que aparentan provenir de un comercio legítimo para dirigir al incauto a un sitio web no autorizado, en donde a través de mentiras se instruye al ingenuo a proporcionar información personal, de manera que el sitio web que ha obtenido acceso de forma no autorizada puede robar la información personal facilitada por la víctima engañada así para proporcionar sus datos de carácter personal al atacante para darles mal uso.

Existe otra forma de phishing, denominado tabjacking que opera sobre las pestañas de los navegadores web, espera a que pase un tiempo de inactividad sobre una pestaña que se queda abierta y cambia ésta, más

el icono, por otra página falsa con apariencia de la web que se está utilizando como Facebook, Twitter, Gmail, etc. En esta mientras el usuario está concentrado en otro sitio web un código escrito en JavaScript detecta ese intervalo entonces cambia el ícono luego cambia el contenido por uno de otro sitio, con la intención de robar información confidencial del usuario. El sitio cambia, pero se ve idéntico a uno popular que el usuario seguramente usa. Así, el usuario no se da cuenta que el sitio donde continúa navegando no es ya el original, que está siendo utilizado por el atacante.

Los virus informáticos, conocidos como una forma de código malicioso o *malware*, tienen por finalidad alterar el normal funcionamiento de una computadora, sin el permiso o el conocimiento del usuario; remplazan ciertos archivos por otros infectados con un código que destruye los datos almacenados en una computadora o perturba su funcionamiento; la finalidad puede ser desde una broma hasta causar daños importantes en los sistemas, o incluso bloquear redes informáticas.

Pharming, es una ilicitud que consiste en cambiar la dirección de dominio de un sitio, para pasarla a otra máquina. De esta manera, el autor del ilícito hace creer al usuario que el sitio web visitado es el original, pero en realidad es una copia. El usuario proporciona información personal, pensando que es una página web de confianza, y sus datos se dirigen a otras máquinas. Se recomienda que si se va a proporcionar información personal en un sitio, es conveniente comprobar la dirección electrónica, ingresando mejor desde la barra de direcciones del navegador y no desde un enlace.

En otras palabras, es un término del ámbito de la informática que se refiere a una explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*) o en el de los equipos

de los propios usuarios, que permite a un atacante redireccionar en forma malintencionada al usuario a un sitio web falso o fraudulento aunque tenga apariencia idéntica al verdadero. También se le denomina secuestro o envenenamiento del DNS.

Los troyanos, diseñados para permitir a un individuo el acceso remoto a un sistema o equipo; es un archivo que se introduce en un equipo de cómputo y se puede manejar desde otro. Para ello, se presenta como un programa legítimo e inofensivo. Un troyano puede estar ejecutándose en una computadora durante meses sin que el usuario perciba nada.

Algunas de las operaciones que se pueden llevar a cabo desde la máquina en la que se aloja son:

- realizar ataques de denegación de servicio o envío de spam o correo basura;
- instalar otros programas, incluyendo otros programas maliciosos;
- robar información personal: datos de las cuentas bancarias, contraseñas, códigos de seguridad;
- borrar o transferir archivos.

En otras palabras, es un término del ámbito de la informática conocido como una forma de código malicioso o malware, es un tipo de virus que consiste en un programa que aparenta ser inofensivo y útil, pero una vez instalado realiza determinadas acciones que afecta la confidencialidad y privacidad del usuario afectado.

Los *keyloggers*, son programas que se introducen en un equipo de cómputo y registran las pulsaciones que se realizan en el teclado; enseguida, las graban en un archivo y las envían a través internet. De esta forma, otros usuarios acceden a contraseñas, números de una tarjeta de crédito u otro tipo de información personal de manera ilícita.

En otras palabras, es un término del ámbito de la informática que se refiere a un tipo de software que registra cada tecla que presionamos en el teclado, para con posterioridad guardarlas en un archivo y/o enviarlas a través de internet; las aplicaciones que realizan *keylogging* pueden ser distribuidas a través de un troyano o como parte de un virus o gusano informático.

El *sidejacker*, espía y copia la información contenida en las cookies de una máquina conectada a la misma red, y así accede a las cuentas de la víctima. Esta modalidad de ciberataque es frecuente en lugares públicos en donde hay redes wifi, que comparten la misma conexión a internet. Al compartir la red, el atacante se introduce en la computadora de la víctima, toma posesión de sus cookies y así accede a información sobre cuentas, claves, etcétera.

En otras palabras, es un término del ámbito de la informática que consiste en que el atacante escanea y reemplaza las cookies de la víctima con otro sitio web, suplantando así la identidad; el usuario sigue usando su sesión sin darse cuenta de que otra persona en otro equipo de cómputo está también usando la misma.

Los gusanos, (*worm*), se presentan como un programa en apariencia legítimo e inofensivo, pero al ejecutarlos ocasionan los daños. Los gusanos se instalan cuando el usuario descarga programas o aplicaciones de fuentes inseguras.

En otras palabras, es un término del ámbito de la informática conocido como una forma de código malicioso o malware, variante de los virus, que tiene la propiedad de duplicarse así mismo, consiste en un programa semejante a un virus, que se diferencia de éste en el modo en que produce las infecciones, los gusanos realizan copias de sí mismos, infectan otras computadoras y se propagan en la red en forma automática, con independencia de la acción humana.

Referencia: con amplitud cfr. Qués, María Elena, Datos personales y nuevas tecnologías, Argentina, Ed. Educ.ar. Ministerio de Educación Presidencia de la Nación, 2014, págs. 25-28.

Ámbito objetivo de aplicación

El presente Reglamento será de aplicación al tratamiento de datos personales que obren en soportes físicos o electrónicos, que hagan posible el acceso a los datos personales con arreglo a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.

No se aplicarán las disposiciones del presente Reglamento cuando para acceder a los datos personales, se requieran plazos o actividades desproporcionadas.

En términos del artículo 3, fracción V de la Ley, los datos personales podrán estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, concerniente a una persona física identificada o persona física identificable.

Referencia: artículo 3, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Ámbito territorial de aplicación

El presente reglamento será de aplicación obligatoria a todo tratamiento cuando:

I. Sea efectuado en un establecimiento del responsable ubicado en territorio mexicano;

II. Sea efectuado por un encargado con independencia de su ubicación, a nombre de un responsable establecido en territorio mexicano;

III. El responsable no esté establecido en territorio mexicano pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato

o en términos del derecho internacional, y

IV. El responsable no esté establecido en territorio mexicano y utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento. Para efectos de esta fracción, el responsable deberá proveer los medios que resulten necesarios para el efectivo cumplimiento de las obligaciones que impone la Ley, su Reglamento y demás disposiciones aplicables, derivado del tratamiento de datos personales. Para ello, podrá designar un representante o implementar el mecanismo que considere pertinente, siempre que a través del mismo se garantice que el responsable estará en posibilidades de cumplir de manera efectiva, en territorio mexicano, con las obligaciones que la normativa aplicable imponen a aquellas personas físicas o morales que tratan datos personales en México.

Cuando el responsable no se encuentre ubicado en territorio mexicano, pero el encargado lo esté, a este último le serán aplicables las disposiciones relativas a las medidas de seguridad contenidas en el Capítulo III del presente Reglamento.

En el caso de personas físicas, el establecimiento se entenderá como el local en donde se encuentre el principal asiento de sus negocios o el que utilicen para el desempeño de sus actividades o su casa habitación.

Tratándose de personas morales, el establecimiento se entenderá como el local en donde se encuentre la administración principal del negocio; si se trata de personas morales residentes en el extranjero, el local en donde se encuentre la administración principal del negocio en territorio mexicano, o en su defecto el que designen, o cualquier instalación estable que permita el ejercicio efectivo o real de una actividad.

Referencia: artículo 4, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Ampliación de los plazos

En términos del artículo 32, segundo párrafo de la Ley, en caso de que el responsable determine ampliar el plazo de respuesta a una solicitud para el ejercicio de los derechos ARCO o aquél para hacer efectiva la respuesta, éste deberá notificar al solicitante las causas que justificaron dicha ampliación, en cualquiera de los siguientes plazos:

I. En caso de ampliar los veinte días para comunicar la determinación adoptada sobre la procedencia de la solicitud, la justificación de la ampliación deberá notificarse dentro del mismo plazo contado a partir del día en que se recibió la solicitud, o

II. En caso de ampliar los quince días para hacer efectivo el ejercicio del derecho que corresponda, la justificación de la ampliación deberá notificarse dentro del mismo plazo contado a partir del día en que se notificó la procedencia de la solicitud.
Referencia: artículo 97, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Atenuación de sanciones

En términos de lo dispuesto en el artículo 65, fracción III de la Ley, en los casos en que ocurra una vulneración a la seguridad de los datos personales, el Instituto podrá tomar en consideración el cumplimiento de sus recomendaciones para determinar la atenuación de la sanción que corresponda.

Referencia: artículo 58, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Audiencia

Para los efectos del penúltimo párrafo del artículo 45 de la Ley, el Instituto determinará, en su caso, el lugar o medio, fecha y hora para la celebración de la audiencia, la cual podrá posponerse sólo por causa justificada. En dicha audiencia se desahogarán las pruebas que por su naturaleza así lo requieran y se levantará el acta correspondiente.

Referencia: artículo 121, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Autoridad controladora del fichero; Europa

Es la que define el Convenio de referencia, como la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

Referencia: artículo 2, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Autoridad de control; Europa

Es la que la Directiva de referencia, señala que:

1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la referida Directiva.

Autorización de la subcontratación

Cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el encargado, prevean que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el artículo anterior se entenderá como otorgada a través de lo estipulado en éstos.

En caso de que la subcontratación no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos a los que refiere el párrafo anterior, el encargado deberá obtener la autorización correspondiente del responsable previo a la subcontratación.

En ambos casos, se deberá observar lo previsto en el artículo anterior.

Referencia: artículo 55, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Autorización de la subcontratación

Cuando las cláusulas contractuales o los instrumentos jurídicos mediante los cuales se haya formalizado la relación entre el responsable y el encargado, prevean que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el artículo anterior se entenderá como otorgada a través de lo estipulado en éstos.

En caso de que la subcontratación no haya sido prevista en las cláusulas contractuales o en los instrumentos jurídicos a los que refiere el párrafo anterior, el encargado deberá obtener la autorización correspondiente del responsable previo a la subcontratación.

En ambos casos, se deberá observar lo previsto en el artículo anterior.

Referencia: artículo 55, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

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 la ley de referencia. *Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.*

Aviso de privacidad en formatos con espacio limitado

El responsable podrá poner a disposición del titular el aviso de privacidad en términos del artículo anterior, cuando obtenga los datos personales por medios impresos, siempre que el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de forma tal que los datos personales obtenidos también sean mínimos.

Referencia: artículo 28, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Aviso de privacidad para la obtención directa de los datos personales

En términos del artículo 17, fracción II de la Ley, cuando los datos personales sean obtenidos directamente del titular, el responsable deberá proporcionar de manera inmediata al menos la siguiente información:

- I. La identidad y domicilio del responsable;
- II. Las finalidades del tratamiento, y

III. Los mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad de conformidad con el artículo 26 del presente Reglamento.

La divulgación inmediata de la información antes señalada no exime al responsable de la obligación de proveer los mecanismos para que el titular conozca el contenido del aviso de privacidad, de conformidad con el artículo 26 del presente Reglamento.

Referencia: artículo 27, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Aviso de privacidad para obtención indirecta de datos personales

Cuando los datos personales sean obtenidos de manera indirecta del titular, el responsable deberá observar lo siguiente para la puesta a disposición del aviso de privacidad:

I. Cuando los datos personales sean tratados para una finalidad prevista en una transferencia consentida o se hayan obtenido de una fuente de acceso público, el aviso de privacidad se deberá dar a conocer en el primer contacto que se tenga con el titular, o

II. Cuando el responsable pretenda utilizar los datos para una finalidad distinta a la consentida, es decir, vaya a tener lugar un cambio de finalidad, el aviso de privacidad deberá darse a conocer previo el aprovechamiento de los mismos.

Referencia: artículo 29, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

B

Bases de datos

Es el conjunto ordenado de datos personales referentes a una persona identificada o identificable.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Bloqueo. (Ley)

Es la identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Bloqueo. (Reglamento)

De resultar procedente la cancelación, y sin perjuicio de lo establecido en el artículo 32 de la Ley, el responsable deberá:

I. Establecer un periodo de bloqueo con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas, y notificarlo

al titular o a su representante en la respuesta a la solicitud de cancelación, que se emita dentro del plazo de veinte días que establece el artículo 32 de la Ley;

II. Atender las medidas de seguridad adecuadas para el bloqueo;

III. Llevar a cabo el bloqueo en el plazo de quince días que establece el artículo 32 de la Ley, y

IV. Transcurrido el periodo de bloqueo, llevar a cabo la supresión correspondiente, bajo las medidas de seguridad previamente establecidas por el responsable.

Referencia: artículo 107, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

C

Calidad de los datos; España

Es uno de los principios de la protección de datos, que establece la ley de referencia, que consiste en lo siguiente:

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes

para la finalidad para la cual hubieran sido recabados o registrados. No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Referencia: artículo 4, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Calidad de los datos, del Convenio número 108 del Consejo de Europa

Es un principio básico para la protección de datos personales, del Convenio de referencia, que consiste en que todos los datos de carácter personal que sean objeto de un tratamiento automatizado:

- a) Se obtendrán y tratarán leal y legítimamente;
- b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;
- c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;
- d) serán exactos y si fuera necesario puestos al día;
- e) se conservarán bajo una forma que permita la

identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado. Referencia: artículo 5, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Características del aviso de privacidad

El aviso de privacidad deberá caracterizarse por ser sencillo, con información necesaria, expresado en lenguaje claro y comprensible, y con una estructura y diseño que facilite su entendimiento.

Referencia: artículo 24, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Características del consentimiento

La obtención del consentimiento tácito o expreso deberá ser:

I. Libre: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;

II. Específica: referida a una o varias finalidades determinadas que justifiquen el tratamiento, y

III. Informada: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

El consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.

Referencia: artículo 12, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Categoría de datos

Véase: Datos especialmente protegidos. (Principio general relativo a la protección de datos personales).

Categorías especiales de tratamientos; Europa

Es la disposición de la Directiva de referencia, que establece las condiciones generales para la licitud del tratamiento de datos personales, que consisten en lo siguiente:

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1 no se aplicará cuando:

a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o

b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política,

filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o

e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.

5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas

y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos.

Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.

6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.

7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Referencia: artículo 8, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Categorías particulares de datos; Europa

Es un principio básico para la protección de datos del Convenio de referencia, que consiste en que son los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el Derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.

Referencia: artículo 6, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Causales de procedencia

El procedimiento de protección de derechos procederá cuando exista una inconformidad por parte del titular, derivada de acciones u omisiones del responsable con motivo del ejercicio de los derechos ARCO cuando:

I. El titular no haya recibido respuesta por parte del responsable;

II. El responsable no otorgue acceso a los datos personales solicitados o lo haga en un formato incomprensible;

III. El responsable se niegue a efectuar las rectificaciones a los datos personales;

IV. El titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la solicitada, o bien, con el costo o modalidad de la reproducción;

V. El responsable se niegue a cancelar los datos personales;

VI. El responsable persista en el tratamiento a pesar de haber procedido la solicitud de oposición, o bien, se niegue a atender la solicitud de oposición, y

VII. Por otras causas que a juicio del Instituto sean procedentes conforme a la Ley o al presente Reglamento.

Referencia: artículo 115, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Causales de procedencia

El procedimiento de verificación se iniciará de oficio o a petición de parte, por instrucción del Pleno del Instituto.

Cualquier persona podrá denunciar ante el Instituto las presuntas violaciones a las disposiciones previstas

en la Ley y demás ordenamientos aplicables, siempre que no se ubiquen en los supuestos de procedencia del procedimiento de protección de derechos. En este caso, el Pleno determinará, de manera fundada y motivada, la procedencia de iniciar la verificación correspondiente.

Referencia: artículo 129, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Certificación en protección de datos personales

Los esquemas de autorregulación vinculante podrán incluir la certificación de los responsables en materia de protección de datos personales.

En caso de que el responsable decida someterse a un procedimiento de certificación, ésta deberá ser otorgada por una persona física o moral certificadora ajena al responsable, de conformidad con los criterios que para tal fin establezcan los parámetros a los que refiere el artículo 43, fracción V de la Ley.

Referencia: artículo 83, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Cesión o comunicación de datos

Véase: Comunicación de datos. (Principio general relativo a la protección de datos personales).

Cierre de instrucción y resolución

Desahogadas, en su caso, las pruebas, se notificará al presunto infractor que cuenta con cinco días para presentar alegatos, contados a partir del día siguiente de que surta efectos la notificación. Al término de dicho plazo se cerrará la instrucción y la resolución del Instituto deberá emitirse en un plazo no mayor de cincuenta días, siguientes a los que inició el procedimiento.

Cuando haya causa justificada, el Pleno del In-

stituto podrá ampliar por una vez y hasta por un período igual el plazo de cincuenta días al que refiere el párrafo anterior.

