

Protección de Datos Personales en el sector privado



Edgardo Martínez Rojas
Director General de Normatividad y
Estudios

Noviembre 2011

I. Los datos personales y el derecho a la protección de los mismos

¿Qué son los datos personales?

Los datos personales son toda la información concerniente o relativa a una persona física identificada o identificable, tales como:

✓ **Datos de identificación**

Nombre, edad, domicilio, sexo, RFC, CURP...

✓ **Datos patrimoniales**

Cuentas bancarias, saldos, propiedades...

✓ **Datos de salud**

Estados de salud físico y mental...

✓ **Datos biométricos**

Huellas dactilares, iris, palma de la mano...

✓ **Otros**

Ideología, afiliación política, religión, origen étnico, preferencia sexual...

- ✓ Es un **derecho fundamental de tercera generación** que busca la protección de la persona en relación con el tratamiento de su información.
- ✓ Es el **poder de disposición y control** que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso (también denominado **derecho a la autodeterminación informativa**).

II. La protección de los datos personales a nivel internacional

La protección de datos personales a nivel mundial

Directrices de la OCDE (1980)

Convenio 108 (1981)

Resolución 45/95 de la ONU (1990)

Directiva 95/46/CE(1995)

Marco de Privacidad de APEC
(1999)

Carta de Derechos Fundamentales
de la Unión Europea (2000)

Directrices de Armonización de la
Red Iberoamericana (2007)

Estándares internacionales o
Resolución de Madrid (2009)

Las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales recomiendan:

- ✓ Que los países miembros tengan en cuenta en su legislación interna los principios básicos aplicables a la protección de la privacidad y las libertades individuales, establecidos en este documento.
- ✓ Que los estados miembros se esfuercen por eliminar o evitar que aparezcan, en nombre de la protección de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales.
- ✓ Que los países miembros colaboren en la implantación de las Directrices.
- ✓ Que los estados miembros convengán los procedimientos de consulta y cooperación para la aplicación de estas Directrices.

El Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal tiene como finalidad garantizar, en el territorio de cada Estado Parte, el respeto de los derechos y libertades fundamentales de toda persona física, concretamente su derecho a la vida privada, sin importar su nacionalidad y residencia, con respecto al trato automatizado de sus datos ya sea en el sector público o privado.

Esta resolución contiene los principios rectores para la reglamentación de los ficheros computadorizados de datos personales. Dichos principios son los siguientes:

- ✓ Licitud y lealtad
- ✓ Exactitud
- ✓ Finalidad
- ✓ Acceso de la persona interesada
- ✓ No discriminación
- ✓ Facultad de establecer excepciones
- ✓ Seguridad
- ✓ Control y sanciones
- ✓ Flujo de datos a través de las fronteras
- ✓ Campo de aplicación

- ✓ Amplía los principios ya recogidos en otros instrumentos internacionales.
- ✓ Permite la transferencia de datos personales de un Estado Miembro a un tercer país sólo cuando éste garantice un nivel de protección adecuado, salvo ciertas excepciones.
- ✓ Indica que cada Estado Miembro debe disponer de una o más autoridades de control a efecto de velar por la aplicación de esta Directiva en su territorio.
- ✓ Alienta la elaboración de códigos de conducta nacionales y comunitarios que contribuyan a una correcta aplicación de las disposiciones nacionales y comunitarias.
- ✓ Crea un grupo para la protección de las personas en lo que respecta al tratamiento de datos personales.

El Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico (APEC) promueve un acercamiento flexible a la protección de la privacidad de la información en las economías miembros de APEC, evitando la creación de barreras innecesarias para los flujos de información.

El artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea reconoce el derecho a la protección de datos como un derecho fundamental y autónomo, distinto al derecho a la intimidad y la privacidad de las personas.

Ofrecen a los poderes públicos de los Estados Iberoamericanos criterios orientativos para el desarrollo de iniciativas normativas en esta materia, facilitando el establecimiento de un marco homogéneo que favorezca el intercambio de los flujos de información entre los Estados y terceros Estados bajo estándares similares de protección.

- ✓ Contiene los estándares internacionales para la protección de la privacidad, en relación con el tratamiento de datos de carácter personal, que fueron acogidos en la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.
- ✓ Determina y define un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de los datos personales, facilitando los flujos internacionales de éstos en un mundo globalizado.

III. La protección de los datos personales en México

El derecho a la protección de datos personales está previsto a nivel constitucional en los artículos 6, 16 y 73, fracción XXIX-O.

✓ **Las fracciones II y III del artículo 6 constitucional** tienen la virtud de ser las primeras menciones constitucionales expresas que hacen un reconocimiento del derecho a la protección de datos personales y se constituyen como limitantes al ejercicio del derecho de acceso a la información. Estas fracciones señalan que:

- La información a que se refiere la vida privada será protegida en términos de la ley respectiva.
- Toda persona tiene derecho a acceder y rectificar sus datos personales.

