

# **Garantía y Protección de los Datos Personales en la Ciudad de México**

**Agustín Millán Gómez  
Comisionado Ciudadano del Instituto de  
Acceso a la Información Pública del  
Distrito Federal.**

## Contenido

Introducción. ....	3
I. Qué es la protección de datos personales.....	3
II. El caso de México en la protección de los datos personales. Ámbito Federal. ....	5
III. La Protección de datos personales en el Distrito Federal .....	9
IV. Sistematización de los datos personales .....	11
VI. Derechos ARCO y procedimiento para su ejercicio. ....	16
VIII. Conclusiones .....	19

## **Introducción.**

La protección de datos de carácter personal es una de las claves esenciales del respeto a la vida privada dentro de la defensa de los derechos humanos y las libertades fundamentales, por ello es importante que las leyes de transparencia y acceso a la información pública contemplen, como excepción al derecho de acceso, el derecho a la vida privada y la intimidad de las personas, excepto en los casos en los que existan intereses colectivos superiores que justifiquen una intromisión en este derecho personalísimo.

En este sentido, el desarrollo de las tecnologías de la información, cuyo crecimiento ha permitido la obtención y transmisión de grandes bases de datos, ha dado también como resultado el que la protección de datos personales haya cobrado mayor relevancia, pues si bien, estas innovaciones ofrecen grandes ventajas en términos de eficiencia y productividad, también permiten el almacenamiento masivo de información que concierne a las personas lo que, potencialmente, permitiría la creación de perfiles que pueden emplearse inadecuadamente y provocar injerencias arbitrarias o ilegales en la vida privada.

Esta situación ha generado que las legislaciones nacionales y supranacionales se dieran a la tarea de reforzar las garantías de los ciudadanos frente a la nueva amenaza tecnológica, sobre todo, a través de leyes de protección de datos personales.

En el caso de México, debemos mencionar que a nivel federal no existe, hasta el día de hoy, una ley específica que regule la protección de datos personales en posesión tanto de entidades públicas como privadas, aunque existen disposiciones que se encuentran dispersas en diversos ordenamientos jurídicos, en particular en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Por su parte, en el Distrito Federal existe, desde el año de 2008, una Ley de Protección de Datos Personales para los entes públicos, en la cual se establecen los principios y derechos aplicables al tratamiento de estos datos, mismos que analizaremos en el desarrollo del presente trabajo.

### **I. Qué es la protección de datos personales.**

La protección de datos personales es un derecho que consiste en ofrecer a los individuos los medios para controlar el uso ajeno de la información personal que les concierne.<sup>1</sup>

---

<sup>1</sup> LUCAS MURILLO DE LA CUEVA, Pablo, "La protección de datos en la administración de justicia", en: *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, España, 2004, p.233.

Este derecho, también conocido como *habeas data* es, por un lado, un instrumento legal para proteger el derecho a la vida privada y, por otro, una forma de derecho de acceso a la información, que consiste en que todo individuo tenga garantizado el derecho de acceder a la información que le concierne personalmente. La denominación y configuración autónoma de un derecho a la autodeterminación informativa constituyen una realidad relativamente reciente, si tomamos en cuenta que las primeras leyes sobre protección de datos aparecieron en los años setenta.<sup>2</sup>

Sin embargo, el primer documento vinculante en cuanto a la protección de los referidos derechos fue el *Convenio N° 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*. Dicho documento internacional fue el primero en establecer, en los territorios de los Estados parte, la garantía, para cualquier persona física, sin importar su nacionalidad o residencia, del 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.<sup>3</sup>

Fue con dicho documento que los Estados miembros del Consejo de Europa, signatarios del referido convenio, consideraron necesario ampliar la protección de los derechos y las libertades fundamentales de cada individuo, específicamente el respeto de la vida privada, sin dejar de lado el derecho de la libre circulación de la información entre los pueblos.

Asimismo, el origen de este derecho se vincula al desarrollo de la noción de protección de la privacidad, adquiriendo posteriormente, un perfil conceptual y alcance más diferenciado al punto de convertirse en un derecho autónomo y distinto al de intimidad:

*La función del derecho fundamental a la protección de datos es garantizar a toda persona el poder de control sobre sus datos personales, tanto su uso como su destino, con el propósito de impedir su tráfico ilícito y la potencial vulneración de la dignidad del afectado. Esto lleva implícito el poder de disposición sobre sus datos. Por el contrario, la función del derecho a la intimidad es proteger de cualquier invasión los reductos de vida personal o familiar que la persona desea mantener fuera del saber de terceros o de evitar intromisiones contra su propia voluntad.<sup>4</sup>*

---

<sup>2</sup> LUCAS MURILLO DE LA CUEVA, Pablo, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, España, 1990, p. 25.