Referencia: artículo 143, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Comunicación de datos; España

Es uno de los principios de la protección de datos personales, en la ley de referencia, que consiste en lo siguiente:

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.
b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.

Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquél a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquél a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Referencia: artículo 11, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Condiciones específicas para las transferencias internacionales

Sin perjuicio de lo dispuesto en el artículo 37 de la Ley, las transferencias internacionales de datos personales serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponden al responsable que transfirió los datos personales.

Referencia: artículo 74, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Condiciones específicas para las transferencias nacionales

Para realizar una transferencia de datos personales dentro del territorio nacional será necesario que el responsable cumpla con lo previsto en los artículos 36 de la Ley y 68 del presente Reglamento.

Referencia: artículo 71, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Condiciones para la transferencia

Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en el artículo 37 de la Ley; deberá ser informada a este último mediante el aviso de privacidad y limitarse a la finalidad que la justifique.

Referencia: artículo 68, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Confidencialidad del tratamiento; Europa

Es la condición general para la licitud del tratamiento de datos personales, siguiente:

Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, solo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal.

Referencia: artículo 16, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Consentimiento

Es la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Consejos que pueden ser útiles para evitar el robo de tu identidad. (Suplantación de identidad)

«Sin conexión a internet (offline)

Para documentos de identificación

- Limite el número de documentos con información personal que traes contigo, procura tener sólo aquellos que vayas a utilizar.
- Ten copias de tus documentos importantes y mantenlos en un lugar seguro, podrán ser útiles en casa de que extravíes los originales.
- Mantén seguros tus documentos personales en tu casa y cuando viajes. En caso de ya no ser necesarios destruyelos.
- Antes de tirar a la basura revisa que no contenga

documentos con información personal, en caso de que así sea, destrúyelos por completo y verifica que no sea posible extraer información personal por parte de terceros.

Para información financiera

- Al acudir a un cajero automático llévate contigo los comprobantes de la operación, no los dejes en los botes de basura que se encuentran ahí.
- Revisa que el cajero automático no cuente con dispositivos extraños en el lector de tarjetas, de ser el caso, utiliza otro cajero automático.
- Cuando teclees tu NIP en el cajero electrónico, o cuando llenes algún tipo de formulario con información personal debes tener cuidado con las personas que se encuentran a tu alrededor.
- Evita proporcionar información personal o financiera por teléfono.
- Al pagar con tarjeta, no la pierdas de vista, solicita que te lleven la terminal al lugar donde te encuentres, por ejemplo, en restaurantes o gasolineras.
- Revisa constantemente tus estados de cuenta con la finalidad de que te cerciores que los cargos correspondan efectivamente a los que hayas realizado. Si detectas un error realiza la aclaración correspondiente lo antes posible.
- Si recibes una llamada telefónica de donde te solicitan teclear tus datos personales cuelga, las instituciones bancarias no solicitan información a través de este medio.
- Revisa constantemente tu reporte de crédito, a fin de detectar movimientos sospechosos.
- Suscríbete al servicio de ahorro de papel que ofrecen algunas instituciones financieras y compañías de servicios, para sustituir el envío en papel de tus estados de cuenta a tu domicilio, por el envío

de éstos a tu correo electrónico, disminuyendo con esto la circulación de tu información personal.

Para otros servicios

- Protege tu correspondencia utilizando un buzón con llave y recogiénola lo más pronto posible. Notifica de inmediato cualquier cambio de domicilio a los remitentes de la misma.
- Protege tus contraseñas, no las escribas o coloques en tu celular o en algún otro lugar que sea susceptible de ser visto por terceros.
- Si acudes a alguna institución o negocio para solicitar la cancelación de un servicio que no solicitaste, recuerda que podrás ejercer tus derechos de acceso, rectificación, cancelación y oposición, que prevén el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, las leyes de las entidades federativas en materia de transparencia o protección de datos personales, y demás normatividad en la materia.
- Haz caso omiso de los mensajes en los que te comunican que has ganado un premio o te hacen una oferta especial, al menos que tengas seguridad plena de la autenticidad de los mensajes.
- Antes que proporcionen información personal, solicita el aviso de privacidad o leyenda de información, para que puedas conocer quién utilizará tus datos personales, para qué fines, con quién se compartirán en su caso, cómo podrás ejercer tus derechos, entre otras características del tratamiento al que serán sometidos tus datos personales.

- No dejes documentos personales en tu auto cuando uses el servicio de valet parking
- Cuando te soliciten tus huellas dactilares, asegúrate de limpiar la superficie del equipo electrónico en el que las hayas puesto, a fin de que no quede su imagen expuesta y pueda ser retomada de manera indebida. Una técnica común y sencilla de “robar” huellas dactilares es pasar cinta adhesiva encima del equipo electrónico donde la persona proporcionó su huella, para copiar la imagen.

o Con conexión a Internet (online)

Para proteger tus cuentas y dispositivos electrónicos

- Evitar usar computadoras públicas para acceder a tu información personal, de ser necesario, recuerda limpiar el historial al terminar tu navegación. Si utilizas equipos públicos para acceder a internet, evita realizar operaciones en la banca en línea.
- Si requieres abrir una cuenta personal en una computadora de acceso público, asegúrate de cerrarla correctamente al concluir el uso del equipo.
- Si en el navegador aparece una ventana emergente que te recomienda recordar tus contraseñas, indica siempre la opción “NO”.
- Al terminar de usar el navegador, borra los datos del navegador: el historial de descargas y navegación, los datos de formularios almacenados, cookies, contraseñas y navegador y seleccionando la opción “Borrar datos de navegación”.
- Asegúrate de cambiar tus contraseñas y claves de acceso con regularidad. De ig-

ual forma, construye una contraseña segura, recuerda que se deben cumplir con un serie de requisitos, minúsculas, números, símbolos y distintos caracteres.

- Protege tu computadora, teléfono inteligente o Tablet con un software de seguridad (antivirus) y contraseñas seguras.
- Utiliza contraseñas para tus dispositivos móviles y computadora y no las compartas con terceros
- No permitas el acceso remoto a tu computadora.
- Protege la información personal de tu dispositivo, no te conectes a redes inalámbricas que no tengan contraseñas.
- Descarga aplicaciones de tiendas oficiales y de desarrolladores confiables.
- Evita almacenar cantidades excesivas de datos personales sin cifrar en un dispositivo móvil, tales como nombres de usuario, palabras clave, información crediticia o de identificación personal, para evitar que tus datos sean interceptados si el dispositivo es extraviado.
- Antes de que dejes de utilizar, vendas o deseches tus dispositivos electrónicos, asegúrate de borrar tu información personal y restaurar la configuración de fábrica.

En redes sociales

- Utiliza distintas contraseñas y nombres de usuario para diferentes sitios.
- Antes de crear una cuenta en alguna red social asegúrate de haber leído sus políticas de privacidad.
- Configura la privacidad de tus redes sociales, no aceptes cualquier solicitud de amistad a

menos que te encuentres seguro de conocer de forma personal a quien te la envía.

- Piensa antes de publicar información personal.
- No compartas más información de la necesaria en redes sociales, e igual forma configura niveles de privacidad entre tus contactos.

Al navegar en internet

- Evita intercambiar información personal o contraseñas en sitios no seguros.
- Ten cuidado de las ofertas que se publican en internet que son demasiado buenas para ser reales.
- No des click en links o vínculos que descarguen archivos y cierra las ventanas emergentes que puedan abrirse al navegar.
- No abras archivos adjuntos de un correo electrónico que provenga de un remitente desconocido.
- Sé cuidadoso de la información que compartes en línea, verifica que tu información personal sea utilizada para propósitos legítimos.
- Instala en tu computadora paquetes de seguridad que te protejan contra amenazas tecnológicas y mantenlos actualizados.
- No proporciones información personal por correo electrónico ni por internet, a menos que tengas certeza que el sitio sea legítimo.
- Revisa las políticas de privacidad de los sitios que visitas para conocer el uso que se le dará a la información que proporcionas.

Al hacer uso de datos financieros.

- Siempre que se ingrese al portal de un banco o realices alguna compra en línea en donde te sean solicitados datos de tus tarjetas, verifica que la dirección que aparece en la barra del

explorador empiece con HTTPS, ya que la “S” significa que se trata de una página segura.

- No respondas correos electrónicos o mensajes emergentes en los que te soliciten información personal o financiera, ni hagas click en los hipervínculos.
- Haz caso omiso de los correos en los que te soliciten actualizar tus datos bancarios.
- En caso de recibir una notificación por correo electrónico en la que te informen que tu cuenta fue bloqueada reporta esta situación al banco mediante la línea de atención telefónica, y no a través de los teléfonos que en dicha notificación hayas recibido.
- Nunca reveles el número de tu tarjeta de crédito o el código de seguridad de la misma como respuesta a un mensaje que sospeches que es spam.
- Revisa los estados de cuenta bancarios regularmente para asegurar que no hay cargos extraños en la cuenta [sic]».

Referencia: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Guía para prevenir el robo de identidad, México, INAI, 2016, págs. 10-13.

Consentimiento del afectado; España

Es uno de los principios de la protección de datos personales, en la ley de referencia, que consiste en lo siguiente:

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejerci-

cio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7 apartado 6 de la referida ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Referencia: artículo 6, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Consentimiento del interesado, de la Directiva 95/46/CE; Europa

Es toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.

Referencia: artículo 2, de la Directiva 95/46/CE del

Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Consentimiento del interesado, de la Ley Orgánica 15/1999; España

Se entiende como toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Referencia: artículo 3, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Consentimiento escrito

Se considerará que el consentimiento expreso se otorgó por escrito cuando el titular lo externe mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por la normativa aplicable. Tratándose del entorno digital, podrán utilizarse firma electrónica o cualquier mecanismo o procedimiento que al efecto se establezca y permita identificar al titular y recabar su consentimiento.

Referencia: artículo 19, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Consentimiento expreso

El responsable deberá obtener el consentimiento expreso del titular cuando:

- I. Lo exija una ley o reglamento;
- II. Se trate de datos financieros o patrimoniales;
- III. Se trate de datos sensibles;
- IV. Lo solicite el responsable para acreditar el mismo, o
- V. Lo acuerden así el titular y el responsable.

Referencia: artículo 15, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Consentimiento tácito

Salvo que la Ley exija el consentimiento expreso del titular, será válido el consentimiento tácito como regla general, conforme a lo dispuesto en los artículos 11 y 12 del presente Reglamento.
Referencia: artículo 13, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Consentimiento verbal

Se considera que el consentimiento expreso se otorgó verbalmente cuando el titular lo externa oralmente de manera presencial o mediante el uso de cualquier tecnología que permita la interlocución oral.
Referencia: artículo 18, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Conciliación

Admitida la solicitud y sin perjuicio de lo dispuesto por el artículo 54 de la Ley, el Instituto promoverá la conciliación entre las partes, de conformidad con el siguiente procedimiento:

I. En el acuerdo de admisión de la solicitud de protección de derechos, el Instituto requerirá a las partes que manifiesten, por cualquier medio, su voluntad de conciliar, en un plazo no mayor a diez días, contados a partir de la notificación de dicho acuerdo, mismo que contendrá un resumen de la solicitud de protección de datos personales y de la respuesta del responsable si la hubiere, señalando los elementos comunes y los puntos de controversia.

La conciliación podrá celebrarse presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el Instituto. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.

Queda exceptuado de la etapa de conciliación, cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con la Ley y el presente Reglamento, salvo que cuente con representación legal debidamente acreditada;

II. Aceptada la posibilidad de conciliar por las partes, el Instituto señalará el lugar o medio, día y hora para la celebración de una audiencia de conciliación, la cual deberá realizarse dentro de los veinte días siguientes en que el Instituto haya recibido la manifestación de la voluntad de conciliar de las partes, en la que se procurará avenir los intereses entre el titular y el responsable.

El conciliador podrá, en todo momento en la etapa de conciliación, requerir a las partes que presenten en un plazo máximo de cinco días, los elementos de convicción que estime necesarios para la conciliación.

El conciliador podrá suspender cuando lo estime pertinente o a instancia de ambas partes la audiencia de conciliación hasta en dos ocasiones. En caso de que se suspenda la audiencia, el conciliador señalará día y hora para su reanudación.

De toda audiencia de conciliación se levantará el acta respectiva, en la que conste el resultado de la misma. En caso de que el responsable o el titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa;

III. Si alguna de las partes no acude a la audiencia de conciliación y justifica su ausencia en un plazo de tres días, será convocado a una segunda audiencia de conciliación; en caso de que no acuda a esta última, se continuará con el procedimiento de protección de derechos. Cuando alguna de las partes no acuda a la audiencia de conciliación sin justificación alguna, se continuará con el procedimiento;

IV. De no existir acuerdo en la audiencia de conciliación, se continuará con el procedimiento de protección de derechos;

V. En caso de que en la audiencia se logre la conciliación, el acuerdo deberá constar por escrito y tendrá efectos vinculantes y señalará, en su caso, el plazo de su cumplimiento, y

VI. El cumplimiento del acuerdo dará por concluido el procedimiento de protección de derechos, en caso contrario, el Instituto reanudará el procedimiento.

El plazo al que se refiere el artículo 47 de la Ley será suspendido durante el periodo de cumplimiento del acuerdo de conciliación.

El procedimiento establecido en el presente artículo no obsta para que, en términos del artículo 54 de la Ley, el Instituto pueda buscar la conciliación en cualquier momento del procedimiento de protección de derechos.

Referencia: artículo 120, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Contenido de las actas de verificación

En las actas de verificación se hará constar:

I. Nombre, denominación o razón social del verificado;

II. Hora, día, mes y año en que se inicie y concluya la verificación;

III. Los datos que identifiquen plenamente el domicilio, tales como calle, número, población o colonia, municipio o delegación, código postal y entidad federativa en que se encuentre ubicado el lugar en que se practique la verificación, así como número telefónico u otra forma de comunicación disponible con el verificado;

IV. Número y fecha del oficio de comisión que la motivó;

V. Nombre y cargo de la persona con quien se entendió la verificación;

VI. Nombre y domicilio de las personas que fungieron como testigos;

VII. Datos relativos a la actuación;

VIII. Declaración del verificado, si quisiera hacerla, y

IX. Nombre y firma de quienes intervinieron en la verificación, incluyendo los de quienes la hubieran llevado a cabo. Si se negara a firmar el verificado, su representante legal o la persona con quien se entendió la verificación, ello no afectará la validez del acta, debiendo el personal verificador asentar la razón relativa.

Los verificados a quienes se haya levantado acta de verificación, podrán formular observaciones en el acto de la verificación y manifestar lo que a su derecho convenga en relación a los hechos contenidos en ella, o bien, por escrito dentro del término de los cinco días siguientes a la fecha en que se hubiere levantado. *Referencia: artículo 136, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.*

Contenido mínimo de los esquemas de autorregulación

Los esquemas de autorregulación deberán considerar los parámetros que emita la Secretaría, en coadyuvancia con el Instituto, para el correcto desarrollo de este tipo de mecanismos y medidas de autorregulación, considerando al menos lo siguiente:

I. El tipo de esquema convenido, que podrá constituirse en códigos deontológicos, código de buena práctica profesional, sellos de confianza, u otros que posibilite a los titulares identificar a los responsables comprometidos con la protección de sus datos personales;

II. Ámbito de aplicación de los esquemas de autorregulación;

III. Los procedimientos o mecanismos que se emplearán para hacer eficaz la protección de datos personales por parte de los adheridos, así como para medir la eficacia;

IV. Sistemas de supervisión y vigilancia internos y externos;

V. Programas de capacitación para quienes traten los datos personales;

VI. Los mecanismos para facilitar los derechos de los titulares de los datos personales;

VII. La identificación de las personas físicas o morales adheridas, que posibilite reconocer a los responsables que satisfacen los requisitos exigidos por determinado esquema de autorregulación y que se encuentran comprometidos con la protección de los datos personales que poseen, y

VIII. Las medidas correctivas eficaces en caso de incumplimiento.

Referencia: artículo 82, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Es el Convenio celebrado por los representantes de los países miembros, conformado en su totalidad por veintisiete artículos, distribuidos en siete capítulos; es importante porque fue la primera norma para Europa que marcó el modelo común en materia de la protección de datos personales, y que posteriormente sobre la base de los principios básicos que aportó en su capítulo II, fue aprobada la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que sentó las bases para la coordinación de las legislaciones nacionales.

Referencia: Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Costos

El ejercicio de los derechos ARCO será sencillo y gratuito, debiendo cubrir el titular únicamente los gastos de envío, reproducción y, en su caso, certificación de documentos, salvo la excepción prevista en el segundo párrafo del artículo 35 de la Ley.

Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente.

Criterio de minimización

El responsable deberá realizar esfuerzos razonables para que los datos personales tratados sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.

Referencia: artículo 46, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

D

Datos; Europa

Se define como los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario.

Referencia: artículo 2, de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006.