- ✓ **El segundo párrafo del artículo 16 constitucional** establece, por su parte, que cualquier persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición.
- ✓ **El artículo 73, fracción XXIX-O constitucional** prevé que el Congreso tiene la facultad para legislar en materia de protección de datos personales en posesión de particulares.



El sistema de protección de datos personales a nivel federal

La protección de datos personales en México se garantiza a través de dos piezas legislativas:

- ✓ Al **sector público federal** le es aplicable la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG).
- ✓ Al **sector privado** le es aplicable la Ley Federal de Protección de Datos Personales en posesión de los Particulares (LFPDPPP).

Ambos documentos dotan al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) de atribuciones para garantizar el ejercicio de este derecho.

Objeto de la LFPDPPP y sujetos obligados

- ✓ La LFPDPPP se publicó en el Diario Oficial de la Federación el 5 de julio de 2010.
- ✓ Tiene el propósito de proteger 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 derecho a la autodeterminación informativa de las personas.
- ✓ Es aplicable para todas las personas físicas o morales de carácter privado que para sus actividades cotidianas recaben, manejen y utilicen información personal en territorio nacional, con excepción de:
 - Las Sociedades de Información Crediticia.
 - Las personas que recolectan y almacenan datos personales para uso exclusivamente personal o doméstico.

- ✓ Consentimiento
- ✓ Información
- ✓ Licitud
- ✓ Lealtad
- ✓ Finalidad
- ✓ Calidad
- ✓ Proporcionalidad
- ✓ Responsabilidad

- ✓ La manifestación de la voluntad del titular es la principal causa legitimadora del tratamiento de los datos personales, salvo excepciones. El consentimiento puede ser expreso o tácito.
- ✓ El consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.
- ✓ El consentimiento es tácito cuando el titular accede al tratamiento de sus datos una vez que habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

No se necesita el consentimiento del titular para efectuar el tratamiento de sus datos personales cuando:

- ✓ Se haya previsto esta circunstancia en una Ley.
- ✓ Los datos se encuentren en fuentes de acceso público.
- ✓ Los datos se hayan sometido a un proceso de disociación.
- ✓ Se pretenda cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable.
- ✓ Exista una situación de emergencia que pueda dañar a una persona o a sus bienes.
- ✓ Los datos sean indispensables para la atención médica, prevención, diagnóstico, prestación de asistencia sanitaria o tratamiento médico, y el titular no pueda otorgar el consentimiento.
- ✓ Se dicte una resolución de autoridad competente.

- ✓ Este principio consiste en dar a conocer efectivamente a los titulares la existencia misma del tratamiento y las características esenciales de éste, en términos que les resulten fácilmente comprensibles y previo a la obtención de los datos.
- ✓ El **aviso de privacidad** es la herramienta que se utiliza para lograr lo anterior. Es una declaración escrita o verbal que informa al titular cómo, por qué y para qué se tratarán sus datos personales, así como los derechos que le otorga la Ley.
- ✓ En julio de 2011 las empresas debieron expedir los avisos de privacidad correspondientes.

Contenido del aviso de privacidad:

- ✓ La identidad y domicilio del responsable.
- ✓ Las finalidades del tratamiento.
- ✓ Las opciones ofrecidas al titular para limitar el uso y divulgación de sus datos.
- ✓ Los mecanismos para ejercer los derechos ARCO (acceso, rectificación, cancelación y oposición).
- ✓ Las transferencias de datos que se efectúen.
- ✓ El procedimiento para notificar cambios en el aviso de privacidad.
- ✓ El señalamiento expreso de datos sensibles.
- ✓ Los datos personales recabados.
- ✓ Los mecanismos para revocar el consentimiento.
- ✓ La cláusula para aceptar o rechazar las transferencias.

- ✓ El tratamiento de los datos personales deberá llevarse a cabo de forma leal y lícita; es decir, con pleno cumplimiento de la legalidad y respeto de la buena fe y los derechos del individuo cuya información es sometida a tratamiento.
- ✓ El tratamiento únicamente será llevado a cabo en el ámbito de finalidades determinadas, explícitas y legítimas relacionadas con las actividades del responsable.
- ✓ La calidad del dato ha de entenderse específicamente vinculada a su veracidad y exactitud, de forma que aquél refleje fielmente la realidad de la información tratada.

- ✓ Sólo se deberán recabar los datos adecuados o necesarios para la finalidad que justifica el tratamiento.
- ✓ El tratamiento obedecerá a tratar la mínima cantidad de información necesaria para conseguir la finalidad perseguida.
- ✓ Tiene que prevalecer el deber del responsable de velar por el cumplimiento de los principios y rendir cuentas al titular en caso de incumplimiento, independientemente de quién realice el tratamiento y si es dentro o fuera del país donde se recabó la información.