<sup>3</sup> Artículo 1, Convenio N° 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. En <http://www.habeasdata.org.co/wp-content/uploads/2009/01/convenio108-1981.pdf>. 8 de octubre de 2009.

<sup>4</sup> ABAD AMORÓS, Ma. Rosa, "La protección de datos" en: *Derecho de la Información*, BEL Y CORREIDORA (coords.), Ariel, 2003, España, p.357.

En este sentido, y de una definición amplia de este derecho, indica que comprende la prerrogativa que toda persona tiene para:

- a) conocer de su inclusión en bancos de datos o registros;
- b) acceder a toda información que sobre ella conste en los bancos de datos o registros;
- c) actualizar o corregir, en su caso, la información que sobre ella conste en los bancos de datos o registros;
- d) conocer el propósito o fines para los que se va a utilizar la información que conste sobre ella en los bancos de datos;
- e) que se garantice la confidencialidad de determinada información obtenida legalmente para evitar su conocimiento por terceros y
- f) que se garantice la supresión de información sobre la persona con datos sobre su filiación política o gremial, creencias religiosas, vida íntima y toda aquella que pudiera de un modo u otro producir discriminación.<sup>5</sup>

El derecho a la protección de datos personales está integrado por una serie de prerrogativas, principios y procedimientos para el tratamiento de información que concierne a personas físicas, no sólo por parte del Estado o los entes públicos sino también, por parte de terceros o personas de derecho privado.

Este poder de control sobre los datos personales se manifiesta a través de los denominados derechos ARCO (acceso, rectificación, cancelación y oposición), a través de los cuales las personas tienen la facultad de conocer, en todo momento, quién dispone de sus datos y a para qué están siendo utilizados. También es posible la rectificación de los datos en caso de que resulten incompletos o inexactos o, en su caso, la cancelación de los mismos por no ajustarse a las disposiciones aplicables. Asimismo, los titulares de los derechos tienen la posibilidad de oponerse al uso de sus datos si es que los mismos fueron obtenidos sin su consentimiento.

Finalmente, un pilar fundamental para la efectiva protección de datos personales, se encuentra representado por la existencia de órganos garantes que cuenten con un cierto grado de autonomía de gestión e independencia frente a los poderes estatales típicos y ante los cuales los particulares puedan exigir la tutela de sus derechos relacionados con la protección de datos personales.

## **II. El caso de México en la protección de los datos personales. Ámbito Federal.**

---

<sup>5</sup> VILLANUEVA, Ernesto, *Derecho de acceso a la información pública en Latinoamérica*, UNAM, México, 2003, p. XXV.

Hasta el 20 de julio de 2007, el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos (CPEUM) contenía, únicamente, la garantía de acceso a la información y la de libertad de expresión, dicho precepto señalaba:

**Artículo 6o.** *La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho a la información será garantizado por el Estado.*

Posteriormente, y con la adición realizada al referido artículo, se incluyó un párrafo que refiere a la protección de los datos personales, el principio de máxima publicidad, la gratuidad de la información, el principio de rectificación, entre otros principios fundamentales para el desarrollo de la protección de los datos personales. El artículo se lee de la siguiente manera:

**Artículo 6°.-** *La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.*

*Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:*

**I.** *Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.*

**II.** *La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.*

**III.** *Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.*

**IV.** *Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.*

**V.** *Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.*

**VI.** *Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.*

**VII.** *La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.*

Asimismo, el primer semestre del año de 2009 fue muy fructífero en cuanto a la *constitucionalización* de la protección de los datos personales, pues dos artículos más fueron adicionados, estos son el 16 y el 73, los cuales establecen lo siguiente: *(el orden de cita obedece a las fechas en las cuales cada artículo fue adicionado)*

**Artículo 73<sup>6</sup>.** *El Congreso tiene facultad:*

...

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

Al respecto, el artículo Segundo Transitorio del *Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos*, establece que el Congreso de la Unión debe expedir la ley de la materia dentro del plazo de 12 meses, a partir de la entrada en vigor del mismo, por tanto, dicha ley tendrá que ser expedida antes del 4 de mayo de 2010.

Por su parte, el Tercero Transitorio prevé que, en tanto se expide esta ley, continuarán vigentes las disposiciones sobre el particular dictadas por las legislaturas estatales, tales como la Ley de Protección de Datos Personales del Estado de Colima, la cual establece, en su artículo 2º, que es aplicable a los datos en posesión del sector público y privado, así como el Código Civil para el Estado de Jalisco, que contiene normas que resultan aplicables a los datos personales contenidos en registros particulares (artículo 40 bis).