Datos de carácter personal, del Convenio número 108 del Consejo de Europa

Es cualquier información relativa a una persona física identificada o identificable («persona concernida»). *Referencia: artículo 2, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.*

Datos especialmente protegidos; España

Es uno de los principios de la protección de datos personales, en la ley de referencia, que consiste en lo siguiente:

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito

del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios san-

itarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Referencia: artículo 7, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Datos personales

Es cualquier información concerniente a una persona física identificada o identificable.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Datos personales sensibles

Son aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Datos personales; Europa

Es toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. *Referencia: artículo 2, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

Deber de confidencialidad

Véase: Deber de secreto. (Principio general relativo a la protección de datos personales).

Deber de secreto; España

Es uno de los principios de la protección de datos personales, en la ley de referencia, que consiste en lo siguiente:

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Referencia: artículo 10, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Delitos en materia del tratamiento indebido de datos personales.

Véase: México; delitos en materia del tratamiento indebido de datos personales.

Dependencias. (Definiciones)

Se entenderá por dependencias, las señaladas en el artículo 26 de la Ley Orgánica de la Administración Pública Federal.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Derecho a indemnización; España

Es uno de los derechos de las personas, en la ley de referencia, que consiste en lo siguiente:

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones Públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

Referencia: artículo 19, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Derecho a la autodeterminación informativa

Véase: Derecho a la protección de datos personales.

Derecho a la intimidad informática

Véase: Derecho a la protección de datos personales.

Derecho a la protección de datos personales

Es un derecho autónomo, es el derecho que otorga a toda persona una protección contra el posible mal uso de la información de carácter personal que le concierne, que en esencia consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede recabar este tercero, es parte del patrimonio de toda persona la cual tiene derecho a saber quién tiene esos datos, qué se está haciendo con ellos y para qué se están utilizando, pudiendo oponerse a esa posesión o uso; en otras palabras, es el derecho que otorga a toda persona una protección contra la posible utilización de sus datos personales por parte de terceros, sin su autorización, para confeccionar una información que, identificable con él, lo afecte en su entorno personal, social o profesional, en los límites de su intimidad; también denominado «derecho a la autodeterminación informativa» o «derecho a la intimidad informática».

Referencia: artículo 16, párrafo 2º de la Constitución Política de los Estados Unidos Mexicanos. México.

Derecho de acceso, de la Directiva 95/46/CE; Europa

Es la condición general para la licitud del tratamiento de datos personales, de la Directiva de referencia, siguiente:

Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:

a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos:

- la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos;

- la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos;

- el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15;

b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos;

c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado.
Referencia: artículo 12, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Derecho de acceso, de la Ley Orgánica 15/1999; España

Es uno de los derechos de las personas, en la ley de referencia, que consiste en lo siguiente:

responsable que rectifique sus datos personales que resulten ser inexactos o incompletos.

Referencia: artículo 103, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Derecho de rectificación y cancelación; España

Es uno de los derechos de las personas, en la ley de referencia, que consiste en lo siguiente:

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones Públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las dis-

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes.

Referencia: artículo 15, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Derecho de acceso

El titular, en términos de lo dispuesto por el artículo 23 de la Ley, tiene derecho a obtener del responsable sus datos personales, así como información relativa a las condiciones y generalidades del tratamiento.

Referencia: artículo 101, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Derecho de cancelación

En términos del artículo 25 de la Ley, la cancelación implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de los mismos y su posterior supresión.

Referencia: artículo 105, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Derecho de consulta al registro general de protección de datos; España

Es uno de los derechos de las personas, en la ley de referencia, que consiste en lo siguiente:

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Referencia: artículo 14, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Derecho de información en la recogida de datos; España

Es uno de los principios de la protección de datos personales, en la ley de referencia, que consiste en lo siguiente:

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de tránsito, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos despro-

porcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Referencia: artículo 5, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Derecho de oposición del interesado; Europa

Es la condición general para la licitud del tratamiento de datos personales, que establece la Directiva de referencia, que consiste en lo siguiente:

Los Estados miembros reconocerán al interesado el derecho a:

a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;

b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o

ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización.

Referencia: artículo 14, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Derecho de oposición

En términos del artículo 27 de la Ley, el titular podrá, en todo momento, oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando:

I. Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un perjuicio al titular, o

II. Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable.

Referencia: artículo 109, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Derecho de rectificación

De conformidad con lo dispuesto por el artículo 24 de la Ley, el titular podrá solicitar en todo momento al

posiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Referencia: artículo 16, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Derecho fundamental a la protección de datos personales

Véase: Derecho a la protección de datos personales.

Derechos “ARCO”. (Definiciones)

Son los derechos de acceso, rectificación, cancelación y oposición.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Desarrollo de la verificación

El procedimiento de verificación tendrá una duración máxima de ciento ochenta días, este plazo comenzará a contar a partir de la fecha en que el Pleno hubiera dictado el acuerdo de inicio y concluirá con la determinación del mismo, el cual no excederá de ciento ochenta días. El Pleno del Instituto podrá ampliar por una vez y hasta por un periodo igual este plazo.

El Instituto podrá realizar diversas visitas de verificaciones para allegarse de los elementos de convicción necesarios, las cuales se desarrollarán en un plazo máximo de diez días cada una. Este plazo deberá ser notificado al responsable o encargado y, en su caso, al denunciante.

Referencia: artículo 132, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Destinatario; Europa

Es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios.

Referencia: artículo 2, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Día internacional de la protección de datos

El día 28 de enero de cada año, a partir del año 2006, se conmemora el día internacional de la protección de datos.

Referencia: Conmemoración creada por el Consejo de Europa y la Comisión Europea, conjuntamente, el 26 de abril de 2006, con motivo del aniversario de la Convención para la protección de los individuos con respecto al procesamiento automático de datos personales (ETS 108) mejor conocido como el «Convenio 108».

Diferenciación de finalidades

El responsable identificará y distinguirá en el aviso de privacidad entre las finalidades que dieron origen y son necesarias para la relación jurídica entre el responsable y el titular, de aquéllas que no lo son.

Referencia: artículo 41, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995

Es la relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos; se constituye de 72 consideraciones, y 34 artículos; misma Directiva de referencia, que establece en su primer artículo que tiene por objeto:

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.
Referencia: Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Directiva 2006/24/CE; Europa

Es del Parlamento Europeo y del Consejo de 15 de marzo de 2006; sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE; misma suscrita en Estrasburgo el 15 de marzo de 2006, constituida por 17 artículos; misma que en su primer artículo establece su objeto y ámbito, siguiente:

1. La presente Directiva se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles, con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

2. La presente Directiva se aplicara a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Referencia: Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006.

Disociación

Es el procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Disociación de datos

Véase: Procedimiento de disociación.

Domicilio del titular

En la solicitud de acceso, para los efectos del artículo 29, fracción I de la Ley, se deberá indicar el domicilio o cualquier otro medio para que sea notificada la respuesta. En caso de no cumplir con este requisito,

el responsable tendrá por no presentada la solicitud, dejando constancia de ello.

Referencia: artículo 94, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

E

Ejercicio de los derechos

El ejercicio de cualquiera de los derechos ARCO no excluye la posibilidad de ejercer alguno de los otros, ni puede constituir requisito previo para el ejercicio de cualquiera de estos derechos.

Referencia: artículo 87, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Ejercicio del derecho de cancelación

El titular podrá solicitar en todo momento al responsable la cancelación de los datos personales cuando considere que los mismos no están siendo tratados conforme a los principios y deberes que establece la Ley y el presente Reglamento.

La cancelación procederá respecto de la totalidad de los datos personales del titular contenidos en una base de datos, o sólo parte de ellos, según lo haya solicitado.

Referencia: artículo 106, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Elementos del aviso de privacidad

El aviso de privacidad deberá contener los elementos a que se refieren los artículos 8, 15, 16, 33 y 36 de la Ley, así como los que se establezcan en los lineamientos a que se refiere el artículo 43, fracción III de la Ley.

Referencia: artículo 26, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Emisión de regulación secundaria. (De la coordinación entre autoridades)

Cuando la dependencia competente, atendiendo a las necesidades que advierta sobre el sector que regule, determine la necesidad de normar el tratamiento de datos personales en posesión de los particulares podrá, en el ámbito de sus competencias, emitir o modificar regulación específica, en coadyuvancia con el Instituto.

Asimismo, cuando el Instituto derivado del ejercicio de sus atribuciones advierta la necesidad de emitir o modificar regulación específica para normar el tratamiento de datos personales en un sector o actividad determinada, podrá proponer a la dependencia competente la elaboración de un anteproyecto.
Referencia: artículo 77, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Encargado

Es la persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Encargado del tratamiento, de la Directiva 95/46/CE; Europa

Es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Referencia: artículo 2, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Entorno digital. (Definiciones)

Es el ámbito conformado por la conjunción de hardware, software, redes, aplicaciones, servicios o cualquier otra tecnología de la sociedad de la información que permiten el intercambio o procesamiento informatizado o digitalizado de datos.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

España; Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal

Es parte de la legislación del país de España, compuesta de 49 artículos, 6 disposiciones adicionales, 3 disposiciones transitorias, una disposición derogatoria y 3 disposiciones finales; la cual tiene por objeto conforme a su artículo 1, garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Referencia: Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Estafa, fraude, hurto, phishing, plagio, robo, suplantación o usurpación de identidad. Véase: Suplantación de identidad.

Excepción y restricciones; Europa

Es un principio básico para la protección de datos personales del Convenio de referencia, que se refiere

a que no se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del Convenio de referencia, salvo que sea dentro de los límites que se definen en el propio artículo 9 del Convenio número 108 del Consejo de Europa). Por otra parte que sólo será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del Convenio número 108 del Consejo de Europa, cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;

b) para la protección de la persona concernida y de los derechos y libertades de otras personas. Así también podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 del Convenio número 108 del Consejo de Europa, para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Referencia: artículo 9, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Excepciones a los derechos de acceso, rectificación y cancelación; España

Es una disposición sectorial de los ficheros de titularidad pública, en la ley de referencia, que consiste en lo siguiente:

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspeccionadoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del Organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones Tributarias Autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Referencia: artículo 23, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Excepciones al principio del consentimiento

En términos de lo dispuesto por los artículos 10, fracción IV y 37, fracción VII de la Ley, no se requerirá el consentimiento tácito o expreso para el tratamiento de los datos personales cuando éstos deriven de una

relación jurídica entre el titular y el responsable.

No resulta aplicable lo establecido en el párrafo anterior cuando el tratamiento de datos personales sea para finalidades distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular. En ese caso, para la obtención del consentimiento tácito, el responsable deberá observar lo dispuesto en los artículos 8, tercer párrafo de la Ley y 11, 12 y 13 del presente Reglamento, y tratándose de datos sensibles, financieros y patrimoniales, deberá obtener el consentimiento expreso, o bien, expreso y por escrito, según lo exija la Ley.

Referencia: artículo 17, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Excepciones en la transferencia de datos personales a países terceros; Europa

Es la disposición de la Directiva de referencia, que establece:

1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:

a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por

celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.

3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.

En el supuesto de que otro Estado miembro o la Comisión expresaron su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fun-

damentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.

Referencia: artículo 26, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

F

Factores para determinar las medidas de seguridad

El responsable determinará las medidas de seguridad aplicables a los datos personales que trate, considerando los siguientes factores:

- I. El riesgo inherente por tipo de dato personal;
- II. La sensibilidad de los datos personales tratados;
- III. El desarrollo tecnológico, y
- IV. Las posibles consecuencias de una vulneración para los titulares.

De manera adicional, el responsable procurará tomar en cuenta los siguientes elementos:

- I. El número de titulares;
- II. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento;
- III. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
- IV. Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable.

Referencia: artículo 60, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Falta de respuesta

En caso de que el procedimiento se inicie por falta de respuesta del responsable a una solicitud de ejercicio

de los derechos ARCO, el Instituto correrá traslado al responsable para que, en su caso, acredite haber dado respuesta a la misma, o bien, a falta de ésta, emita la respuesta correspondiente y la notifique al titular con copia al Instituto, en un plazo de diez días contados a partir de la notificación.

En caso de que el responsable acredite haber dado respuesta a la solicitud de ejercicio de derechos en tiempo y forma, y haberla notificado al titular o su representante, el procedimiento de protección de derechos será sobreseído por quedar sin materia, de conformidad con lo previsto en el artículo 53, fracción IV de la Ley.

Cuando el responsable acredite haber dado respuesta a la solicitud de ejercicio de derechos en tiempo y forma, y la solicitud de protección de derechos no haya sido presentada por el titular en el plazo que establece la Ley y el presente Reglamento, el procedimiento de protección de derechos se sobreseerá por extemporáneo, de conformidad con lo previsto en el artículo 53, fracción III de la Ley, en relación con el artículo 52, fracción V del mismo ordenamiento.

En caso de que la respuesta sea emitida por el responsable durante el procedimiento de protección de derechos o hubiere sido emitida fuera del plazo establecido por el artículo 32 de la Ley, el responsable notificará dicha respuesta al Instituto y al titular, para que este último, en un plazo de quince días contados a partir de la notificación, manifieste lo que a su derecho convenga, a efecto de continuar el curso del procedimiento. Si el titular manifiesta su conformidad con la respuesta, el procedimiento será sobreseído por quedar sin materia.

Cuando el responsable no atienda el requerimiento al que refiere el primer párrafo del presente artículo, el Instituto resolverá conforme a los elementos que consten en el expediente.

Referencia: artículo 124, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Fe pública

En el ejercicio de las funciones de verificación, el personal del Instituto estará dotado de fe pública para constatar la veracidad de los hechos en relación con los trámites a su cargo.

Referencia: artículo 130, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Fichero automatizado; Europa

Significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado.

Referencia: artículo 2, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Fichero de datos personales; Europa

Es ("fichero"): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Referencia: artículo 2, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Figura del encargado

El encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia

de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Referencia: artículo 49, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Formalización de las transferencias internacionales

A tal efecto, el responsable que transfiera los datos personales podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se prevean al menos las mismas obligaciones a las que se encuentra sujeto el responsable que transfiere los datos personales, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

Referencia: artículo 75, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Formalización de las transferencias nacionales

La transferencia deberá formalizarse mediante algún mecanismo que permita demostrar que el responsable transferente comunicó al responsable receptor las condiciones en las que el titular consintió el tratamiento de sus datos personales.

Referencia: artículo 73, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Fraude, estafa, hurto, phishing, plagio, robo, suplantación o usurpación de identidad. Véase: Suplantación de identidad.

Fuente de acceso público

Son aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito

que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el reglamento de la ley de referencia.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Fuentes de acceso público

Para los efectos del artículo 3, fracción X de la Ley, se consideran fuentes de acceso público:

I. Los medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;

II. Los directorios telefónicos en términos de la normativa específica;

III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa, y

IV. Los medios de comunicación social.

Para que los supuestos enumerados en el presente artículo sean considerados fuentes de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contraprestación, derecho o tarifa.

No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.

El tratamiento de datos personales obtenidos a través de fuentes de acceso público, respetará la expectativa razonable de privacidad, a que se refiere el tercer párrafo del artículo 7 de la Ley.

Referencia: artículo 7, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Funciones de seguridad

Para establecer y mantener de manera efectiva las medidas de seguridad, el responsable podrá desarrollar las funciones de seguridad por sí mismo, o bien, contratar a una persona física o moral para tal fin.

Referencia: artículo 59, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

G

Garantías complementarias para la persona concernida; Europa

Es un principio para la protección de datos personales, que establece el Convenio de referencia, que consiste en que cualquier persona deberá poder:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del Derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del artículo 8 del Convenio número 108 del Consejo de Europa.

Referencia: artículo 8, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Gastos y procedimientos de asistencia; Europa
Es la disposición del Convenio de referencia, que consiste en que:

1. La ayuda mutua que las Partes se concedan con arreglo a los términos del artículo 13, así como la asistencia que ellas presten a las personas concernidas residentes en el extranjero con arreglo a los términos del artículo 14, no dará lugar al pago de gastos y derechos que no sean los correspondientes a los expertos y a los intérpretes. Dichos gastos y derechos correrán a cargo de la Parte que haya designado a la autoridad que haya presentado la petición de asistencia.

2. La persona concernida no podrá estar obligada a pagar, en relación con las gestiones emprendidas por su cuenta en el territorio de otra Parte, los gastos y derechos que no sean los exigibles a las personas que residan en el territorio de dicha Parte.

3. Las demás modalidades relativas a la asistencia referentes, concretamente a las formas y procedimientos así como a las lenguas que se utilicen se establecerán directamente entre las Partes concernidas.
Referencia: artículo 17, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Grupos sin personalidad jurídica

Las personas integrantes de un grupo que actúe sin personalidad jurídica y que trate datos personales

para finalidades específicas o propias del grupo se considerarán también responsables o encargados, según sea el caso.

Referencia: artículo 8, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Guía para el borrado seguro de datos personales

Es un documento de apoyo para los involucrados en el tratamiento de datos personales, en particular para aquellos responsables o encargados del tratamiento de datos personales que están menos familiarizados con el tema de seguridad de la información, la cual permite conocer métodos y técnicas basadas en las mejores prácticas y estándares, para la eliminación segura de los datos personales en los sistemas de tratamiento.