Figuras en materia de datos personales

Figura	Características
Titular	✓ Persona física a quien corresponden los datos personales.
Responsable	✓ Persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales.
Encargado	✓ Persona física o jurídica que sola o conjuntamente con otras trata datos personales por cuenta del responsable.
Departamento de Datos	✓ Persona o área que da trámite a las solicitudes de derechos ARCO. ✓ Fomenta la protección de datos personales dentro de la organización.
Tercero	✓ Persona física o moral, nacional o extranjera, distinta del titular, responsable y encargado.

Derecho	Derechos del titular
Acceso	✓ Acceder a sus datos personales. ✓ Conocer el aviso de privacidad.
Rectificación	✓ Rectificar sus datos personales cuando sean inexactos o incompletos.
Cancelación	✓ Cancelar sus datos personales previo bloqueo.
Oposición	✓ Oponerse al tratamiento de sus datos personales por causa legítima.

Plazos para ejercer derechos ARCO



**Solicitud de
Derechos ARCO**



**Ante el
Responsable**

Prorrogables por un plazo igual

**20 días hábiles
determinación
adoptada**

**15 días
hábiles
efectivo el
derecho**



Comunicación al Titular

**La entrega es gratuita,
por regla general**

✓ **Sus facultades normativas:**

- Interpretar en el ámbito administrativo la LFTAIPG y la LFPDPPP.
- Emitir criterios y recomendaciones para garantizar el pleno derecho a la protección de datos personales.
- Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información.
- Expedir regulación en materia de protección de datos en coadyuvancia con las dependencias de la APF.

- ✓ **Sus facultades en materia de cooperación nacional e internacional:**
 - Acudir a foros internacionales en la materia.
 - Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos personales.

- ✓ **Sus facultades sancionadoras:**
 - Llevar a cabo el procedimiento de imposición de sanciones.



Procedimiento para la defensa de los derechos ARCO ante el IFAI

Sector público. Recurso de revisión (LFTAIPG)	Sector privado. Procedimiento de protección de derechos (LFPDPPP)
Reconoce la tutela de los derechos de acceso y rectificación.	Reconoce la tutela de los derechos de acceso, rectificación, cancelación y oposición. Se podrá hacer efectivo hasta febrero de 2012.
Plazo máximo de 50 días hábiles prorrogables por una sola vez.	Plazo máximo de 50 días hábiles prorrogables por una sola vez.
La resolución es definitiva e inatacable para los sujetos obligados.	Los sujetos regulados podrán impugnar las resoluciones del IFAI promoviendo el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.
No prevé un mecanismo de conciliación.	Un elemento innovador de esta Ley es el procedimiento conciliatorio que las partes -responsable y titular- podrán llevar a cabo para solucionar el conflicto en cualquier etapa del procedimiento de protección de derechos.



Otros procedimientos que se sustancian ante el IFAI de acuerdo con la LFPDPPP

Verificación	Imposición de sanciones
<p>Inicia:</p> <ul style="list-style-type: none">✓ De oficio: derivada del incumplimiento a resoluciones dictadas con motivo de procedimiento de protección de derechos.✓ A petición de parte: cuando se presuma fundada y motivadamente, la existencia de violaciones a la ley.	<p>Este procedimiento se detona cuando el IFAI tiene conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de la LFPDPPP como consecuencia del desahogo del procedimiento de protección de derechos o del procedimiento de verificación.</p>
<p>El IFAI tendrá acceso a la información y documentación que considere necesaria y los servidores públicos estarán obligados a guardar la confidencialidad sobre la información que conozcan.</p>	<p>Prevé un periodo para la presentación y desahogo de pruebas, al término del cual el IFAI deberá resolver en definitiva.</p>
<p>En el Reglamento de la LFPDPPP se desarrollará la forma, términos y plazos en que se sustanciará este procedimiento.</p>	<p>En el Reglamento de la LFPDPPP se desarrollará la forma, términos y plazos en que se sustanciará este procedimiento.</p>

- ✓ La LFPDPPP prevé una serie de conductas consideradas como infracciones, las cuales serán castigadas con las siguientes sanciones:
- ✓ No atender la solicitud del titular → apercibimiento.
- ✓ Tratar datos en contra de los principios, omitir el aviso de privacidad, mantener datos personales inexactos, declarar dolosamente la inexistencia de datos, etc. → multa.
- ✓ Incumplir el deber de confidencialidad, cambiar sustancialmente de finalidad sin avisar al titular, vulnerar la seguridad de las bases, transferir datos sin consentimiento del titular, etc. → multa.
- ✓ Los montos pueden incrementarse por:
 - Reincidencia o
 - Por tratarse de datos sensibles.