Por su parte, el artículo 16 dispone:

**Artículo 16<sup>7</sup>.** *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 legítima 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 terceros.*

[...]

Las adiciones al artículo 16 constitucional revisten especial importancia debido a la inclusión de los derechos ARCO en la legislación general mexicana, lo que forja la creación de un derecho subjetivo, exigible por todos los gobernados.

---

<sup>6</sup> Publicado en el Diario Oficial de la Federación el día 30 de abril de 2009.

<sup>7</sup> Publicado en el Diario Oficial de la Federación el día 1 de junio de 2009.

Ahora bien, en el año 2002 fue creado por decreto presidencial, el Instituto Federal de Acceso a la Información Pública (IFAI)<sup>8</sup>, que es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información a nivel federal; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades federales.

Al respecto, resulta conveniente resaltar que en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, se localiza un capítulo completo dedicado a la protección de los datos personales en poder del Estado, el Capítulo IV, del Título I de la referida Ley establece, entre otras cuestiones, que los sujetos obligados son responsables de los datos personales, los cuales deben ser tratados de forma adecuada, pertinente y no excesiva en relación con los propósitos para los cuales se hayan obtenido. Asimismo, los entes públicos se encuentran obligados, de oficio, a sustituir, rectificar o completar los datos personales que fueren inexactos, ya sea total o parcialmente.

En este sentido, y como excepción a los principios de clasificación y reserva de los datos personales en poder de los entes públicos, así como del de previo consentimiento del titular de los datos para ser proporcionados, se encuentran algunos supuestos en los cuales los sujetos obligados pueden entregar y transferir datos personales; así por ejemplo, el caso en el que, por instrucción judicial, se ordene al ente público la entrega de ciertos datos personales o cuando se transmitan entre sujetos obligados o entre dependencias y entidades ciertos datos personales, siempre y cuando éstos se utilicen para el ejercicio de facultades propias de los mismos.

Finalmente y contra la negativa de entregar o corregir datos personales, resulta procedente la interposición de un recurso de revisión ante el IFAI.

Ahora bien, en el ámbito federal existen diversas disposiciones aplicables a la protección de los datos personales en poder del Estado, entre ellas podemos señalar las siguientes:

- Ley de Información Estadística y Geográfica.
- Ley para regular las Sociedades de Información Crediticia.
- Ley Federal de Protección al Consumidor.
- Código Federal de Instituciones y Procedimientos Electorales
- Ley General de Salud.

---

<sup>8</sup> <http://www.ifai.org.mx/Acercafai/Marco>. 8 de octubre de 2009.

No obstante, al día de hoy, no existe en el ámbito federal una ley específica, concreta y delimitada que se dedique, exclusivamente, a la protección de los datos personales<sup>9</sup>.

### III. La Protección de datos personales en el Distrito Federal

Desde la promulgación de la primera Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (LTAIPDF) en el año de 2003, ya se encontraba un capítulo dedicado a la protección de los datos personales en posesión de los entes públicos; sin embargo, con la entrada en vigor de la nueva LTAIPDF, en el mes de mayo de 2008, se excluyó la tutela de los datos personales, así como el capítulo relativo al sistema de archivos, estableciendo en sus artículos transitorios la obligación de la Asamblea Legislativa de aprobar la legislación respectiva a datos personales y archivos públicos del Distrito Federal.<sup>10</sup>

Fue así como el 4 de octubre de 2008, se publicó la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF) y no obstante que en dicha ley no se encuentra una definición de “protección de datos personales”, la LTAIPDF la define como “*la garantía que tutela la privacidad de datos personales en poder de los entes públicos*”.

Ahora bien, la LPDPDF tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos. En este sentido, y en referencia al concepto de datos personales, establece:

*Datos personales: La información numérica, alfabética, gráfica acústica o de cualquier otro tipo concerniente a una persona física identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos<sup>11</sup>.*

---

<sup>9</sup> Al respecto, considero importante señalar que se han presentado ante el Congreso de la Unión algunas iniciativas para la creación de una Ley de Datos Personales Federal, entre las que destacan aquellas que pugnan por la creación de un Instituto especializado y encargado de proteger y velar por la aplicación de la normatividad de protección de datos, y otras que señalan la necesidad de otorgar dicha facultad de interpretación y aplicación de la Ley de Datos al Instituto Federal de Acceso a la Información Pública (IFAI).

<sup>10</sup> Sobre este particular, los asambleístas consideraron que por su relevancia estas materias deberían contar con una ley específica. La LPDPDF se publicó en la Gaceta Oficial del Distrito Federal el 3 de octubre de 2008 y la Ley de Archivos local el 8 del mismo mes y año.