Referencia: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Guía para el borrado seguro de datos personales, México, Ed. INAI, 2016, págs. 3-4.

H

Hábeas data

Habeas data, del latín jurídico, españolizado: ‘hábeas data’, que significa: tener datos presentes, siendo *hábeas* la segunda persona singular del presente de subjuntivo del verbo latino *habere* entendido como: tener. También significa: que tengas tus datos. (Derecho que consiste en que toda persona pueda acceder a la información sobre ellas que figura en los registros públicos). Constituye una institución o proceso legal que garantiza el derecho a la protección de los datos personales, protege al ciudadano contra el uso ilegal o indebido de los datos personales por parte de entidades públicas o privadas, tutelando de forma eficaz éste derecho²¹.

En palabras del jurista uruguayo Nelson Nicoliello Carmona el vocablo de marras, significa: «tengamos los datos. Derecho constitucional moderno, que consiste en la facultad de que las personas tengan acceso a la información sobre ellas, que exista en los registros públicos, y la de poder rectificarlos en caso necesario»²².

²¹Cfr. La acepción es de Barberia, María Emma, *Diccionario de latín jurídico*, Argentina, Ed. Valletta ediciones, 2006, pág. 63.

²²Esta es la definición que nos ofrece Nicoliello, Nelson, *Diccionario del latín jurídico*, Argentina, Ed. Euros Editores S.R.L., reimpresión 2004, pág. 118.

El jurista mexicano Germán Cisneros Farías ofrece para esta voz en estudio la acepción siguiente: «que tengamos los datos; derecho de toda persona, en el marco de un proceso constitucional, a tomar conocimiento personal de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, asimismo también rectificación, con fidelidad, o actualización de aquellos»²³.

En este sentido ha escrito la jurista María de los Ángeles Guzmán García, que el hábeas data es una garantía constitucional moderna que tiene su origen en Latinoamérica, cuyo nombre se compone de dos vocablos: del latín *habeas*, que significa tener, e inglés *data*, que significa información o datos, cuya garantía está destinada a salvaguardar el derecho a la protección de datos personales ante un tribunal.

La Constitución de Brasil de 1988 fue la primera en introducir la acción de “hábeas data”, que se ocupa de garantizar el derecho de los ciudadanos al acceso y rectificación de sus datos personales en posesión de terceros. Esta figura se encuentra actualmente en Argentina, Ecuador, Perú, Paraguay, Uruguay y Venezuela; en 1999, Chile emite su Ley de Protección de Datos, Argentina, con su ley del año 2000, ha desarrollado el derecho en América Latina.

La razón por la que surge en Latinoamérica se vincula con motivos de orden geopolítico, a sociedades que salían de regímenes militarizados a partir de la década de 1980 y relacionadas con el autoritarismo con el que se manejó la información,

²³Cisneros Farías, Germán, *Diccionario de frases y aforismos latinos*, México, Ed. Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2003, pág. 43.

como instrumento de represión política. Así, surgió la acción de “hábeas data”.

La acción de “hábeas data”, se define como “el derecho que asiste a toda persona, identificada o identificable, a solicitar judicialmente la exhibición de los registros públicos o privados, en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación. Esta herramienta tiende a proteger a las personas contra “calificaciones sospechosas”, incluidas en registros, especialmente estatales, aunque también pueden serlo privados, que sin darle derecho de contradecirlas, pueden llegar a perjudicarle de cualquier modo”, (Ekmekdjian y Pizzolo, 1996). La particularidad de esta acción es que garantiza la defensa del derecho a la protección de datos personales ante una autoridad judicial, y no ante una autoridad administrativa, como sucede en el caso de los países europeos.

En la actualidad el concepto de “hábeas data”, es una forma de denominar el “derecho de autodeterminación informativa” o el “derecho a la protección de datos personales”, pero, su naturaleza es diferente en atención a la autoridad garante. El “hábeas data” implica el ejercicio del derecho frente a una autoridad judicial, por tanto, a través de procedimiento judicial respectivo; mientras que la “autodeterminación informativa” o “protección de datos” es frente a una autoridad que forma parte de la administración pública, cuyas resoluciones pueden ser impugnadas ante autoridad judicial²⁴.

²⁴Cfr. Guzmán García, María de los Ángeles, en *Diccionario de derecho procesal constitucional y convencional*, 2.ª ed., México, Ed. Consejo de la Judicatura Federal y la Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2014, págs. 694-695.

De la correlación de los significados destacados, se colige que 'hábeas data', es sólo en otras naciones, es decir, fuera de México, el derecho de toda persona, en el marco de un proceso constitucional de su país, a tomar conocimiento personal de los datos a ella referidos y de su finalidad, derecho que consiste en que toda persona pueda acceder a la información sobre ellas que figura en los registros públicos o privados, también puede consistir en la facultad de que las personas tengan acceso a la información sobre ellas, que exista en los registros públicos, y la de poder rectificarlos, en caso necesario, también la supresión, confidencialidad, o actualización de aquellos datos.

Hurto de identidad, estafa, fraude, phishing, plagio, robo, suplantación o usurpación de identidad. Véase: Suplantación de identidad.

I

Identificación del personal verificador

Al iniciar la visita, el personal verificador deberá exhibir credencial vigente con fotografía, expedida por el Instituto que lo acredite para desempeñar dicha función, así como la orden escrita fundada y motivada a la que se refiere el artículo anterior, de la que deberá dejar copia con quien se entendió la visita.

Referencia: artículo 134, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Identificador de celda; Europa

Se define como la identidad de la celda desde que se origina o termina una llamada de teléfono móvil.

Referencia: artículo 2, de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006.

Identificador de usuario; Europa

Se define como un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a Internet o a un servicio de comunicaciones por Internet, o de su registro en uno de dichos servicios.

Referencia: artículo 2, de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006.

Impugnación de valoraciones; España

Es un derecho de las personas, en la ley de referencia, que establece lo siguiente:

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.

3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.

4. La valoración sobre el comportamiento de los ciudadanos basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Referencia: artículo 13, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Impugnación de valoraciones personales

Véase: Impugnación de valoraciones. (Derecho de los titulares de datos).

Incentivos para la autorregulación

Cuando un responsable adopte y cumpla un esquema de autorregulación, dicha circunstancia será tomada en consideración para determinar la atenuación de

la sanción que corresponda, en caso de verificarse algún incumplimiento a lo dispuesto por la Ley y el presente Reglamento, por parte del Instituto. Asimismo, el Instituto podrá determinar otros incentivos para la adopción de esquemas de autorregulación, así como mecanismos que faciliten procesos administrativos ante el mismo.

Referencia: artículo 81, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Información

Véase: Derecho de información en la recogida de datos. (Principio general relativo a la protección de datos personales).

Información de personas físicas con actividad comercial y datos de representación y contacto

Las disposiciones del presente Reglamento no serán aplicables a la información siguiente:

I. La relativa a personas morales;

II. Aquélla que refiera a personas físicas en su calidad de comerciantes y profesionistas, y

III. La de personas físicas que presten sus servicios para alguna persona moral o persona física con actividades empresariales y/o prestación de servicios, consistente únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como algunos de los siguientes datos laborales: domicilio físico, dirección electrónica, teléfono y número de fax; siempre que esta información sea tratada para fines de representación del empleador o contratista.

Referencia: artículo 5, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Información del interesado; Europa

Es la condición general para la licitud del tratamiento de datos personales, que establece la Directiva de referencia, siguiente:

Información en caso de obtención de datos recabados del propio interesado los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello:

- a) la identidad del responsable del tratamiento y, en su caso, de su representante;
- b) los fines del tratamiento de que van a ser objeto los datos;
- c) cualquier otra información tal como:

- los destinatarios o las categorías de destinatarios de los datos,

- el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder,

- la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.

Referencia: artículo 10, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Información mínima al titular en caso de vulneraciones de seguridad

El responsable deberá informar al titular al menos lo siguiente:

- I. La naturaleza del incidente;
- II. Los datos personales comprometidos;
- III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;
- IV. Las acciones correctivas realizadas de forma inmediata, y
- V. Los medios donde puede obtener más información al respecto.

Referencia: artículo 65, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Inicio. (Del procedimiento de imposición de sanciones)

Para efectos del artículo 61 de la Ley, el Instituto iniciará el procedimiento de imposición de sanciones cuando de los procedimientos de protección de derechos o de verificación, se determinen presuntas infracciones a la Ley susceptibles de ser sancionadas conforme al artículo 64 de la misma. Desahogado el procedimiento respectivo, se emitirá la resolución correspondiente.

El procedimiento iniciará con la notificación que se haga al presunto infractor, en el domicilio que el Instituto tenga registrado, derivado de los procedimientos de protección de derechos o de verificación.

La notificación irá acompañada de un informe que describa los hechos constitutivos de la presunta infracción, emplazando al presunto infractor para que en un término de quince días, contados a partir de que surta efectos la notificación, manifieste lo que

a su derecho convenga y rinda las pruebas que estime convenientes.

Referencia: artículo 140, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Inicio. (Del procedimiento de protección de derechos)

La solicitud para iniciar el procedimiento de protección de derechos deberá presentarse por el titular o su representante; ya sea mediante escrito libre, en los formatos que para tal efecto determine el Instituto o a través del sistema que éste establezca, en el plazo previsto en el artículo 45 de la Ley.

Tanto el formato como el sistema deberán ser puestos a disposición por el Instituto en su sitio de Internet y en cada una de las oficinas habilitadas que éste determine.

Al promover una solicitud de protección de derechos, el titular o su representante deberán acreditar su identidad o personalidad respectivamente, en los términos establecidos en el artículo 89 del presente Reglamento. En el caso del titular, éste también podrá acreditar su identidad a través de medios electrónicos u otros, en términos de lo que prevean las disposiciones legales o reglamentarias aplicables.

El Instituto podrá tener por reconocida la identidad del titular o la personalidad del representante cuando la misma ya hubiere sido acreditada ante el responsable al ejercer su derecho ARCO.

Referencia: artículo 113, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Inicio. (Del procedimiento de verificación)

El Instituto, con el objeto de comprobar el cumplimiento de las disposiciones previstas en la Ley o en la

regulación que de ella derive, podrá iniciar el procedimiento de verificación, requiriendo al responsable la documentación necesaria o realizando las visitas en el establecimiento en donde se encuentren las bases de datos respectivas.

Referencia: artículo 128, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Tiene por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la ley de referencia y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.

Con fecha 7 de febrero de 2014 fue publicado en el Diario Oficial de la Federación el “Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia”, que crea un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados.

Es un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización inter-

na, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos establecidos en las leyes respectivas, con domicilio legal en la Ciudad de México.

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, tiene como antecedente al Instituto Federal de Acceso a la Información y Protección de Datos, que cambió su denominación a partir de la publicación de 9 de mayo de 2016, de la Ley Federal de Transparencia y Acceso a la Información Pública.

Referencia: artículo 38, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

L

Listado de exclusión. (Definiciones)

Base de datos que tiene por objeto registrar de manera gratuita la negativa del titular al tratamiento de sus datos personales.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Listados de exclusión

Para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas.

Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales.

En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.

Referencia: artículo 110, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

M

Mecanismos de coordinación

Para la elaboración, emisión y publicación de la regulación a que se refiere el artículo 40 de la Ley, la dependencia y el Instituto establecerán los mecanismos de coordinación correspondientes.

En todos los casos, la dependencia y el Instituto, en el ámbito de sus atribuciones, determinarán las disposiciones que normen el tratamiento de datos personales en el sector o actividad que corresponda. *Referencia: artículo 78, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.*

Medidas compensatorias

En términos del tercer párrafo del artículo 18 de la Ley, cuando resulte imposible dar a conocer el aviso de privacidad al titular o exija esfuerzos desproporcionados, en consideración al número de titulares o a la antigüedad de los datos, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios generales expedidos por el Instituto, mismos que serán publicados en el Diario Oficial de la Federación, bajo los cuales podrán utilizarse los medios que se establecen en el artículo 35 del presente Reglamento.

Los casos que no actualicen los criterios generales emitidos por el Instituto requerirán la autorización expresa de éste, previo a la instrumentación de la medida compensatoria, de conformidad con el pro-

cedimiento establecido en los artículos 33 y 34 del presente Reglamento.

Referencia: artículo 32, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medidas correctivas en caso de vulneraciones de seguridad

En caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes, a efecto de evitar que la vulneración se repita.

Referencia: artículo 66, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medidas de seguridad administrativas. (Definiciones)

Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medidas de seguridad físicas. (Definiciones)

Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:

a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;

b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;

c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y

d) Garantizar la eliminación de datos de forma segura.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medidas de seguridad técnicas. (Definiciones)

Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;

b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Se incluyan acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros, y

d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medidas para el principio de responsabilidad

En términos del artículo 14 de la Ley, el responsable deberá adoptar medidas para garantizar el debido

tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad.

Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:

I. Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;

II. Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;

III. Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;

IV. Destinar recursos para la instrumentación de los programas y políticas de privacidad;

V. Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;

VI. Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;

VII. Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;

VIII. Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;

IX. Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento, o

X. Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.

Referencia: artículo 48, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medios de difusión

Para la difusión de los avisos de privacidad, el responsable podrá valerse de formatos físicos, electrónicos, medios verbales o cualquier otra tecnología, siempre y cuando garantice y cumpla con el deber de informar al titular.

Referencia: artículo 25, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medios de impugnación

Contra la resolución al procedimiento de protección de derechos procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

Referencia: artículo 126, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medios de impugnación

En contra de la resolución al procedimiento de verificación, se podrá interponer el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.
Referencia: artículo 138, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medios de impugnación

En contra de la resolución al procedimiento de imposición de sanciones procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.
Referencia: artículo 144, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medios para el cumplimiento del derecho de acceso

La obligación de acceso se dará por cumplida cuando el responsable ponga a disposición del titular los datos personales en sitio, respetando el periodo señalado en el artículo 99 del presente Reglamento, o bien, mediante la expedición de copias simples, medios magnéticos, ópticos, sonoros, visuales u holográficos, o utilizando otras tecnologías de la información que se hayan previsto en el aviso de privacidad. En todos los casos, el acceso deberá ser en formatos legibles o comprensibles para el titular.

Cuando el responsable así lo considere conveniente, podrá acordar con el titular medios de reproducción de la información distintos a los informados en el aviso de privacidad.

Referencia: artículo 102, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medios para el ejercicio de los derechos

El titular, para el ejercicio de los derechos ARCO, podrá presentar, por sí mismo o a través de su representante, la solicitud ante el responsable conforme a los medios establecidos en el aviso de privacidad. Para tal fin, el responsable pondrá a disposición del titular, medios remotos o locales de comunicación electrónica u otros que considere pertinentes.

Asimismo, el responsable podrá establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO, lo cual deberá informarse en el aviso de privacidad.

Referencia: artículo 90, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Medios para presentar la solicitud de protección de derechos

La solicitud de protección de derechos podrá presentarse en el domicilio del Instituto, en sus oficinas habilitadas, por correo certificado con acuse de recibo o en el sistema al que refiere el artículo anterior, en este último caso, siempre que el particular cuente con la certificación del medio de identificación electrónica a que se refiere el artículo 69-C de la Ley Federal de Procedimiento Administrativo u otras disposiciones legales aplicables. En todo caso, se entregará al promovente un acuse de recibo en el cual conste de manera fehaciente la fecha de la presentación de la solicitud.

Cuando el promovente presente su solicitud por medios electrónicos a través del sistema que establezca el Instituto, se entenderá que acepta que las notificaciones le sean efectuadas por dicho sistema o a través de otros medios electrónicos generados por éste, salvo que señale un medio distinto para efectos de las notificaciones.

Cuando la solicitud sea presentada por el titular o su representante en la oficina habilitada por el Instituto, ésta hará constar la acreditación de la identidad o, en su caso, de la personalidad del representante, y podrá enviar o registrar por medios electrónicos, tanto la solicitud, como los documentos exhibidos. En este caso, la solicitud se tendrá por recibida, para efectos del plazo a que se refiere el artículo 47 de la Ley, cuando el Instituto, a través de ese mismo medio, genere el acuse de recibo correspondiente.

Lo anterior, sin perjuicio de que la oficina habilitada remita al Instituto por correo certificado, la constancia de identidad del titular o el documento de acreditación de la personalidad del representante, así como la solicitud y los documentos anexos, para su integración al expediente respectivo.

En el caso de que el titular envíe la solicitud y sus anexos por correo certificado, el plazo a que se refiere el artículo 47 de la Ley empezará a contar a partir de la fecha que conste en el sello de recepción del Instituto.

