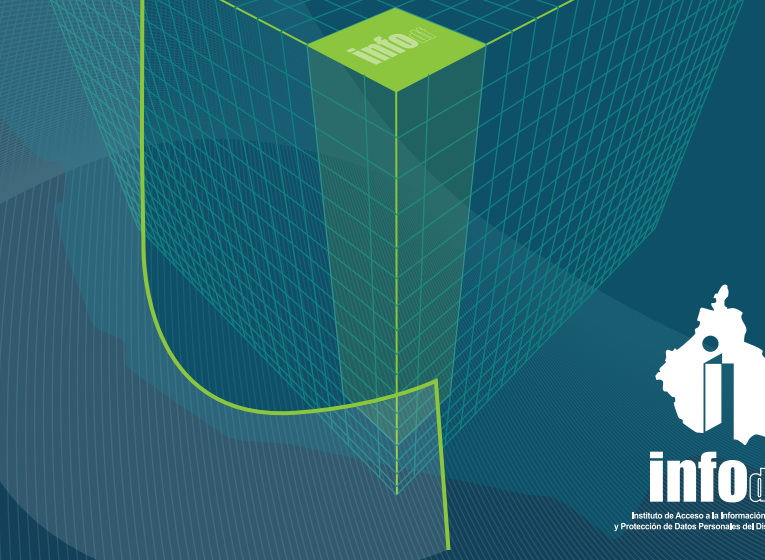
Transparencia y Datos Personales en el Distrito Federal

Texto de apoyo a la formación de servidores públicos en el conocimiento de las leyes de transparencia y protección de datos personales

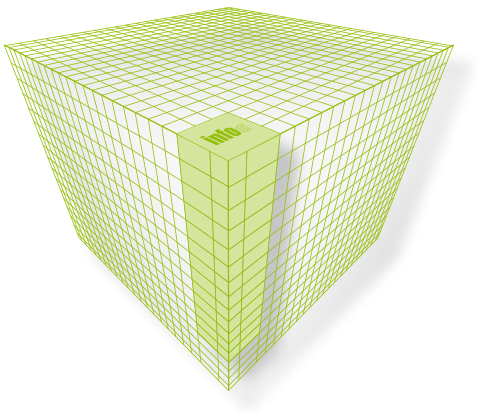


infodf
Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal

Transparencia

y Datos Personales en el Distrito Federal

Texto de apoyo a la formación de servidores públicos
en el conocimiento de las leyes de transparencia
y protección de datos personales

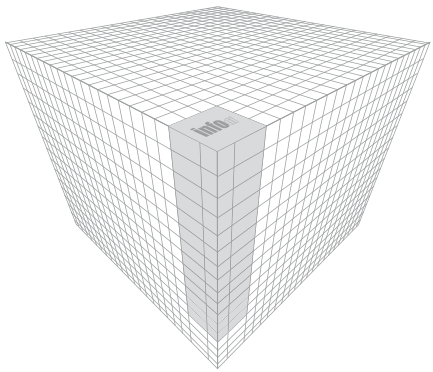


INSTITUTO DE ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES DEL DISTRITO FEDERAL
La Morena 865, Col. Narvarte Poniente, Del. Benito Juárez, México D.F. C.P. 03020
Teléfono: 56 36 21 20
www.infodf.org.mx
Ejemplar de distribución gratuita, prohibida su venta
Diseño y formación: InfoDF
Impreso en México en los talleres de Servicio Editorial Gráfico y/o Omar Aguilar Sánchez

Transparencia

y Datos Personales en el Distrito Federal

Texto de apoyo a la formación de servidores públicos
en el conocimiento de las leyes de transparencia
y protección de datos personales



Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal | infodf

DIRECTORIO

Oscar M. Guerra Ford
Comisionado Ciudadano Presidente

Jorge Bustillos Roqueñí
Comisionado Ciudadano

Areli Cano Guadiana
Comisionada Ciudadana

Salvador Guerrero Chiprés
Comisionado Ciudadano

Agustín Millán Gómez
Comisionado Ciudadano

Coordinación

Jorge Bustillos Roqueñí
Comisionado Ciudadano

Betsabé Hernández López Castellanos
Directora de Capacitación y Cultura de la Transparencia

Colaboradores

Rodrigo Santisteban Maza
Jorge Barrera Reyes
Berenice Islas Pérez
Víctor García Cruz
María Guadalupe Rodríguez Morales
Diana Hernández Patiño
Gabriela I. Montes Márquez
Alejandra Pacheco Pérez
Alejandra Sánchez Camacho

ÍNDICE

Presentación

Este libro comprende los textos básicos de apoyo para la capacitación en el conocimiento de las leyes de transparencia y acceso a la información y de protección de datos personales en el Distrito Federal, sus antecedentes, sus conceptos rectores, sus contenidos más destacados y sus alcances.