<sup>11</sup> Artículo 2, Ley de Protección de Datos Personales para el Distrito Federal

En relación con dicho concepto, algunos estudiosos de la materia han señalado que la intención del legislador es que la definición de datos personales sea tan amplia como sea posible con el fin de incluir toda información referente a una persona identificable como, por ejemplo, el nombre, firma, huella, fotografías, imágenes de vídeo e incluso grabaciones sonoras.

En este sentido, la LPDPDF establece que la interpretación de la misma debe ser conforme a la Constitución y a los distintos instrumentos internacionales suscritos por México en materia de derechos humanos, así como la interpretación que sobre los mismos hayan realizado los órganos internacionales respectivos.

Esta previsión otorga atribuciones a los órganos que aplican la Ley, como es el caso del Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF), de contar con una amplia gama de herramientas interpretativas, pues se tiene la posibilidad de acudir a los textos de las sentencias dictadas por órganos protectores de derechos humanos en el ámbito internacional, como es el caso de la Comisión y la Corte Interamericana de Derechos Humanos.

En este punto, resulta importante mencionar que el InfoDF es un órgano autónomo del Distrito Federal con personalidad jurídica y patrimonio propio, así como con autonomía presupuestaria de operación y de decisión en materia de transparencia y acceso a la información pública.

El InfoDF, es el encargado de dirigir y vigilar el cumplimiento de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y de la Ley de Protección a Datos Personales del Distrito Federal; por tanto, sus objetivos son los de garantizar el derecho de acceso a la información pública, la transparencia, la rendición de cuentas, así como la protección de los datos personales que obran en los archivos de la Administración Pública del D.F.

Ahora bien, la LPDPDF, a efecto de garantizar la debida protección de los datos personales, además de establecer los derechos ARCO, incluye una serie de principios rectores en el tratamiento de este tipo de datos, como son el de finalidad, calidad, consentimiento, deber de información, seguridad, confidencialidad, disponibilidad y temporalidad. El incumplimiento de estos principios constituye una vulneración a la protección de datos personales.

Asimismo, los principios generales de protección de datos constituyen el contenido esencial del derecho a la protección de datos personales y configuran un sistema de tutela que garantiza un uso racional de los datos personales.

Dado su carácter obligatorio, el responsable del sistema debe adoptar las medidas necesarias para evitar que se produzca una vulneración de los mismos, lo que traería como consecuencia la comisión de una infracción a la Ley, situación por la cual resulta de suma importancia que todos los servidores públicos que intervengan en el tratamiento de los datos personales, conozcan y respeten estos principios.

#### IV. Sistematización de los datos personales

La Ley establece que un sistema de datos personales consiste en todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso<sup>12</sup>.

La cuestión a dilucidar es cómo identificar si estamos en presencia de un sistema de datos personales o no y, por tanto, si hay obligación de cumplir con las disposiciones que la LPDPDF determina.

En la práctica, la identificación de estos sistemas no es una labor sencilla, pues cotidianamente los entes públicos en el desarrollo de sus funciones utilizan datos personales, pero en muchas ocasiones éstos datos no están incorporados a un sistema como tal.

Sin embargo, existen algunos factores que pueden resultar útiles a la hora de determinar si estamos ante un sistema de datos personales, éstos son: la finalidad, los usos previstos, las personas de las que se obtendrán los datos, la descripción de éstos y el órgano responsable del sistema.

Por tanto, podemos afirmar que estamos en presencia de un sistema de datos personales, si nos encontramos ante un conjunto de datos que se obtienen de un colectivo de personas para el cumplimiento de una finalidad determinada. Esta finalidad, comúnmente, está estrechamente vinculada al ejercicio de competencias legales y al cumplimiento de funciones administrativas; por lo cual, serán las funciones y atribuciones normativas que desarrolla un determinado ente público, en el ámbito de su competencia, y que requieren se recabe información personal de los ciudadanos, las que darán lugar a la identificación de un sistema de datos personales.

Así, al interior de un sujeto obligado por la LPDPDF nos encontraremos, al menos, con sistemas de datos personales relativos al personal que labora en el ente, así como con sistemas de proveedores y, dependiendo de su actividad específica, habrá sistemas de beneficiarios, contribuyentes, becarios, prestadores de servicio social y otros sistemas específicos que obedecerán a la especialidad de las atribuciones que tiene cada institución.

Entonces, un sistema de datos personales, **será un conjunto organizado de datos de carácter personal**, cualquiera que sea su soporte y organización, siempre que tenga una estructura que permita un fácil acceso a los datos de una persona determinada.