Referencia: artículo 114, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Modalidades de medidas compensatorias

Las medidas compensatorias de comunicación masiva deberán contener la información prevista en el artículo 27 del presente Reglamento y se darán a conocer a través de avisos de privacidad que se publicarán en cualquiera de los medios siguientes:

- I. Diarios de circulación nacional;
- II. Diarios locales o revistas especializadas, cuando se demuestre que los titulares de los datos personales residan en una determinada entidad federativa o pertenezcan a una determinada actividad;

III. Página de Internet del responsable;

IV. Hiperenlaces o hipervínculos situados en una página de Internet del Instituto, habilitados para dicho fin, cuando el responsable no cuente con una página de Internet propia;

V. Carteles informativos;

VI. Difusión en cápsulas informativas en radiodifusoras, o

VII. Otros medios alternos de comunicación masiva.

Referencia: artículo 35, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

México; delitos en materia del tratamiento indebido de datos personales

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, establece figuras delictivas respecto a la protección de datos personales, recoge los delitos en sus artículos 67 a 69, siguientes:

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.

Referencia: artículos 67 a 69, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

México; entidades federativas de la República Mexicana, leyes estatales vigentes en materia de protección de datos personales u organismos públicos autónomos especializados en materia de información pública y protección de datos personales

Aguascalientes. Lineamientos para la Protección de Datos Personales. Publicado el 12 de julio del año 2010, última reforma el 17 de enero del 2011.

Instituto de Transparencia del Estado de Aguascalientes. www.itea.org.mx

Baja California. Instituto de Transparencia y Acceso a la Información Pública de Baja California.

www.itaipbc.org.mx

Baja California Sur. Instituto de Transparencia y Acceso a la Información Pública del Estado de Baja California Sur.

www.itai.org.mx

Campeche. Ley de Protección de Datos Personales del Estado de Campeche y sus Municipios. De 24 de diciembre del 2012.

Comisión de Transparencia y Acceso a la Información Pública del Estado de Campeche.

www.cotaippec.org.mx

Chiapas. Instituto de Acceso a la Información Pública de la Administración Pública Estatal de Chiapas.

www.iaipchiapas.org.mx

Chihuahua. Ley de Protección de Datos Personales del Estado de Chihuahua. Publicada el 26 de junio del 2013.

Instituto Chihuahuense para la Transparencia y

Acceso a la Información Pública.
www.ichitaip.org.mx

Coahuila. Instituto Coahuilense de Acceso a la Información Pública.
www.icaei.org.mx

Colima. Ley de Protección de Datos Personales. Publicada el 21 de junio de 2003, última reforma el 12 de mayo del 2012.
Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos del Estado de Colima.
www.infocol.org.mx

Ciudad de México. Ley de Protección de Datos Personales para el Distrito Federal. Publicada el 3 de octubre de 2008.
Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales, y Rendición de Cuentas de la Ciudad de México.
www.infodf.org.mx

Durango. Ley de Protección de Datos Personales del Estado de Durango. Publicada el 5 de diciembre de 2013.
Instituto Duranguense de Acceso a la Información Pública y de Protección de Datos Personales.
www.idaip.org.mx

Estado de México. Ley de Protección de Datos Personales del Estado de México. Publicada el 31 de agosto de 2012.
Instituto de Transparencia, Acceso a la Información Pública, y Protección de Datos Personales del Estado de México.
<http://www.itaipem.org.mx>

Guanajuato. Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato. Publicada el 19 de mayo de 2006, última reforma el 7 de junio del 2013.

Instituto de Acceso a la Información Pública para el Estado de Guanajuato.

www.iacip-gto.org.mx

Guerrero. Instituto de Transparencia, Acceso a la información, y Protección de Datos Personales del Estado de Guerrero.

www.itaig.org.mx

Hidalgo. Instituto de Acceso a la Información Pública Gubernamental del Estado de Hidalgo.

www.iaipgh.org.mx

Jalisco. Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco. www.itei.org.mx

Michoacán. Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales.

www.itaimich.org.mx

Morelos. Instituto Morelense de Información Pública y Estadística.

www.imipe.org.mx

Nayarit. Instituto de Transparencia y Acceso a la Información Pública del Estado de Nayarit.

www.itainayarit.org

Nuevo León. Comisión de Transparencia y Acceso a la Información del Estado de Nuevo León.

www.ctainl.org.mx

Oaxaca. Ley de Protección de Datos Personales del Estado de Oaxaca. Publicada el 23 de agosto de 2008. Instituto de Acceso a la Información Pública y Protección de Datos de Oaxaca.
www.iaipoaxaca.org.mx

Puebla. Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados del Estado de Puebla. Publicada el 25 de noviembre del 2013. Comisión para el Acceso a la Información Pública y Protección de Datos Personales del Estado de Puebla.
www.caip.org.mx

Querétaro. Comisión Estatal de Información Gubernamental Querétaro.
www.ceigqro.org.mx

Quintana Roo. Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo.
www.idaipqroo.org.mx

San Luis Potosí. Comisión Estatal de Garantía de Acceso a la Información Pública de San Luis Potosí.
www.cegaipslp.org.mx

Sinaloa. Comisión Estatal para el Acceso a la Información Pública Sinaloa.
www.ceaipsinaloa.org.mx

Sonora. Ley de Acceso a la Información Pública y Protección de Datos Personales del Estado de Sonora. Última reforma el 12 de agosto del 2013. Instituto de Transparencia Informativa del Estado de Sonora.
www.transparenciasonora.org

Tabasco. Instituto Tabasqueño de Transparencia y Acceso a la Información Pública.
www.itaip.org.mx

Tamaulipas. Instituto de Transparencia y Acceso a la Información de Tamaulipas.
www.itait.org.mx

Tlaxcala. Ley de Protección de Datos Personales del Estado de Tlaxcala. Publicada el 14 de mayo de 2012.
Instituto de Acceso a la Información Pública y Protección de Datos Personales del Estado de Tlaxcala.
www.caip-tlax.org.mx

Veracruz. Ley número 581 para la Tutela de los Datos Personales en el Estado de Veracruz. Publicada el 2 de octubre del 2012. Lineamientos para la Tutela de los Datos Personales en el Estado de Veracruz, última adición el 27 de diciembre del 2013.
Instituto Veracruzano de Acceso a la Información y Protección de Datos Personales.
www.ivaiv.org.mx

Yucatán. Instituto Estatal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales Yucatán.
www.inaipyucatan.org.mx

Zacatecas. Instituto Zacatecano de Transparencia, Acceso a la Información, y Protección de Datos Personales.
www.izai.org.mx

México; Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Es parte de la legislación federal de Estados Unidos Mexicanos, que se conforma de 69 artículos, y artículos transitorios, misma ley que dispone en su artículo primero que la presente ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas”.

Referencia: Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación, de la Secretaría de Gobernación, el día lunes 5 de julio de 2010. Estados Unidos Mexicanos.

México; Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Es parte de la legislación federal de Estados Unidos Mexicanos, que se conforma de 64 artículos, y 11 artículos transitorios, misma ley que dispone en su primer artículo que: “es de orden público. Tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal”.

Referencia: Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, expedida el 10 de junio de 2002, publicada el 11 de junio de 2002, México.

México; Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Es parte de la legislación federal de Estados Unidos Mexicanos, que se conforma de 144 artículos, y 5 artículos transitorios, mismo reglamento que dispone en su artículo primero que: “el presente ordenamiento tiene por objeto reglamentar las disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares”.

Referencia: Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado el 21 de diciembre de 2012. México.

México; Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos

Es parte de la legislación federal de Estados Unidos Mexicanos, que se conforma de 44 artículos, y 4 transitorios, mismo reglamento interior que dispone en su artículo 1 que: “el presente Reglamento Interior tiene por objeto establecer la estructura y regular el funcionamiento y operación del Instituto Federal de Acceso a la Información y Protección de Datos”; además en su artículo 2 que: “El Instituto Federal de Acceso a la Información y Protección de Datos es un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos establecidos en las leyes respectivas, con domicilio legal en la Ciudad de México”. En el transitorio segundo abroga el

Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos, publicado en el Diario Oficial de la Federación el día veintinueve de octubre de dos mil doce y demás disposiciones jurídicas que se opongan al presente Reglamento.

Referencia: Reglamento Interior de del Instituto Federal de Acceso a la Información y Protección de datos, publicado el 20 de febrero de 2014. México.

N

Negativa por parte del responsable

El responsable que niegue el ejercicio de cualquiera de los derechos ARCO deberá justificar su respuesta, así como informar al titular el derecho que le asiste para solicitar el inicio del procedimiento de protección de derechos ante el Instituto.

Referencia: artículo 100, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Notificación de vulneraciones de seguridad

El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, en cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

O

Objetivos específicos de la autorregulación

Los esquemas de autorregulación podrán traducirse en códigos deontológicos o de buenas prácticas profesionales, sellos de confianza, políticas de privacidad, reglas de privacidad corporativas u otros mecanismos, que incluirán reglas o estándares específicos y tendrán los siguientes objetivos primordiales:

I. Coadyuvar al cumplimiento del principio de responsabilidad al que refiere la Ley y el presente Reglamento;

II. Establecer procesos y prácticas cualitativos en el ámbito de la protección de datos personales que complementen lo dispuesto en la Ley;

III. Fomentar que los responsables establezcan políticas, procesos y buenas prácticas para el cumplimiento de los principios de protección de datos personales, garantizando la privacidad y confidencialidad de la información personal que esté en su posesión;

IV. Promover que los responsables de manera voluntaria cuenten con constancias o certificaciones sobre el cumplimiento de lo establecido en la Ley, y mostrar a los titulares su compromiso con la protección de datos personales;

V. Identificar a los responsables que cuenten con políticas de privacidad alineadas al cumplimiento de los principios y derechos previstos en la Ley, así como de competencia laboral para el debido cumplimiento de sus obligaciones en la materia;

VI. Facilitar la coordinación entre los distintos esquemas de autorregulación reconocidos internacionalmente;

VII. Facilitar las transferencias con responsables que cuenten con esquemas de autorregulación como puerto seguro;

VIII. Promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de privacidad, incluyendo herramientas, transparencia, supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación, y

IX. Encauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.

Estos esquemas serán vinculantes para quienes se adhieran a los mismos; no obstante, la adhesión será de carácter voluntario.

Referencia: artículo 80, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Objeto. (Disposiciones generales)

El presente ordenamiento tiene por objeto reglamentar las disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *Referencia: artículo 1, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.*

Objeto de la autorregulación

De conformidad con lo establecido en el artículo 44 de la Ley, las personas físicas o morales podrán convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en materia de protección de datos personales, que complementen lo dispuesto por la Ley, el presente Reglamento y las disposiciones que se emitan por las dependencias en desarrollo del mismo y en el ámbito de sus atribuciones. Asimismo, a través de dichos esquemas el responsable podrá demostrar ante el Instituto el cumplimiento de las obligaciones previstas en dicha normativa.

Lo anterior con el objeto de armonizar los tratamientos que lleven a cabo quienes se adhieren a los mismos y facilitar el ejercicio de los derechos de los titulares.

Referencia: artículo 79, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Objeto, de la Directiva 95/46/CE; Europa

Es la disposición general de la Directiva de referencia, que señala:

1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fun-

damentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.

2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1. *Referencia: artículo 1, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

Objeto y fin, del Convenio número 108 del Consejo de Europa

Es la disposición del Convenio de referencia, que establece que el fin de dicho Convenio es garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos).

Referencia: artículo 1, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Obligación de notificación a la autoridad de control; Europa

Es la disposición de la Directiva de referencia, que establece unas de las condiciones generales para la licitud del tratamiento de datos personales, siguientes:

1. Los Estados miembros dispondrán que el responsable del tratamiento o, en su caso, su representante, efectúe una notificación a la autoridad de control contemplada en el artículo 28, con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos, total o parcialmente automatizados, destinados a la consecución de un fin o de varios fines conexos.

2. Los Estados miembros podrán disponer la simplificación o la omisión de la notificación, sólo en los siguientes casos y con las siguientes condiciones:

- cuando, para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados habida cuenta de los datos a que se refiere el tratamiento, los Estados miembros precisen los fines de los tratamientos, los datos o categorías de datos tratados, la categoría o categorías de los interesados, los destinatarios o categorías de destinatarios a los que se comuniquen los datos y el período de conservación de los datos y/o

- cuando el responsable del tratamiento designe, con arreglo al Derecho nacional al que está sujeto, un encargado de protección de los datos personales que tenga por cometido, en particular:

- hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en virtud de la presente Directiva,

- llevar un registro de los tratamientos efectuados por el responsable del tratamiento, que contenga la información enumerada en el apartado 2 del artículo 21, garantizando así que el tratamiento de los datos no pueda ocasionar una merma de los derechos y libertades de los interesados.

3. Los Estados miembros podrán disponer que no se aplique el apartado 1 a aquellos tratamientos cuya única finalidad sea la de llevar un registro que, en virtud de disposiciones legales o reglamentarias, esté destinado a facilitar información al público y estén abiertos a la consulta por el público en general o por toda persona que pueda demostrar un interés legítimo.

4. Los Estados miembros podrán eximir de la obligación de notificación o disponer una simplificación de la misma respecto de los tratamientos a que se refiere la letra d) del apartado 2 del artículo 5.

5. Los Estados miembros podrán disponer que los tratamientos no automatizados de datos de carácter personal o algunos de ellos sean notificados eventualmente de una forma simplificada.

Referencia: artículo 18, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Obligaciones del encargado

El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:

I. Tratar únicamente los datos personales conforme a las instrucciones del responsable;

II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;

III. Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables;

IV. Guardar confidencialidad respecto de los datos personales tratados;

V. Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y

VI. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

Los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente. *Referencia: artículo 50, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.*

Ofrecimiento de pruebas

Los medios de prueba que podrán ofrecerse son los siguientes:

- I. La documental pública;
- II. La documental privada;
- III. La inspección, siempre y cuando se realice a través de la autoridad competente;
- IV. La presuncional, en su doble aspecto, legal y humana;
- V. La pericial;
- VI. La testimonial, y
- VII. Las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.

V. Identificar a los responsables que cuenten con políticas de privacidad alineadas al cumplimiento de los principios y derechos previstos en la Ley, así como de competencia laboral para el debido cumplimiento de sus obligaciones en la materia;

VI. Facilitar la coordinación entre los distintos esquemas de autorregulación reconocidos internacionalmente;

VII. Facilitar las transferencias con responsables que cuenten con esquemas de autorregulación como puerto seguro;

VIII. Promover el compromiso de los responsables con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos, así como para auspiciar mecanismos para implementar políticas de privacidad, incluyendo herramientas, transparencia, supervisión interna continua, evaluaciones de riesgo, verificaciones externas y sistemas de remediación, y

IX. Encauzar mecanismos de solución alternativa de controversias entre responsables, titulares y terceras personas, como son los de conciliación y mediación.

Estos esquemas serán vinculantes para quienes se adhieran a los mismos; no obstante, la adhesión será de carácter voluntario.

Referencia: artículo 80, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

En caso de que se ofrezca prueba pericial o testimonial, se precisarán los hechos sobre los que deban versar y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o el interrogatorio respectivo en preparación de las mismas. Sin estos señalamientos se tendrán por no ofrecidas dichas pruebas.

Referencia: artículo 119, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Ofrecimiento y desahogo de pruebas

El presunto infractor en su contestación se manifestará concretamente respecto de cada uno de los hechos que se le imputen de manera expresa, afirmándolos, negándolos, señalando que los ignora por no ser propios o exponiendo cómo ocurrieron, según sea el caso; y presentará los argumentos por medio de los cuales desvirtúe la infracción que se presume y las pruebas correspondientes.

En caso de que se ofrezca prueba pericial o testimonial, se precisarán los hechos sobre los que deban versar y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o el interrogatorio respectivo en preparación de las mismas. Sin estos señalamientos se tendrán por no ofrecidas dichas pruebas.

Referencia: artículo 141, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Opinión del instituto respecto de las transferencias

Los responsables, en caso de considerarlo necesario, podrán solicitar la opinión del Instituto respecto a si las transferencias internacionales que realicen

cumplen con lo dispuesto por la Ley y el presente Reglamento.

Referencia: artículo 76, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Oposición del tratamiento para finalidades distintas

El titular podrá negar o revocar su consentimiento, así como oponerse para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular, sin que ello tenga como consecuencia la conclusión del tratamiento para estas últimas finalidades.

Referencia: artículo 42, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

P

Parámetros de autorregulación

Los parámetros de autorregulación a los que se refiere el artículo 43, fracción V de la Ley contendrán los mecanismos para acreditar y revocar a las personas físicas o morales certificadoras, así como sus funciones; los criterios generales para otorgar los certificados en materia de protección de datos personales, y el procedimiento de notificación de los esquemas de autorregulación vinculante.

Referencia: artículo 85, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Persona física identificable. (Definiciones)

Toda persona física cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información. No se considera persona física identificable cuando para lograr la identidad de ésta se requieran plazos o actividades desproporcionadas.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Personas facultadas para el ejercicio de los derechos

Los derechos ARCO se ejercerán:

I. Por el titular, previa acreditación de su identidad, a través de la presentación de copia de su documento de identificación y habiendo exhibido el original para su cotejo. También podrán ser admis-

ibles los instrumentos electrónicos por medio de los cuales sea posible identificar fehacientemente al titular, u otros mecanismos de autenticación permitidos por otras disposiciones legales o reglamentarias, o aquéllos previamente establecidos por el responsable. La utilización de firma electrónica avanzada o del instrumento electrónico que lo sustituya eximirá de la presentación de la copia del documento de identificación, y

II. Por el representante del titular, previa acreditación de:

- a) La identidad del titular;
- b) La identidad del representante, y
- c) La existencia de la representación, mediante instrumento público o carta poder firmada ante dos testigos, o declaración en comparecencia personal del titular.