Desde el momento en que nace el derecho de acceso a la información pública en el Distrito Federal, en mayo de 2004, una prioridad y enorme reto para el órgano garante de transparencia, en ese entonces, el Consejo de Información Pública (CONSI), fue emprender una tarea intensa y permanente de capacitación en las materias de interés del Instituto para los servidores públicos.

Una prioridad estratégica que igualmente el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal ha hecho suya desde su nacimiento (INFODF-2006). Ello fue así, porque desde entonces se advertía que no bastaba con que hubiera una buena Ley y un órgano garante, para que el derecho pudiera ejercerse; se requería preparar y capacitar a los servidores públicos en las tareas y obligaciones que se desprendían de ese nuevo derecho. A la demanda previsible de información habría que anteponer a un servidor público capacitado y habilitado en el uso de la información y de las herramientas para darle la debida atención.

Las acciones de capacitación desde entonces han ido evolucionando y sus herramientas se han actualizado y modernizado al ritmo del continuo cambio normativo en la materia. Desplegando talleres y cursos tanto presenciales como virtuales, estos últimos accesibles a través de una aula virtual de aprendizaje, actividades de fomento para la autoformación a distancia, celebración de pláticas y conferencias, formación de instructores, así como, la especialización en la materia a través de un Diplomado, que hoy se ofrece en su modalidad virtual y presencial, contando siempre con el respaldo de la UNAM y de la UAM.

Las reformas legislativas a la norma original, nacida en 2003, el crecimiento de entes obligados en las leyes, el incremento y rotación de los servidores públicos así como el surgimiento de la Ley de Datos Personales, entre otros, han sido factores que han demandado de las acciones de capacitación, un esfuerzo extraordinario detonando nuevos materiales de apoyo para fomentar el conocimiento, tanto en cultura de transparencia como de protección de datos personales en el sector público y en los partidos políticos.

El presente libro refleja el esfuerzo, ahora especialmente encaminado a ofrecer elementos que les permita a los estudiosos del tema, en las dos modalidades (presencial y en línea) del Diplomado, identificar y comprender la evolución histórica,

los principales contenidos de las leyes de transparencia y acceso a la información pública y de protección de datos personales en posesión de entes gubernamentales y partidos políticos del Distrito Federal, que las caracterizan como normas vanguardistas en nuestro país. Reseña la evolución que ha nivel mundial han tenido estas normas, las modalidades y circunstancias bajo las cuales se fueron estableciendo en nuestro país, particularmente en la capital. Se abordan paso a paso los principales cambios que la norma va sufriendo, permitiendo distinguir los avances que se producen en cada una de ellas, para favorecer el establecimiento de las reglas que progresivamente han ampliado el espectro de acceso a información, así como las facilidades para el ejercicio de este derecho juntamente con la protección de los espacios de la vida privada.

El texto permite identificar los principios y conceptos rectores de ambos derechos, básicos para entender la dimensión de su alcance; revisa con detalle los procedimientos para el ejercicio y atención de cada una de las modalidades. Se aborda el estudio de los procedimientos de impugnación o de defensa de los mismos, que estas leyes ponen en manos de las personas, permitiendo a particulares y servidores públicos encargados de atenderlos, identificar los pasos a seguir para garantizar esos derechos. Se registra también la evolución e importancia que ha tenido la incorporación de herramientas tecnológicas para el ejercicio de ellos y para la evaluación de las prácticas en la materia.