---

<sup>12</sup> Capítulo II del Título Segundo “De la tutela de datos personales”.

Ahora bien, por disposición legal<sup>13</sup>, a cada ente público le corresponde determinar a través de su titular, la creación, modificación y supresión de sistemas de datos personales de acuerdo a su ámbito de competencia; así por ejemplo, en el caso de la Jefatura de Gobierno, correspondería a su titular, el Jefe de Gobierno, esta determinación, en el caso del InfoDF, correspondería al Pleno, al ser éste la instancia directiva del Instituto, en tanto que dicha facultad en el caso del Instituto Electoral del Distrito Federal está atribuida al Consejo General. Esto dependerá de la estructura de cada ente.

Por otra parte, tal determinación debe ser publicada en la Gaceta Oficial del Distrito Federal, la que deberá incluir, en los casos de creación o modificación de sistemas de datos personales, al menos, los siguientes aspectos:

- a) La finalidad del sistema de datos personales y los usos previstos para el mismo;
- b) Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos;
- c) El procedimiento de recolección de los datos de carácter personal;
- d) La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo;
- e) De la cesión de las que pueden ser objeto los datos;
- f) Las instancias responsables del tratamiento del sistema de datos personales;
- g) La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición; y
- h) El nivel de protección exigible.

En tanto que en las disposiciones que se dicten para la supresión de sistemas de datos personales se deberá indicar el destino que vaya a darse a los datos contenidos en los mismos o, en su caso, las medidas previstas para su destrucción, de la cual podrán excluirse aquellos datos que, previa disociación, sean tratados para finalidades estadísticas o históricas.

La publicación, en la Gaceta Oficial del Distrito Federal, de los acuerdos por medio de los cuales se determina la creación de un sistema de datos personales, además de darle publicidad al acto, permite dotar a dichos acuerdos de fuerza normativa, pues los interesados cuentan con certeza jurídica acerca de la finalidad del tratamiento que van a recibir los datos que proporcionen y de la instancia a la que pueden acudir a ejercer los derechos que la Ley otorga.

---

<sup>13</sup> Artículo 7 LPDPDF.

Por otra parte, los sistemas de datos personales en posesión de los entes públicos deben inscribirse en el Registro que al efecto habilita el InfoDF, lo cual permitirá a los interesados conocer los sistemas de datos personales que obran en las distintas dependencias locales lo que facilita, también, el ejercicio de los derechos ARCO.

La información que debe contener el registro es similar a la que debe contener el acuerdo de creación de un sistema de datos personales:

CREACIÓN	REGISTRO
I. La identificación del sistema de datos personales, indicando su denominación y normativa aplicable, así como la descripción de la finalidad y usos previstos.	I. Nombre del Sistema y, en su caso, fecha de publicación en la Gaceta Oficial del Distrito Federal;
II. El origen de los datos, indicando el colectivo de personas sobre las que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos; su procedencia (propio interesado, representante, ente público, etcétera) así como el procedimiento de obtención de los mismos (formulario, Internet, transmisión electrónica, etcétera).	II. Nombre y cargo del responsable del sistema.
III. La estructura básica del sistema con descripción detallada de datos identificativos y, en su caso, de los especialmente protegidos, así como las restantes categorías de datos de carácter personal; modo de tratamiento utilizado en su organización (manual o automatizado). En su caso, señalar los datos de carácter obligatorio y facultativo.	III. Identificación del sistema, finalidades y usos previstos, así como el soporte en el que se encuentra;
IV. Las cesiones de datos que se tengan previstas, indicando, en su caso, los destinatarios o categorías de destinatarios.	IV. La categoría de los datos personales contenidos en el sistema, forma de recolección y actualización de los mismos;
V. La identificación de la unidad administrativa a la que corresponde el sistema de datos personales, así como del cargo del responsable.	V. Unidad administrativa en la que se encuentra el sistema;
VI. Domicilio oficial y dirección electrónica de la Oficina de Información Pública ante la cual se presentarán las solicitudes para ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento.	VI. Destino y personas físicas o morales a las que puedan ser transmitidos;
VII. Indicación del nivel de seguridad que resulte aplicable: básico, medio o alto.	VII. Modo de interrelacionar la información contenida en el sistema y el plazo de conservación de los datos;
	VIII. Teléfono y correo electrónico del responsable;
	IX. Normativa aplicable al sistema; e
	X. Indicación del nivel de seguridad aplicable: básico, medio o alto.