Para el ejercicio de los derechos ARCO de datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad establecida por ley, se estará a las reglas de representación dispuestas en el Código Civil Federal.

Referencia: artículo 89, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Personas físicas o morales acreditadas

Las personas físicas o morales acreditadas como certificadores tendrán la función principal de certificar que las políticas, programas y procedimientos de privacidad instrumentados por los responsables que de manera voluntaria se sometan a su actuación, aseguren el debido tratamiento y que las medidas de seguridad adoptadas son las adecuadas para su protección. Para ello, los certificadores podrán valerse

de mecanismos como verificaciones y auditorías.

El procedimiento de acreditación de los certificadores a los que refiere el párrafo anterior, se llevará a cabo de acuerdo con los parámetros que prevé el artículo 43, fracción V de Ley. Estos certificadores deberán garantizar la independencia e imparcialidad para el otorgamiento de certificados, así como el cumplimiento de los requisitos y criterios que se establezcan en los parámetros en mención.

Referencia: artículo 84, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Plazos de conservación de los datos personales

Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento, y deberán atender las disposiciones aplicables a la materia de que se trate, y tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión.

Referencia: artículo 37, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Plagio de identidad, estafa, fraude, hurto, phishing, robo, suplantación o usurpación de identidad. Véase: Suplantación de identidad.

Presentación de alegatos

Dictado el acuerdo que tenga por desahogadas todas las pruebas, se pondrán las actuaciones a disposición de las partes, para que éstos, en caso de quererlo, formulen alegatos en un plazo de cinco días, contados a partir de la notificación del acuerdo a que se refiere este artículo. Al término de dicho plazo, se cerrará la instrucción y el Instituto emitirá su resolución en el plazo establecido en el artículo 47 de la Ley.

Referencia: artículo 122, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de calidad

Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.

Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga.

Cuando los datos personales no fueron obtenidos directamente del titular, el responsable deberá adoptar medidas razonables para que éstos respondan al principio de calidad, de acuerdo con el tipo de datos personales y las condiciones del tratamiento.

El responsable deberá adoptar los mecanismos que considere necesarios para procurar que los datos personales que trate sean exactos, completos, pertinentes, correctos y actualizados, a fin de que no se altere la veracidad de la información, ni que ello tenga como consecuencia que el titular se vea afectado por dicha situación.

Referencia: artículo 36, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de consentimiento

El responsable deberá obtener el consentimiento para el tratamiento de los datos personales, a menos que no sea exigible con arreglo a lo previsto en el artículo 10 de la Ley.

La solicitud del consentimiento deberá ir referida a una finalidad o finalidades determinadas, previstas en el aviso de privacidad.

Cuando los datos personales se obtengan personalmente o de manera directa de su titular, el consentimiento deberá ser previo al tratamiento.

Referencia: artículo 11, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de finalidad

Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad, en términos del artículo 12 de la Ley.

Para efectos del párrafo anterior, la finalidad o las finalidades establecidas en el aviso de privacidad deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales.

Referencia: artículo 40, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de información

El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad, de conformidad con lo previsto en la Ley y el presente Reglamento.

Referencia: artículo 23, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de lealtad

El principio de lealtad establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad, en los términos establecidos en el artículo 7 de la Ley.

No se podrán utilizar medios engañosos o fraudulentos para recabar y tratar datos personales. Existe una actuación fraudulenta o engañosa cuando:

I. Exista dolo, mala fe o negligencia en la información proporcionada al titular sobre el tratamiento;

II. Se vulnere la expectativa razonable de privacidad del titular a la que refiere el artículo 7 de la Ley, o

III. Las finalidades no son las informadas en el aviso de privacidad.

Referencia: artículo 44, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de licitud

El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional.

Referencia: artículo 10, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de proporcionalidad

Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido.

Referencia: artículo 45, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de responsabilidad

En términos de los artículos 6 y 14 de la Ley, el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano.

Para cumplir con esta obligación, el responsable podrá valerse de estándares, mejores prácticas internacionales, políticas corporativas, esquemas de autorregulación o cualquier otro mecanismo que determine adecuado para tales fines.

Referencia: artículo 47, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principios de protección de datos

De acuerdo con lo previsto en el artículo 6 de la Ley, los responsables deben cumplir con los siguientes principios rectores de la protección de datos personales:

- I. Licitud;
- II. Consentimiento;
- III. Información;

- IV. Calidad;
- V. Finalidad;
- VI. Lealtad;
- VII. Proporcionalidad, y
- VIII. Responsabilidad.

Asimismo, el responsable deberá observar los deberes de seguridad y confidencialidad a que se refieren los artículos 19 y 21 de la Ley.

Referencia: artículo 9, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principios para la transferencia de datos personales a países terceros; Europa

Es la disposición de la Directiva de referencia, que consiste en lo siguiente:

1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado.

2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas

de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2.

4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate.

5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4.

6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.

Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión. *Referencia: artículo 25, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

Principios relativos a la calidad de los datos; Europa

Son las condiciones para licitud del tratamiento de datos personales, que establece la Directiva de referencia, siguientes:

1. Los Estados miembros dispondrán que los datos personales sean:

- a) tratados de manera leal y lícita.
- b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas;
- c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
- d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;
- e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los

que fueron recogidos o para los que se traten ulteriormente.

Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado.

Referencia: artículo 6, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Principios relativos a la legitimación del tratamiento de datos

Son las condiciones para licitud del tratamiento de datos personales, que establece la Directiva de referencia, siguientes:

Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

a) el interesado ha dado su consentimiento de forma inequívoca,

b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o

c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o

d) es necesario para proteger el interés vital del interesado, o

e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o

f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la Directiva referida.

Referencia: artículo 7, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Procedimiento ante la negativa al cese en el tratamiento

En caso de negativa por parte del responsable al cese en el tratamiento ante la revocación del consentimiento, el titular podrá presentar ante el Instituto la denuncia correspondiente a que refiere el Capítulo IX del presente Reglamento.

Referencia: artículo 22, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Procedimiento para la autorización de medidas compensatorias

El Instituto tendrá un plazo de diez días siguientes a la recepción de la solicitud de medida compensatoria, para emitir la resolución correspondiente.

Si el Instituto no resuelve en el plazo establecido, la solicitud de medida compensatoria se entenderá como autorizada.

Una vez presentada la solicitud por el responsable ante el Instituto, éste valorará los esfuerzos desproporcionados para dar a conocer el aviso de privacidad, tomando en cuenta lo siguiente:

- I. El número de titulares;
- II. La antigüedad de los datos;
- III. La capacidad económica del responsable;
- IV. El ámbito territorial y sectorial de operación del responsable, y
- V. La medida compensatoria a utilizar.

En caso de que el Instituto en su valoración considere que la medida compensatoria propuesta no cumple con el principio de información, podrá proponer al responsable la adopción de alguna medida compensatoria alterna a la propuesta por el responsable en su solicitud.

La propuesta del Instituto se hará del conocimiento del responsable, a fin de que éste exponga lo que a su derecho convenga en un plazo no mayor a cinco días, contados a partir del día siguiente en que haya recibido la notificación.

Si el responsable no responde en el plazo que señala el párrafo anterior, el Instituto resolverá con los elementos que consten en el expediente.

Cuando el Instituto determine que el responsable no justificó la imposibilidad de dar a conocer el aviso de privacidad al titular o que ello exige esfuerzos desproporcionados, no será autorizado el uso de medidas compensatorias.

La autorización que en su caso otorgue el Instituto estará vigente mientras no se modifiquen las circunstancias bajo las cuales se autorizó la medida compensatoria.

Referencia: artículo 34, del Reglamento de la Ley Federal de Protección de Datos Personales en Pose-

sión de los Particulares. México.

Procedimientos específicos para el ejercicio de los derechos “ARCO”

Cuando las disposiciones aplicables a determinadas bases de datos o tratamientos establezcan un procedimiento específico para solicitar el ejercicio de los derechos ARCO, se estará a lo dispuesto en aquéllas que ofrezcan mayores garantías al titular, y no contravengan las disposiciones previstas en la Ley.

Referencia: artículo 92, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Procedimientos para conservación, bloqueo y supresión de los datos personales

El responsable establecerá y documentará procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales, que incluyan los periodos de conservación de los mismos, de conformidad con el artículo anterior.

Referencia: artículo 38, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Propósitos del bloqueo

En términos del artículo 3, fracción III de la Ley, el bloqueo tiene como propósito impedir el tratamiento, a excepción del almacenamiento, o posible acceso por persona alguna, salvo que alguna disposición legal prevea lo contrario.

El periodo de bloqueo será hasta el plazo de prescripción legal o contractual correspondiente.

Referencia: artículo 108, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Protección de datos personales

Véase: Derecho a la protección de datos personales.

Protección más amplia; Europa

Es un principio básico para la protección de datos del Convenio de referencia, que consiste en que ninguna de las disposiciones del capítulo II de los Principios Básicos para la Protección de Datos, se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el Convenio número 108 del Consejo de Europa.

Referencia: artículo 11, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Prueba del aviso de privacidad

Para efectos de demostrar la puesta a disposición del aviso de privacidad en cumplimiento del principio de información, la carga de la prueba recaerá, en todos los casos, en el responsable.

Referencia: artículo 31, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Prueba del cumplimiento de las obligaciones en materia de transferencias

Para efectos de demostrar que la transferencia, sea ésta nacional o internacional, se realizó conforme a lo que establece la Ley y el presente Reglamento la carga de la prueba recaerá, en todos los casos, en el responsable que transfiere y en el receptor de los datos personales.

Referencia: artículo 69, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Prueba del cumplimiento de los plazos de conservación

Al responsable le corresponde demostrar que los datos personales se conservan o, en su caso, bloquean, suprimen o cancelan cumpliendo los plazos previstos en el artículo 37 del presente Reglamento, o bien, en atención a una solicitud de derecho de cancelación.

Referencia: artículo 39, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Prueba para demostrar la obtención del consentimiento

Para efectos de demostrar la obtención del consentimiento, la carga de la prueba recaerá, en todos los casos, en el responsable.

Referencia: artículo 20, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Principio de información

El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad, de conformidad con lo previsto en la Ley y el presente Reglamento.

Referencia: artículo 23, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

R

Receptor de los datos personales

El receptor de los datos personales será un sujeto regulado por la Ley y el presente Reglamento en su carácter de responsable, y deberá tratar los datos personales conforme a lo convenido en el aviso de privacidad que le comunique el responsable transferente.

Referencia: artículo 72, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Reconducción del procedimiento

En caso de que la solicitud de protección de derechos no actualice alguna de las causales de procedencia previstas en el artículo 115 del presente Reglamento, sino que refiera al procedimiento de verificación contenido en el Capítulo IX de este Reglamento, ésta se turnará a la unidad administrativa competente, en un plazo no mayor a diez días, contados a partir del día en que se recibió la solicitud.

Referencia: artículo 127, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Reconducción del procedimiento

En caso de que la denuncia presentada no refiera al procedimiento previsto en el presente capítulo, sino que actualice alguna de las causales de procedencia del procedimiento de protección de derechos, con-

tenidas en el artículo 115 del presente Reglamento, ésta se turnará a la unidad administrativa competente, en un plazo no mayor a diez días, contados a partir del día en que se recibió la solicitud.

Referencia: artículo 139, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Red Iberoamericana de Protección de Datos

Surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países.

Se constituyó como una respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los países iberoamericanos, a través del diálogo y colaboración en materia de protección de datos de carácter personal. Se encuentra abierta a todos los países de la región que deseen promover y ejecutar iniciativas y proyectos relacionados con esta materia.

Creó un foro integrador que permite la participación de diversos actores sociales, tanto del sector público como privado. Esta iniciativa contó desde sus inicios con el apoyo político de los participantes en la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos celebrada en Santa Cruz de la Sierra, Bolivia, 14 y 15 de noviembre de 2003, mismo que quedó plasmado en su Declaración Final en la que dan cuenta del carácter de la protección de datos personales como Derecho Fundamental, así como de la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

A partir de ese momento, se convirtió en un foro de promoción del Derecho Fundamental a la protección de datos en esta comunidad, cuyo impulso y responsabilidad asumieron también los representantes políticos de los respectivos Estados signatarios de la Declaración de Santa Cruz de la Sierra.

Los objetivos y la organización están en el Reglamento aprobado con motivo del VI Encuentro Iberoamericano de Protección de Datos, celebrado en Cartagena de Indias, Colombia, del 27 al 30 de mayo de 2008.

La Red no constituye un organismo internacional, y no cuenta con personalidad jurídica. Tampoco está conformada por los representantes de los gobiernos de los países participantes, sino únicamente por quienes pertenecen a algún organismo público cuya actuación impacte sobre la protección de datos personales en sus respectivos países. Por ello, puede concluirse que la Red es un espacio para compartir experiencias e impulsar la adecuada protección del derecho cuidando el valor que brindan distintas perspectivas, con el ánimo de fortalecer coincidencias.

Referencia: con amplitud cfr. Instituto Federal de Acceso a la Información y Protección de Datos, Libro Blanco 2006-2012, Volumen IV, Tomo III, México, Ed. IFAI, 2012, págs. 2-5.

Registro de esquemas de autorregulación

Los esquemas de autorregulación notificados en términos del último párrafo del artículo 44 de la Ley formarán parte de un registro, que será administrado por el Instituto y en el que se incluirán aquéllos que cumplan con los requisitos que establezcan los parámetros previstos en el artículo 43, fracción V de la Ley.

Referencia: artículo 86, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Registro de solicitudes

El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO. El plazo para que se atienda la solicitud empezará a computarse a partir del día en que la misma haya sido recibida por el responsable, en cuyo caso éste anotará en el acuse de recibo que entregue al titular la correspondiente fecha de recepción.

El plazo señalado se interrumpirá en caso de que el responsable requiera información al titular, en términos de lo dispuesto por el artículo siguiente.

Referencia: artículo 95, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Registro Público de Consumidores y Registro Público de Usuarios

El Registro Público de Consumidores previsto en la Ley Federal de Protección al Consumidor y el Registro Público de Usuarios previsto en la Ley de Protección y Defensa al Usuario de Servicios Financieros, continuarán vigentes y se regirán de conformidad con lo que establezcan las leyes en cita y las disposiciones aplicables que de ellas deriven.

Referencia: artículo 111, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Relación entre el responsable y el encargado

La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el

responsable, que permita acreditar su existencia, alcance y contenido.

Referencia: artículo 51, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Remisión. (Definiciones)

La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Remisiones de datos personales

Las remisiones nacionales e internacionales de datos personales entre un responsable y un encargado no requerirán ser informadas al titular ni contar con su consentimiento.

El encargado, será considerado responsable con las obligaciones propias de éste, cuando:

I. Destine o utilice los datos personales con una finalidad distinta a la autorizada por el responsable, o

II. Efectúe una transferencia, incumpliendo las instrucciones del responsable.

El encargado no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, remita los datos personales a otro encargado designado por este último, al que hubiera encomendado la prestación de un servicio, o transfiera los datos personales a otro responsable conforme a lo previsto en el presente Reglamento.

Referencia: artículo 53, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Requerimiento de información adicional

En el caso de que la información proporcionada en la solicitud sea insuficiente o errónea para atenderla, o bien, no se acompañen los documentos a que hacen referencia los artículos 29, fracción II y 31 de la Ley, el responsable podrá requerir al titular, por una vez y dentro de los cinco días siguientes a la recepción de la solicitud, que aporte los elementos o documentos necesarios para dar trámite a la misma. El titular contará con diez días para atender el requerimiento, contados a partir del día siguiente en que lo haya recibido. De no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente.

En caso de que el titular atienda el requerimiento de información, el plazo para que el responsable dé respuesta a la solicitud empezará a correr al día siguiente de que el titular haya atendido el requerimiento.

En caso de que el responsable no requiera al titular documentación adicional para la acreditación de su identidad o de la personalidad de su representante, se entenderá por acreditada la misma con la documentación aportada por el titular desde la presentación de su solicitud.

Referencia: artículo 96, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Requisitos de la denuncia

La denuncia deberá indicar lo siguiente:

I. Nombre del denunciante y el domicilio o el medio para recibir notificaciones, en su caso;

II. Relación de los hechos en los que basa su denuncia y los elementos con los que cuente para probar su dicho, y

III. Nombre y domicilio del denunciado o, en su caso, datos para su ubicación.

La denuncia podrá presentarse en los mismos medios establecidos para el procedimiento de protección de derechos.

Cuando la denuncia se presente por medios electrónicos a través del sistema que establezca el Instituto, se entenderá que se acepta que las notificaciones sean efectuadas por dicho sistema o a través de otros medios electrónicos generados por éste, salvo que se señale un medio distinto para efectos de las mismas.