Periodos de implementación de la LFPDPPP

Plazo	Actividad
6 de julio de 2010	✓ Ley entra en vigor.
2011	✓ Ejecutivo expide Reglamento.
Julio 2011	✓ Empresas designan a persona/departamento que atenderá a particulares.
	✓ Empresas emiten aviso de privacidad.
Enero de 2012	✓ Titulares pueden ejercer derechos ARCO ante responsables.
Febrero de 2012	✓ Particulares pueden presentar su solicitud de protección de derechos al IFAI.

El IFAI busca construir un compromiso de corresponsabilidad con todos los actores involucrados, a fin lograr un alto nivel de acatamiento de la LFPDPPP en aras de una efectiva protección de los datos personales.

IV. Casos prácticos en el ámbito internacional

- ✓ En 1998 la Sra. Bodil Lindqvist subió una página a Internet con información personal de sus compañeros de parroquia, en la cual incluyó sus nombres, teléfonos, aficiones, situación familiar y en un caso hizo alusión a la lesión del pie de una de sus compañeras.
- ✓ El caso se denunció y el Ministerio Fiscal inició un proceso penal en su contra. La Sra. Lindqvist fue condenada a pagar una multa de 450 euros, pero recurrió la sentencia.
- ✓ El Tribunal de Apelación Sueco planteó varias dudas al Tribunal de Justicia de las Comunidades Europeas (TJE) sobre la interpretación de la Directiva 95/46/CE en este caso.
- ✓ La importancia de este asunto reside en que fue la primera sentencia que el TJE resolvió sobre la interpretación de dicha Directiva, a petición de un Estado Miembro.

Así, el TJE fijó los siguientes criterios en este caso:

- ✓ La publicación en Internet del nombre de una persona y sus datos personales como teléfono y aficiones sí constituye un tratamiento automatizado de datos personales.
- ✓ La expresión "datos de salud" comprende la información sobre aspectos físicos y psíquicos de la salud de una persona.
- ✓ No constituye una transferencia de datos personales a terceros países la publicación de una página web en un país estando el servidor en ese mismo país.
- ✓ La Directiva 95/46/CE no entraña la restricción al principio de libertad de expresión. Las autoridades y tribunales deben garantizar el equilibrio justo entre los derechos e intereses en juego.
- ✓ Los Estados pueden extender su normatividad interna a situaciones no comprendidas por la Directiva.

Caso de la webcam en diario deportivo

- ✓ Un Diario Deportivo Español colocó una webcam de baja resolución en sus instalaciones, la cual recogía imágenes del interior de la redacción cada 15 segundos. Las imágenes se difundían en Internet para reflejar la actividad del Diario y enriquecer la información ofrecida por éste a través de la red.
- ✓ El Diario explicó esta práctica a los empleados en una asamblea general de trabajadores pero nunca recabó su consentimiento.
- ✓ Una empleada denunció el hecho ante la Agencia Española de Protección de Datos, la cual impuso una multa de 6,000 euros al Diario por no haber recabado el consentimiento de los afectados.

- ✓ Este caso refleja la importancia de informar a los empleados sobre lo que se hace con sus datos personales.
- ✓ No basta sólo con informar, sino que los datos personales nunca deben emplearse para fines que superen la propia organización del trabajo y los procedimientos de gestión internos de una institución o empresa.

Caso de la opositora número 1

- ✓ En julio de 2003, Marta adquirió unos libros a una Academia para utilizarlos en un examen de oposición. A efecto de que se le enviaran las facturas de compra, ella entregó su nombre y domicilio a la Academia.
- ✓ Marta obtuvo el primer lugar en el concurso de oposición del puesto de Ayudante Técnico Sanitario, lo cual se publicó en el portal del Ministerio de Sanidad y Consumo.
- ✓ La Academia se enteró de que su compradora fue la "opositora número 1" y en la publicidad de la Academia incluyó el nombre y apellidos de Marta. Se imprimieron mil folletos publicitarios.

Caso de la opositora número 1

- ✓ Marta denunció este hecho ante la Agencia Española de Protección de Datos porque su nombre estaba usándose sin su consentimiento y para una finalidad distinta para la cual ella entregó los datos.
- ✓ La Agencia sancionó a la Academia con una multa de 60,000 euros porque los datos no pueden utilizarse para finalidades incompatibles con aquellas para las que fueron recogidos.
- ✓ Con este caso se demuestra que los datos personales que poseen las empresas de sus clientes sirven para llevar a cabo operaciones de tráfico mercantil, sin que en ningún caso deban emplearse para otras finalidades no previstas por la empresa, no comunicadas al interesado y, sobre todo, no consentidas por los auténticos dueños de los datos.