Un principio fundamental que se regula en la LPDPDF, es la obligación de cumplir con el denominado “**deber de información**” o “derecho de información al interesado”, el cual constituye el fundamento previo necesario para el correcto funcionamiento de un esquema jurídico de protección de datos, ya que resultaría altamente complejo que los interesados pudieran ejercer derechos tales como el de acceso o de oposición al tratamiento de sus datos, si previamente no conocen en qué sistema y bajo qué parámetros serán tratados sus datos.

En este sentido, los entes públicos tienen la obligación de informar a los interesados, al momento de recabar sus datos personales, de forma expresa, precisa e inequívoca lo siguiente (artículo 9):

- I. De la existencia de un sistema de datos personales, del tratamiento de datos personales, de la finalidad de la obtención de éstos y de los destinatarios de la información;
- II. Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas;
- III. De las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos;
- IV. De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por disposición de una Ley sean considerados públicos;
- V. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y
- VI. Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

Para el cumplimiento de esta obligación, el InfoDF emitió un acuerdo por medio del cual aprobó la leyenda que deben utilizar los entes públicos para informar a los interesados de estas advertencias:

***“Los datos personales recabados serán protegidos, incorporados y tratados en el Sistema de Datos Personales (nombre del sistema de datos personales), el cual tiene su fundamento en (fundamento legal que faculta al Ente público para recabar los datos personales), cuya finalidad es (describir la finalidad del sistema) y podrán ser transmitidos a (destinatario y finalidad de la transmisión), además de otras transmisiones previstas en la Ley de Protección de Datos Personales para el Distrito Federal.***

***Los datos marcados con un asterisco (\*) son obligatorios y sin ellos no podrá acceder al servicio o completar el trámite (indicar el servicio o trámite de que se trate)***

***Asimismo, se le informa que sus datos no podrán ser difundidos sin su consentimiento expreso, salvo las excepciones previstas en la Ley.***

***El responsable del Sistema de datos personales es (nombre del responsable), y la dirección donde podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, así como la revocación del consentimiento es (indicar el domicilio de la Oficina de Información Pública correspondiente).***

***El interesado podrá dirigirse al Instituto de Acceso a la Información Pública del Distrito Federal, donde recibirá asesoría sobre los derechos que tutela la Ley de Protección de Datos Personales para el Distrito Federal al teléfono: 5636-4636; correo electrónico: datos.personales@infodf.org.mx o www.infodf.org.mx”***

Asimismo, se prevé que si los datos no fueron obtenidos directamente del interesado, el ente público deberá hacer de su conocimiento los aspectos que conforman el deber de información dentro de un plazo de tres meses y que no habrá obligación de hacerlo si el interesado fue informado con anterioridad de que sus datos están incorporados en un sistema, del tratamiento, finalidad, y destinatarios de la información; de una posible difusión, en la que habrá que otorgar su consentimiento expreso, salvo que por ley sean considerados públicos; y, de la posibilidad de ejercer los derechos ARCO.

En caso de que los datos personales procedan de fuentes de acceso público tampoco habrá obligación de informar al interesado estos aspectos, ni tampoco si alguna ley así lo prevé expresamente o, en caso de que resulte material o jurídicamente imposible o requiera de esfuerzos desproporcionados, en razón del número de interesados y/o la antigüedad de los datos.

Otro principio básico en materia de protección de datos que fue incorporado a la LPDPDF, es el relativo a los **datos especialmente protegidos**, conocidos como datos sensibles, como lo son el origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual.

En este sentido, resulta importante señalar que la protección de datos personales sensibles tiene como objetivo dificultar la identificación de personas por sus características íntimas que las hacen más vulnerables, se trata, en definitiva, de una protección que se basa en el riesgo de discriminación o de persecución política, social, racial o religiosa.

Además de lo relativo a los datos sensibles, la LPDPDF también hace referencia a los sistemas creados con fines administrativos por instituciones de seguridad pública, estableciéndose que los mismos quedarán sujetos al régimen general de protección de la Ley.

En cuanto a los datos de carácter personal obtenidos para fines policiales, se establece (artículo 11) que los mismos pueden ser recabados sin consentimiento y que los datos deben estar limitados a los supuestos y categorías que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención o persecución de los delitos.

Asimismo, se establece que los datos personales recabados con fines policiales se cancelarán cuando dejen de ser necesarios para las investigaciones que motivaron su almacenamiento.