Cuando las actuaciones se lleven a cabo como consecuencia de una denuncia, el Instituto acusará recibo de la misma, pudiendo solicitar la documentación que estime oportuna para el desarrollo del procedimiento.

Referencia: artículo 131, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Requisitos de la solicitud de protección de derechos

El promovente, en términos del artículo 46 de la Ley, deberá adjuntar a su solicitud de protección de derechos la información y documentos siguientes:

I. Copia de la solicitud del ejercicio de derechos que corresponda, así como copia de los documentos anexos para cada una de las partes, de ser el caso;

II. El documento que acredite que actúa por su propio derecho o en representación del titular;

III. El documento en que conste la respuesta del responsable, de ser el caso;

IV. En el supuesto en que impugne la falta de respuesta del responsable, deberá acompañar una copia en la que obre el acuse o constancia de recepción de la solicitud del ejercicio de derechos por parte del responsable;

V. Las pruebas documentales que ofrece para demostrar sus afirmaciones;

VI. El documento en el que señale las demás pruebas que ofrezca, en términos del artículo 119 del presente Reglamento, y

VII. Cualquier otro documento que considere procedente someter a juicio del Instituto.

Si el titular no pudiera acreditar que acudió con el responsable, ya sea porque éste se hubiere negado a recibir la solicitud de ejercicio de derechos ARCO o a emitir el acuse de recibido, lo hará del conocimiento del Instituto mediante escrito, y éste le dará vista al responsable para que manifieste lo que a su derecho convenga, a fin de garantizar al titular el ejercicio de sus derechos ARCO.

Referencia: artículo 116, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Requisitos para el ejercicio del derecho de rectificación

La solicitud de rectificación deberá indicar a qué datos personales se refiere, así como la corrección que haya de realizarse y deberá ir acompañada de la documentación que ampare la procedencia de lo solicitado. El responsable podrá ofrecer mecanis

mos que faciliten el ejercicio de este derecho en beneficio del titular.

Referencia: artículo 104, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Resolución

El procedimiento de verificación concluirá con la resolución que emita el Pleno del Instituto, en la cual, en su caso, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma establezca.

La resolución del Pleno podrá instruir el inicio del procedimiento de imposición de sanciones o establecer un plazo para su inicio, el cual se llevará a cabo conforme a lo dispuesto por la Ley y el presente Reglamento.

La determinación del Pleno será notificada al verificado y al denunciante.

Referencia: artículo 137, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Resoluciones

Las resoluciones del Instituto deberán cumplirse en el plazo y términos que las mismas señalen, y podrán instruir el inicio de otros procedimientos previstos en la Ley.

Referencia: artículo 125, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Responsabilidad

Se refiere a la disposición de la Directiva de referencia, que consiste en que:

1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido.

2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño.

Referencia: artículo 23, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Responsable

Es la persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Referencia: artículo 3, de la Ley Federal de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Responsable del tratamiento

Es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos, personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.

Referencia: artículo 2, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Robo de identidad, estafa, fraude, phishing, hurto, plagio, suplantación o usurpación de identidad. Véase: Suplantación de identidad.

Respuesta por parte del responsable

En todos los casos, el responsable deberá dar respuesta a las solicitudes de derechos ARCO que reciba, con independencia de que figuren o no datos personales del titular en sus bases de datos, de conformidad con los plazos establecidos en el artículo 32 de la Ley.

La respuesta al titular deberá referirse exclusivamente a los datos personales que específicamente se hayan indicado en la solicitud correspondiente, y deberá presentarse en un formato legible y comprensible y de fácil acceso. En caso de uso de códigos, siglas o claves se deberán proporcionar los significados correspondientes.

Referencia: artículo 98, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Restricciones al ejercicio de los derechos

El ejercicio de los derechos ARCO podrá restringirse por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceras personas, en los casos y con los alcances previstos en las leyes aplicables en la materia, o bien mediante resolución de la autoridad competente debidamente fundada y motivada.

Referencia: artículo 88, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Revocación del consentimiento

En cualquier momento, el titular podrá revocar su consentimiento para el tratamiento de sus datos personales, para lo cual el responsable deberá establecer mecanismos sencillos y gratuitos, que permitan al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.

Los mecanismos o procedimientos que el responsable establezca para atender las solicitudes de revocación del consentimiento no podrán exceder los plazos previstos en el artículo 32 de la Ley.

Cuando el titular solicite la confirmación del cese del tratamiento de sus datos personales, el responsable deberá responder expresamente a dicha solicitud.

En caso de que los datos personales hubiesen sido remitidos con anterioridad a la fecha de revocación del consentimiento y sigan siendo tratados por encargados, el responsable deberá hacer de su conocimiento dicha revocación, para que procedan a efectuar lo conducente.

Referencia: artículo 21, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

S

Sanciones y recursos; Europa

Es un principio básico para la protección de datos personales, que se refiere a que cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de Derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el segundo capítulo del Convenio número 108 del Consejo de Europa.

Referencia: artículo 10, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Seguridad de los datos, Convenio número 108 del Consejo de Europa

Es un principio básico para la protección de datos personales, en el Convenio de referencia, que consiste en que son las medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Referencia: artículo 7, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Seguridad de los datos, Ley Orgánica 15/1999; España

Es uno de los principios de la protección de datos personales, en la ley de referencia, que consiste en lo siguiente:

1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de la referida ley. *Referencia: artículo 9, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.*

Seguridad del tratamiento; Europa

Son las condiciones generales para la licitud del tratamiento de datos personales, en la Directiva de referencia, siguientes:

1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales. Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse.

2. Los Estados miembros establecerán que el responsable del tratamiento, en caso de tratamiento por cuenta del mismo, deberá elegir un encargado del tratamiento que reúna garantías suficientes en relación con las medidas de seguridad técnica y de organización de los tratamientos que deban efectuarse, y se asegure de que se cumplen dichas medidas.

3. La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular:

- que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento;

- que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato o del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente. *Referencia: artículo 17, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

Servicios de atención al público

Cuando el responsable disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados, podrá atender las solicitudes para el ejercicio de los derechos ARCO a través de dichos servicios, siempre y cuando los plazos no contravengan los establecidos en el artículo 32 de la Ley. En tal caso, la identidad del titular se considerará acreditada por los medios establecidos por el responsable para la identificación de los titulares en la prestación de sus servicios o contratación de sus productos, siempre que a través de dichos medios se garantice la identidad del titular.

Referencia: artículo 91, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Solicitud del consentimiento tácito

Cuando el responsable pretenda recabar los datos personales directa o personalmente de su titular, deberá previamente poner a disposición de éste el aviso de privacidad, el cual debe contener un mecanismo para que, en su caso, el titular pueda manifestar su negativa al tratamiento de sus datos

personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular.

En los casos en que los datos personales se obtengan de manera indirecta del titular y tenga lugar un cambio de las finalidades que fueron consentidas en la transferencia, el responsable deberá poner a disposición del titular el aviso de privacidad previo al aprovechamiento de los datos personales. Cuando el aviso de privacidad no se haga del conocimiento del titular de manera directa o personal, el titular tendrá un plazo de cinco días para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular. Si el titular no manifiesta su negativa para el tratamiento de sus datos de conformidad con lo anterior, se entenderá que ha otorgado su consentimiento para el tratamiento de los mismos, salvo prueba en contrario.

Cuando el responsable utilice mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que le permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en ese momento se deberá informar al titular sobre el uso de esas tecnologías, que a través de las mismas se obtienen datos personales y la forma en que se podrán deshabilitar.

Referencia: artículo 14, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Solicitud para autorización de medidas compensatorias

El procedimiento para que el Instituto autorice el

uso de medidas compensatorias de comunicación masiva, al que refiere el segundo párrafo del artículo anterior, iniciará siempre a petición del responsable.

El responsable presentará su solicitud directamente ante el Instituto o a través de cualquier otro medio que éste haya habilitado para tal efecto. La solicitud deberá contener la siguiente información:

I. Nombre, denominación o razón social del responsable que la promueva y, en su caso, de su representante, así como copia de la identificación oficial que acredite su personalidad y original para su cotejo. En el caso del representante, se deberá presentar copia del documento que acredite la representación del responsable y original para su cotejo;

II. Domicilio para oír y recibir notificaciones, y nombre de la persona autorizada para recibirlas;

III. Tratamiento al que pretende aplicar la medida compensatoria y sus características principales, tales como finalidad; tipo de datos personales tratados; si se efectúan transferencias; particularidades de los titulares, entre ellas edad, ubicación geográfica, nivel educativo y socioeconómico, entre otros;

IV. Causas o justificación de la imposibilidad de dar a conocer el aviso de privacidad a los titulares o el esfuerzo desproporcionado que esto exige. El responsable deberá informar sobre el número de titulares afectados, antigüedad de los datos, si existe o no contacto directo con los titulares, y su capacidad económica;

V. Tipo de medida compensatoria que pretende aplicar y por qué periodo la publicaría;

VI. Texto propuesto para la medida compensatoria, y

VII. Documentos que el responsable considere necesarios presentar ante el Instituto.

Referencia: artículo 33, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Solicitud del consentimiento expreso

Cuando el consentimiento expreso sea exigido en términos de una disposición legal o reglamentaria, el responsable deberá facilitar al titular un medio sencillo y gratuito para que, en su caso, lo pueda manifestar.

Referencia: artículo 16, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Soporte electrónico. (Definiciones)

Medio de almacenamiento al que se pueda acceder sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos personales, incluidos los microfilms.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Soporte físico. (Definiciones)

Medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Subcontratación de servicios

Toda subcontratación de servicios por parte del encargado que implique el tratamiento de datos personales deberá ser autorizada por el responsable, y se realizará en nombre y por cuenta de este último.

Una vez obtenida la autorización, el encargado deberá formalizar la relación con el subcontratado a través de cláusulas contractuales u otro instrumento jurídico que permita acreditar su existencia, alcance y contenido.

La persona física o moral subcontratada asumirá las mismas obligaciones que se establezcan para el encargado en la Ley, el presente Reglamento y demás disposiciones aplicables.

La obligación de acreditar que la subcontratación se realizó con autorización del responsable corresponderá al encargado.

Referencia: artículo 54, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Suplantación de identidad

Consiste en el accionar que se produce cuando una persona se hace pasar por un tercero, utilizando de forma no autorizada, su información personal o su documento de identidad sustraído o extraviado, para obtener así, el suplantador préstamos, tarjetas de crédito, teléfonos móviles, o cometer otros malos usos, fraudes o estafas en perjuicio de sus víctimas, los titulares verdaderos de los datos; también se denomina estafa, fraude, hurto, phishing, plagio, robo, suplantación o usurpación de identidad.

En la República Mexicana, se encontró como figura delictiva, establecida en formas diferentes en los códigos penales de las entidades federativas siguientes: Baja California, Baja California Sur, Ciu-

dad de México, Estado de México, Jalisco, Nayarit, Nuevo León, Quintana Roo, Sonora, Tamaulipas, Tlaxcala y Zacatecas.

Baja California. El Código Penal para el Estado de Baja California, en su artículo 175 Quinquies, establece: «al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación o suplantación en su identidad, se le impondrá pena de seis meses a seis años de prisión y de cuatrocientos a seiscientos días multa.

Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien además se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito así como en el supuesto de que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico reconocido en el rubro de la informática, telemática o sus afines.

Serán equiparables al delito de usurpación o suplantación de identidad y se impondrán las penas establecidas por este artículo, cuando se actúen las siguientes conductas:

I.- Al que por algún uso del medio informático, telemático o electrónico alcance un lucro indebido o genere un daño patrimonial para sí o para otro valiéndose de alguna manipulación informática o interceptación de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;

II.- Al que transfiera, posea o utilice datos identificativos de otra persona con la intención de cometer, intentar o favorecer cualquier actividad ilícita, y

III.- Al que asuma, suplante o se apropie o utilice a través del internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca».

Baja California Sur. El Código Penal para el Estado de Baja California Sur, en su artículo 363, establece: «al que por cualquier medio incluyendo el informático, usurpe o suplante a otro con fines ilícitos, para ejercer un derecho que legítimamente pertenezcan a otro o de apropiamiento de la identidad de otra persona, se le impondrá una pena de tres a seis años de prisión y multa de quinientos a seiscientos días.

La misma pena se impondrá a quien otorgue su consentimiento para que con fines ilícitos, otro lleve a cabo la usurpación de su identidad».

Además en su artículo 364, establece: «se equipara a la usurpación de identidad y se impondrán las mismas penas previstas en el artículo 363, las siguientes conductas:

I. Al que utilizando medios telemáticos o informáticos, valiéndose de alguna manipulación informática o de intersección de datos, accese a base de datos automatizadas no autorizadas y lleve a cabo el empleo no autorizado de datos personales o suplante identidades y obtenga un lucro indebido para sí o para otro;

II. A quien transfiera, posea o utilice sin autorización datos de identificación de otra persona con la intención de cometer o favorecer cualquier actividad ilícita; y

III. Al que asuma, suplante, se apropie, o utilice a través de internet o cualquier sistema informáti-

co, o medio de comunicación la identidad de una persona física o jurídica que no le pertenezca.

Se aumentará hasta en una mitad las penas previstas para las presentes conductas y suspensión del derecho de ejercer la actividad profesional por un lapso igual a la pena de prisión que corresponda cuando el sujeto activo tenga licenciatura, ingeniería o cualquier otro grado académico en carrera afín a la informática o telemática».

Ciudad de México. El Código Penal para el Distrito Federal, en su artículo 211 Bis, establece: «al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.

Se aumentaran en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo».

Estado de México. El Código Penal para el Estado de México, en su artículo 264, establece: «se le impondrán de uno a cuatro años de prisión y de cien a quinientos días multa, a quien ejerza con fines ilícitos un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.

Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el pár-

rafo que precede prevista en el presente artículo a quienes:

I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de la identidad;

II. Utilicen datos personales, sin consentimiento de quien deba otorgarlo;

III. Otorguen el consentimiento para llevar a cabo la usurpación de su identidad; y

IV. Se valgan de la homonimia para cometer algún ilícito.

Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos».

Jalisco. El Código Penal para el Estado de Jalisco, en su artículo 143-Quáter, establece: «comete el delito de suplantación de identidad quien suplante con fines ilícitos o de lucro, se atribuya la identidad de otra persona por cualquier medio, u otorgue su consentimiento para llevar la suplantación de su identidad, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona. Este delito se sancionará con prisión de tres a ocho años y multa de mil a dos mil salarios.

Serán equiparables al delito de suplantación de identidad y se impondrán las penas establecidas en este artículo:

I. Al que por algún uso de medio electrónico, telemático o electrónico obtenga algún lucro indebido para sí o para otro o genere un daño patrimonial a otro, valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo

objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;

II. Al que transfiera, posea o utilice datos identificativos de otra persona con la intención de cometer, favorecer o intentar cualquier actividad ilícita;

o
III. Al que asuma, suplante, se apropie o utilice, a través de internet, cualquier sistema informático o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona.

Se aumentará hasta en una mitad las penas previstas en el presente artículo, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito; así como en el supuesto en que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico en el rubro de informática, computación o telemática».

Nayarit. El Código Penal para el Estado de Nayarit, en su artículo 326, establece: «se le impondrán de tres a siete años de prisión y de cien a quinientos días multa, a quien ejerza con fines ilícitos, un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.

Se equiparan a la usurpación de identidad y se impondrán las penas previstas en el párrafo que precede a quienes:

I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de la identidad;

II. Utilicen datos personales, sin consentimiento de quien deba otorgarlo;

III. Otorguen el consentimiento para llevar a cabo la usurpación de su identidad, y

IV. Se valgan de la homonimia, parecido físico o similitud de la voz para cometer algún ilícito.

Las sanciones previstas en este artículo se impondrán con independencia de las que correspondan por la comisión de otro u otros delitos».

Nuevo León. El Código Penal para el Estado de Nuevo León, en su artículo 444, establece: «comete el delito de suplantación de identidad quien se atribuya por cualquier medio la identidad de otra persona, u otorgue su consentimiento para llevar la suplantación de su identidad, produciendo con ello un daño moral o patrimonial u obteniendo un lucro o un provecho indebido para sí o para otra persona. Este delito se sancionará con prisión de tres a ocho años y multa de mil a dos mil cuotas».

Quintana Roo. El Código Penal para el Estado Quintana Roo, en su artículo 195-Sexties (sic), establece: «el delito de usurpación se define como al que por cualquier medio usurpe o suplante con fines ilícitos o de lucro la identidad de una persona o otorgue consentimiento para llegar (sic) a cabo la usurpación o suplantación de su identidad, se le impondrá una pena de seis meses a seis años de prisión y de cuatrocientos a seiscientos días de multa».