## **VI. Derechos ARCO y procedimiento para su ejercicio.**

Un aspecto fundamental de los sistemas jurídicos en materia de protección de datos lo constituye el establecimiento en las leyes de los denominados derechos ARCO:

- A.** Acceso
- R.** Rectificación
- C.** Cancelación
- O.** Oposición

La posibilidad de ejercer estos derechos es lo que dota a la persona de una verdadera facultad de disposición sobre sus propios datos personales ya que mediante ellos puede conocer qué datos tienen los entes públicos, rectificarlos en caso de errores, cancelarlos si dejaron de ser necesarios y oponerse a su tratamiento si es que fueron obtenidos sin su consentimiento.

La Ley establece la posibilidad de ejercer los derechos ARCO a toda persona y precisa que se trata de derechos independientes por lo que el ejercicio de alguno no es condicionante ni impedimento para ejercer otro.

Por tanto, cualquier persona puede ejercitar los derechos de acceso, rectificación, cancelación y oposición sobre datos de carácter personal que le conciernan tratados por los entes públicos. Siendo un requisito indispensable el de la identificación del interesado o de su representante legal.

Mediante los derechos ARCO toda persona tiene derecho a que se le informe gratuitamente del origen de los datos y a saber a qué otras personas o entidades, sean de derecho público o privado, han sido comunicados sus datos personales, derecho que se complementa con el de rectificar la información incorrecta o no actualizada, así como con el derecho a solicitar que se destruyan aquellos datos que sean inexactos o incompletos, o aquéllos que no cumplan el principio de adecuación con la finalidad para la que se recabaron.

Ahora bien, el procedimiento para el ejercicio de los derechos ARCO se hará de conformidad con lo dispuesto en el Capítulo II, del Título Cuarto de la LPDPDF “De los derechos y del procedimiento para su ejercicio”. Asimismo, deberán observarse las disposiciones contenidas en los “Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del Sistema INFOMEX del Distrito Federal” y las de los “Lineamientos para la protección de datos personales en el Distrito Federal”.

Sólo el titular de los datos, llamado interesado, o su representante legal, pueden solicitar el acceso, rectificación, cancelación y oposición sobre datos personales. El procedimiento comenzará con la presentación de la solicitud ante la Oficina de Información Pública (OIP) del ente público que corresponda y podrá presentarse por los siguientes medios:

- I. Por **escrito material** ante la Oficina de Información Pública (OIP), o enviado por correo ordinario, certificado o mensajería;
- II. **Verbal**, de manera oral y directa, la cual será capturada por el responsable de la OIP en el formato respectivo e ingresada al sistema INFOMEX;
- III. **Correo electrónico** a la dirección de correo electrónico asignada a la OIP;
- IV. Por el sistema electrónico **INFOMEX**
- V. Vía telefónica, al 5636-4636, a través del servicio **TELINFO**.

La solicitud debe indicar los siguientes requisitos:

- I. **Ente público** a quien se dirija;
- II. **Nombre** completo del interesado y, en su caso, el de su representante legal;
- III. **Descripción** clara y precisa **de los datos** personales respecto de los que se busca ejercer algún derecho ARCO;
- IV. Cualquier **otro elemento** que facilite su **localización**;
- V. El **domicilio**, mismo que se debe encontrar dentro del **Distrito Federal**, u otro **medio** para recibir notificaciones (correo electrónico, OIP, si no lo indica se notificará por estrados).

Además de éstos se prevén requisitos específicos dependiendo del derecho a ejercer:

- **Acceso:** indicar la modalidad en la que prefiere se otorgue el acceso que puede ser consulta directa, copias simples o certificadas.
- **Rectificación:** señalar el dato erróneo y la corrección que deba realizarse, acompañado de la documentación que lo avale.
- **Cancelación:** indicar las razones por las cuales se considera que el tratamiento de los datos no se apega a las disposiciones normativas.
- **Oposición:** señalar los motivos por los que no se está de acuerdo en el uso o difusión de los datos.

Recibida la solicitud el ente público cuenta con un plazo de quince días hábiles para responderla, plazo que podrá ampliarse por un periodo igual si existe causa justificada para ello.

En caso de que la solicitud no sea clara o no cumpla con todos los requisitos, la OIP puede, dentro del plazo de cinco días, después de recibida la solicitud, pedir al solicitante que corrija las deficiencias, quien tendrá cinco días para hacerlo o, de lo contrario, no se dará trámite a la solicitud, pues se tendrá por no presentada. Cabe precisar que requerimiento interrumpe el plazo para dar respuesta.

Recibida la solicitud se deberá emitir una respuesta, dentro del plazo de quince días hábiles (ampliables), en donde se notificará si la misma fue o no procedente. De ser procedente, esto es que el ente dé una respuesta positiva a la petición, lo hará del conocimiento del solicitante al medio indicado para recibir notificaciones para que, dentro de los diez días siguientes, se haga efectiva tal determinación.