Además, en su artículo 195-Septies, establece: «se equiparan a la usurpación de identidad y se im-

pondrán las mismas penas previstas en el artículo 195-Sexties a quienes:

I. Cometan un hecho ilícito previsto en las disposiciones legales con motivo de la usurpación de la identidad;

II. Utilicen datos personales sin consentimiento al que deba otorgarlo;

III. Otorguen el consentimiento para llevar a cabo la usurpación de su Identidad y se valgan de la homonimia para cometer algún ilícito, y

IV. Al que por algún uso del medio informático, telemático o electrónico, o use la red de Internet montando sitios espejos o de trampa captando información crucial para el empleo no autorizado de datos, suplante identidades, modifique indirectamente mediante programas automatizados imagen, correo o vulnerabilidad del sistema operativo cualquier archivo principal, secundario y terciario del sistema operativo que afecta la confiabilidad y variación de la navegación de la red para obtener lucro indebido.

En el supuesto que el activo tenga licenciatura, ingeniería o cualquier grado académico reconocido en los rubros mencionados, la pena se aumentará hasta en una mitad más».

Sonora. El Código Penal para el Estado de Sonora, en sus artículos 241 Bis, 241 Bis 1, y 241 Bis 2, establece: «artículo 241 Bis.- Al que por cualquier medio usurpe la personalidad o identidad de otra persona, con fines ilícitos, se le impondrá una pena

de dos a seis años de prisión y de cuatrocientos a seiscientos días multa.

Al que otorgare su consentimiento para ser suplantado por un tercero en su persona o identidad, con fines ilícitos, se le considerará igualmente responsable del delito previsto en el párrafo anterior o del contemplado en el artículo siguiente, aplicándose las mismas penas que al usurpador.

Artículo 241 Bis 1.- Cometerá también el delito de Usurpación de Personalidad o identidad y se impondrá una pena de dos a seis años de prisión y de cuatrocientos a seiscientos días multa, el que con el objeto de suplantar a otro con fines ilícitos, se acredite con la personalidad de éste, alterando, reproduciendo, falsificando, utilizando o proporcionando, ante terceros, cuando menos alguna de la siguiente información o documentos personales del suplantado:

- I.- Nombre;
- II.- Número de Seguridad Social;
- III.- Registro Federal de Contribuyentes;
- IV.- Clave Única de Registro de Población;
- V.- Clave de Elector;
- VI.- Números de Tarjeta de Crédito, números confidenciales y/o claves de acceso a servicios de banca por Internet, telefónicos o cualquier otro dato o elemento que permita el acceso a los servicios bancarios del afectado;
- VII.- Tarjetas de Crédito o plásticos bancarios del titular o adicionales;
- VIII.- Chequeras del titular de cuenta;
- IX.- Actas de Nacimiento o del Estado Civil;
- X.- Credencial para votar con fotografía o de elector;
- XI.- Licencia de conducir;
- XII.- Pasaporte;

- XIII.- Cédulas Profesionales;
- XIV.- Títulos Profesionales, Certificados o Constancias de Estudios;
- XV.- Credenciales Escolares o laborales;
- XVI.- Declaraciones Fiscales;
- XVII.- Documentos o Constancias laborales;
- XVIII.- Expedientes públicos o judiciales;
- XIX.- Boletas Prediales; Recibos de Agua, Teléfono, Suministro de Energía Eléctrica; Estado de Cuenta Bancarios y/o de Servicios;
- XX.- Poderes Notariales;
- XXI.- Huellas dactilares;
- XXII.- Grabaciones de voz;
- XXIII.- Imágenes de retina;
- XXIV.- Número de teléfono celular, de oficina, domicilio o cualquier otro que permita la ubicación del titular;
- XXV.- Firma Autógrafa;
- XXVI.- Firma Electrónica; o
- XXVII.- Cualquier información o documento que identifique física o electrónicamente a un individuo; o permita el acceso a sus bienes o patrimonio o responsabilidades.

Artículo 241 Bis 2.- En caso de que quien usurpe la personalidad o identidad de otro, se valga para ello de una homonimia, de la igualdad física genética entre hermanos gemelos, o del parecido físico con el suplantado, para cometer el ilícito, se aumentarán en una mitad las sanciones previstas en el Artículo 241 Bis, para este delito. La misma pena a que refiere este artículo se aplicará cuando el ilícito sea cometido por un servidor público aprovechándose de sus funciones, o por quien sin serio, se valga de su profesión o empleo para ello».

Tamaulipas. El Código Penal para el Estado de Tamaulipas, en su artículo 400 fracción V, es-

tablece: «V.- El apoderamiento material de documentos u objetos personales ajenos, con la finalidad de suplantar la identidad del propietario de éstos, o hacer uso de estos o de la información que contienen o acceder a ella por cualquier medio, con la finalidad de obtener un lucro para sí o para otro».

Tlaxcala. El Código Penal para el Estado de Tlaxcala, en su artículo 282, establece: «al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de dos a seis años de prisión y multa de cuatrocientos a seiscientos días de salario.

Se aumentaran en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo».

Zacatecas. El Código Penal para el Estado de Zacatecas, en su artículo 227 Bis, establece: «se sancionará con prisión de uno a cuatro años y multa de doscientas a trescientas cuotas, a quien ejerza ilícitamente un derecho o use cualquier tipo de datos, informaciones o documentos que legítimamente pertenezcan a otro, que lo individualiza ante la sociedad y que le permite a una persona física o jurídica colectiva ser identificada o identificable, para hacerse pasar por él.

Se equiparan a la usurpación de identidad y se impondrán las mismas penas previstas en el párrafo anterior a quienes otorguen el consentimiento para llevar a cabo la usurpación de identidad o se valgan de la homonimia, parecido físico o similitud de la voz para cometer algún ilícito.

Las sanciones previstas en este artículo se impondrán con independencia de las que correspon-

dan por la comisión de otro u otros delitos».

Supresión. (Definiciones)

Actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable.

Referencia: artículo 2, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Supuestos para la creación de bases de datos personales sensibles

En términos de lo previsto en el artículo 9, segundo párrafo de la Ley, sólo podrán crearse bases de datos que contengan datos personales sensibles cuando:

- I. Obedezca a un mandato legal;
- II. Se justifique en términos del artículo 4 de la Ley, o
- III. El responsable lo requiera para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persiga.

Referencia: artículo 56, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

T

Tercero

Es la persona física o moral nacional o extranjera, distinta del titular o del responsable de los datos.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Tercero; Europa

Es la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Referencia: artículo 2, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Tercero interesado

En caso de que no se haya señalado tercero interesado, éste podrá apersonarse en el procedimiento mediante escrito en el que acredite interés jurídico para intervenir en el asunto, hasta antes del cierre de instrucción. Deberá adjuntar a su escrito el documento en el que se acredite su personalidad cuando no actúe en nombre propio y las pruebas documentales que ofrezca.

Referencia: artículo 123, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Titular

Es la persona física a quien corresponden los datos personales.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Transferencia

Es toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Transferencias dentro del mismo grupo del responsable

En el caso de transferencias de datos personales entre sociedades controladoras, subsidiarias o afiliadas bajo el control común del mismo grupo del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable, el mecanismo para garantizar que el receptor de los datos personales cumplirá con las disposiciones previstas en la Ley, el presente Reglamento y demás normativa aplicable, podrá ser la existencia de normas internas de protección de datos personales cuya observancia sea vinculante, siempre y cuando éstas cumplan con lo establecido en la Ley, el presente Reglamento y demás normativa aplicable.

Referencia: artículo 70, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Tratamiento

Es la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Referencia: artículo 3, de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Tratamiento automatizado; Europa

Son las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión.

Referencia: artículo 2, del Convenio número 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

Tratamiento de datos personales; Europa

Es «tratamiento»: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

Referencia: artículo 2, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Tratamiento de datos personales en decisiones sin intervención humana valorativa

Cuando se traten datos personales como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, el responsable deberá informar al titular que esta situación ocurre.

Asimismo, el titular podrá ejercer su derecho de acceso, a fin de conocer los datos personales que se utilizaron como parte de la toma de decisión correspondiente y, de ser el caso, el derecho de rectificación, cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto, para que, de acuerdo con los mecanismos que el responsable tenga implementados para tal fin, esté en posibilidad de solicitar la reconsideración de la decisión tomada.

Referencia: artículo 112, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Tratamiento de datos personales en el denominado cómputo en la nube

Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente:

a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;

b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;

c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y

d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y

II. Cuento con mecanismos, al menos, para:

a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;

b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;

c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;

d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y

e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.

En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.

Para fines del presente Reglamento, por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.

Las dependencias reguladoras, en el ámbito de sus competencias, en coadyuvancia con el Instituto, emitirán criterios para el debido tratamiento de datos personales en el denominado cómputo en la nube.
Referencia: artículo 52, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Tratamiento de datos personales y libertad de expresión

Es la condición general para la licitud del tratamiento de datos personales, establecida en la Directiva de referencia, siguiente:

En lo referente al tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del capítulo II, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.
Referencia: artículo 9, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Tutela de los derechos; España

Es uno de los derechos de las personas, establecido en la ley de referencia, que consiste en lo siguiente:

1. Las actuaciones contrarias a lo dispuesto en la referida ley pueden ser objeto de reclamación por los interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del Organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Referencia: artículo 18, de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Tratamiento derivado de una relación jurídica

Cuando el tratamiento tenga como propósito cumplir con una obligación derivada de una relación jurídica, no se considerará para uso exclusivamente personal. *Referencia: artículo 6, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.*

Tratamiento para finalidades distintas

El responsable no podrá llevar a cabo tratamientos para finalidades distintas que no resulten compatibles o análogas con aquéllas para las que hubiese recabado de origen los datos personales y que hayan sido previstas en el aviso de privacidad, a menos que:

I. Lo permita de forma explícita una ley o reglamento, o

II. El responsable haya obtenido el consentimiento para el nuevo tratamiento.

Referencia: artículo 43, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Tratamiento para fines mercadotécnicos, publicitarios o de prospección comercial

Entre las finalidades del tratamiento a las que refiere la fracción II del artículo 16 de la Ley, en su caso, se deberán incluir las relativas al tratamiento para fines mercadotécnicos, publicitarios o de prospección comercial.

Lo anterior sin perjuicio de lo establecido por las disposiciones vigentes que regulen el tratamiento para los fines señalados en el párrafo anterior, cuando éstas contemplen una protección mayor para el titular que la dispuesta en la Ley y el presente Reglamento.

Referencia: artículo 30, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

U

Usurpación de identidad, estafa, fraude, hurto, phishing, plagio, robo, suplantación o usurpación de identidad.

Véase: Suplantación de identidad.

V

Visitas de verificación

El personal del Instituto que lleve a cabo las visitas de verificación deberá estar provisto de orden escrita fundada y motivada con firma autógrafa de la autoridad competente del Instituto, en la que deberá precisarse el lugar en donde se encuentra el establecimiento del responsable, o bien en donde se encuentren las bases de datos objeto de la verificación, el objeto de la visita, el alcance que deba tener la misma y las disposiciones legales que lo fundamenten.

Referencia: artículo 133, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Vulneraciones de seguridad

Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:

- I. La pérdida o destrucción no autorizada;
- II. El robo, extravío o copia no autorizada;
- III. El uso, acceso o tratamiento no autorizado, o
- IV. El daño, la alteración o modificación no autorizada.

Referencia: artículo 63, del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México.

Bibliografía

ALMUZARA ALMAIDA, Cristina, coordinadora, COUDERT, Fanny; MARZO PORTERA, Ana; NAVALPOTRO NAVALPOTRO, Yolanda, *Estudio práctico sobre la protección de datos de carácter personal*, 2.ª ed., España, Lex Nova, 2007.

BARBERIA, María Emma, *Diccionario de latín jurídico*, Argentina, Ed. Valletta ediciones, 2006.

BERLÍN VALENZUELA, Francisco, (Coordinador), MORENO COLLADO, Jorge, CAMPOSECO CADENA, Miguel Ángel, GONZÁLEZ OROPEZA, Manuel, MOLINA PIÑEIRO, Luis, NAMORADO URRUTIA, Pericles, OROZCO GÓMEZ, Javier, PEDROZA DE LA LLAVE, Susana Thalía, RIVERA ALVELAIS, Francisco, y VEGA VERA, David, *Diccionario universal de términos parlamentarios*, 2.ª ed., México, Cámara de Diputados del H. Congreso de la Unión, Comité del Instituto de Investigaciones Legislativas LVII Legislatura, Miguel Ángel Porrúa, 1998.

CORTÉS GONZÁLEZ, Jaime, GONZÁLEZ VÁZQUEZ, Horacio, LUGO GONZÁLEZ, Martín, y AMEZCUA ROSALES, Carlos Guillermo, *Diccionario de derecho a la protección de datos personales*, México, Umbral, 2010.

CORTÉS GONZÁLEZ, Jaime, *Prontuario de derecho a la protección de datos personales*, México, Amate, 2008.

CISNEROS FARÍAS, Germán, *Diccionario de frases y aforismos latinos*, México, Ed. Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2003.

DE GORTARI DE GORTARI, Elí Eduardo, *Diccionario de la lógica*, México, Plaza y Valdés Editores, reimpresión 1988.

FERNÁNDEZ FERNÁNDEZ, Antonio, *Diccionario de dudas: A-H*, España, Ediciones Nobel, Ediciones de la Universidad de Oviedo, 2007.

GARCÍA TORRES, Antonio, *La protección de datos personales en México*, México, publicado por el Senado de la República, 2006.

GÓMEZ-ROBLEDO VERDUZCO, Alonso y ORNELAS NUÑEZ, Lina, *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*, México, Universidad

Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2006.

GUZMÁN GARCÍA, María de los Ángeles, en *Diccionario de derecho procesal constitucional convencional*, 2.ª ed., México, Consejo de la Judicatura Federal y la Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2014.

INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS, *Libro Blanco 2006-2012*, Volumen IV, Tomo III, México, IFAI, 2012.

NICOLIELLO, Nelson, *Diccionario del latín jurídico*, Argentina, Ed. Euros Editores S.R.L., reimpresión 2004.

REAL ACADEMIA ESPAÑOLA, *Diccionario de la Lengua Española*, Tomo 2 h/z, 23.ª ed., Edición del Tricentenario, México, Espasa Libros S.L.U.-Editorial Planeta Mexicana, S.A., de C.V., 2014.

QUÉS, María Elena, *Datos personales y nuevas tecnologías*, Argentina, Edu.car. Ministerio de Educación Presidencia de la Nación, 2014.

TAMAYO Y TAMAYO, Mario, *Diccionario de la investigación científica*, 2.ª ed., México, Limusa Noriega Editores, 2004.

Documentación:

Insituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *Guía para el borrado seguro de datos personales*, México, INAI, 2006

Insituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *Guía para prevenir el robo de identidad*, México, INAI, 2006

Hemerografía:

Boletín Oficial del Estado, número 4. Suplemento. Publicado el jueves 4 de enero de 2001, pág. 112. Sentencia pronunciada por el Pleno del Tribunal Constitucional Español, en el recurso de inconstitucionalidad número 1463-2000, parte II, fundamentos jurídicos, apartado 7. Reino de España.

PIÑAR MAÑAS, José Luis, “La mirada europea. Protección de datos personales”, en Revista Nexos, México, D. F., año 29 vol. XXIX núm. 353 mayo de 2007.

Jurisprudencia mexicana:

Jurisprudencia (común), tesis: PC.I.A. J/12 K (10a.) Registro No. 2 006 753, el Pleno en Materia Administrativa del Primer Circuito, en *Gaceta*

del Semanario Judicial de la Federación,
México, Décima Época, Libro 7, junio de 2014,
Tomo II, pág. 1127.

Legislación y documentación extranjera:

Convenio número 108 del Consejo de Europa para la
protección de las personas con respecto al
tratamiento automatizado de datos de carácter
personal.

Directiva 95/46/CE del Parlamento Europeo y
del Consejo de 24 de octubre de 1995 relativa a
la protección de las personas en lo que respecta
al tratamiento de datos personales y a la libre
circulación de estos datos.

Directiva 2006/24/CE del Parlamento Europeo y
del Consejo de 15 de marzo de 2006.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección
de Datos de Carácter Personal. España.

Legislación federal vigente de México:

Constitución Política de los Estados Unidos Mexicanos.
Publicada en el Diario Oficial de la Federación
el 5 de febrero de 1917.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación, de la Secretaría de Gobernación, el día lunes 5 de julio de 2010. Estados Unidos Mexicanos.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, expedida el 10 de junio de 2002. México.

Ley General de Transparencia y Acceso a la Información Pública, publicada el 4 de mayo de 2015. México.

Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. España.

Legislación federal vigente de México:

Constitución Política de los Estados Unidos Mexicanos. Publicada en el Diario Oficial de la Federación el 5 de febrero de 1917.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicada en el Diario Oficial de la Federación, de la Secretaría de Gobernación, el día lunes 5 de julio de 2010. Estados Unidos Mexicanos.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, expedida el 10 de junio de 2002. México.

Ley General de Transparencia y Acceso a la Información Pública, publicada el 4 de mayo de 2015. México



Diccionario de derecho mexicano
a la protección de datos personales en posesión
de los particulares

se terminó de imprimir
en octubre de 2016
en los talleres gráficos
de Amate Editorial, S.A. de C. V.
Madero 616, Centro
Guadalajara, Jalisco
Tel-fax: 36120751
36120068

amateditorial@gmail.com
www.amateeditorial.com.mx

Otros títulos de los autores