De no ser procedente, la respuesta deberá contener las razones y las normas jurídicas aplicables que determinaron la negativa. Dicha respuesta debe estar suscrita y firmada, tanto por el responsable del sistema como por el titular de la OIP del ente público que corresponda, pudiendo recaer ambas funciones en la misma persona.

En caso de que los datos personales sobre los cuales se pretende ejercer un derecho ARCO no sean localizados en los sistemas del ente, se deberá elaborar un acta, que deberá ser notificada al solicitante dentro del plazo de respuesta, en la que se dará cuenta de los sistemas en que fueron buscados los datos personales, acta que deberá estar firmada por un representante del órgano interno de control, del titular de la OIP y del responsable del sistema de datos personales.

Independientemente del medio a través del cual se reciba la solicitud, la identidad del interesado o la personalidad, identidad y facultades de su representante legal, se acreditarán en el momento que se presenten en la OIP correspondiente para obtener la respuesta sobre la solicitud de sus datos personales.

Para acreditar la identidad del titular o representante legal, se deberá presentar documento oficial en original.

La Ley establece que el trámite de la solicitud es gratuito, lo cual constituye un principio comúnmente adoptado en las leyes sobre la materia. Sin embargo, se prevé que el solicitante debe cubrir los costos de reproducción de los datos solicitados según lo previsto en el Código Financiero, los cuales se cobrarán de manera previa a la entrega de la información y se calcularán atendiendo a los costos de los materiales, del envío y, en su caso, de la certificación de documentos.

Finalmente, y en caso de que la persona se considere agraviada con la respuesta del ente público que haya recaído a su solicitud para ejercer cualquiera de los derechos ARCO o ante la omisión de la misma, resulta procedente la interposición de un recurso de revisión ante en InfoDF, quien se guiará por lo dispuesto en la LTAIPDF para dar trámite y resolución al mismo.

## VIII. Conclusiones

El Distrito Federal está a la vanguardia en materia de protección de datos personales, pues es una de las pocas entidades dentro de la República mexicana, junto con Colima, Guanajuato y Oaxaca, que cuenta con una ley específica en la materia y la única que, dentro de su capitulado, detalla los aspectos que deben contener las medidas de seguridad en sus distintos niveles –básico, medio y alto-, medidas que revisten dos características principales.

En primer lugar, se trata de medidas mínimas exigibles, por lo que los entes públicos obligados al cumplimiento de la Ley deberán observarlas sin perjuicio de que, cuando el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos presentes lo ameriten, deban adoptarse medidas adicionales necesarias para garantizar la protección y resguardo de la información.

En segundo lugar, estas medidas son acumulativas, lo que significa que al nivel medio le aplicarán las medidas de seguridad previstas para el nivel básico, además de las del propio nivel medio y las del nivel alto implicarán la adopción de las medidas de los niveles anteriores y las propias del nivel alto.

Una cuestión que vale la pena destacar es que la única ley en la materia aplicable tanto al sector público como al privado es la de Colima, la cual otorga protección a los datos personales en posesión de estos sectores dentro de dicho Estado.

Por otro lado, debemos también hacer mención a otra norma estatal: a la Ley de Información Pública, Estadística y Protección de Datos Personales del Estado de Morelos, la cual, si bien no es específica sobre la materia que nos ocupa, dedica el Título IV a regular aspectos fundamentales para la garantía de este derecho como la que establece que ninguna persona está obligada a dar información que pudiera propiciar expresión de discriminación e intolerancia sobre su persona, honor, reputación y dignidad, disposición que recoge el principio de especial protección a los datos sensibles.

En el ámbito federal, a pesar de no contar con una ley específica, los datos personales en posesión de entidades federales, gozan de protección en virtud de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y también han sido expedidas normas específicas para la protección de los datos personales, como es el caso de los Lineamientos de Protección de Datos Personales expedidos por el IFAI y aplicables a toda la Administración Pública Federal.

Vale la pena señalar que, en el nivel federal, en los ámbitos legislativo y judicial, la protección de datos personales ha sido objeto de desarrollo reglamentario tanto en el Congreso de la Unión, compuesto por las Cámaras de Diputados y de Senadores, como en la Suprema Corte de Justicia de la Nación y del Consejo de

la Judicatura Federal, órgano de administración y vigilancia de los Juzgados y Tribunales federales.

Finalmente, solo nos resta esperar a que próximamente sea publicada la Ley Federal de Protección de Datos Personales, aplicable a las entidades privadas, para que este derecho sea una realidad nacional y las personas cuenten con la protección que este derecho otorga ante todas las instancias, públicas o privadas.