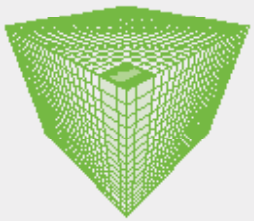
En materia de datos personales se da cuenta de un análisis detenido de los principios rectores de la materia, así como su interacción con los derechos de acceso, rectificación, cancelación y oposición, y del tratamiento de los datos obrantes en los sistemas de datos personales, y su protección de conformidad con los estándares fijados por la Ley.

Se trata en suma, de un libro que reúne un conjunto de elementos que buscan facilitar el conocimiento de la leyes, sus antecedentes y su aplicación; sin duda, es un texto que viene a complementar la serie de materiales de apoyo con los que hoy cuenta el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, para las actividades de capacitación de los servidores públicos, y que sin duda encontraran en las leyes comentadas un complemento ideal para profundizar en el detalle de su estudio. El estudio, análisis y discusión de los alcances y contenidos de las disposiciones normativas, así como, de los cambios que éstas han traído y que demandan, contribuirán siempre a la formación del nuevo servidor público que nuestros tiempos reclaman, el servidor público de la transparencia.

Jorge Bustillos Roqueñí
Comisionado Ciudadano del InfoDF

infodf

Transparencia y Datos Personales en el Distrito Federal



Capítulo I

Derecho de Acceso a la Información Pública

1. Introducción

Para adentrarnos en el conocimiento del tema de transparencia y acceso a la información en el Distrito Federal, abordaremos el estudio de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y sus implicaciones para los Entes Obligados en tres grandes apartados:

- El primer apartado aborda el proceso de institucionalización del derecho a la información pública en México, el cual tiene su origen en la suscripción de distintos instrumentos internacionales, que llevaron al legislador a reflexionar sobre la pertinencia de elevar al Derecho de Acceso a la Información a un rango Constitucional.

  De igual forma, presenta el proceso de regulación del Derecho de Acceso a la Información Pública gubernamental en México, cuya disparidad en su contenido propició la reforma al artículo 6º Constitucional, en el que se incorporan los principios rectores del Derecho de Acceso a la Información, que homogenizan el contenido de las leyes de las distintas entidades federativas.

  Finalmente se expone la evolución que ha tenido la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal hasta su última reforma, del 29 de agosto de 2011.

- El segundo apartado explica los conceptos básicos que se involucran en el Derecho de Acceso a la Información Pública gubernamental.

- El último apartado profundiza en el conocimiento del contenido de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, que en lo sucesivo la identificaremos también bajo las siglas LTAIPDF:

  - Aspectos generales de la Ley.

  - Obligaciones.

  - Principios rectores del acceso a la información.

  - Procedimiento de acceso a la información.

  - Órgano garante.

  - Medios de defensa.

  - Infracciones a la Ley.

Disposiciones con las que se busca garantizar, plenamente, el ejercicio del Derecho de Acceso a la Información de las personas.

2. Institucionalización del Derecho de Acceso a la Información Pública

2.1 Marco internacional[1]

En este primer apartado, se identificarán las bases que los instrumentos internacionales han dado lugar a la conformación del Derecho de Acceso a la Información y que han marcado las directrices para su reconocimiento en la Constitución Política de los Estados Unidos Mexicanos.

A nivel internacional, el acceso a la información ha sido reconocido como un derecho humano, inherente al hombre por el sólo hecho de serlo, mediante diversos instrumentos (pactos, convenios y los tratados internacionales), los cuales deben ser respetados por todos aquellos estados que los suscriben.

De esta manera, el derecho a la información, como derecho humano, incide el desarrollo económico, social, político y cultural del hombre, toda vez que la información es un instrumento indispensable para el ejercicio de otros derechos.

En 1789, en el marco de la Revolución Francesa, se emitió la Declaración de los Derechos del Hombre y del Ciudadano, en la cual se enumeran los derechos naturales e imprescriptibles que todo ser humano tiene por el sólo hecho de ser hombre (libertad, propiedad y seguridad); dentro de los que se encuentran las libertades de opinión, pensamiento, prensa y petición, previstas en su artículo 11, que a la letra dice[2]:

> ***Artículo 11.-*** La libre comunicación de los pensamientos y de las opiniones es uno de los derechos más preciados del hombre; todo ciudadano puede, por tanto, escribir e imprimir libremente, salvo la responsabilidad que el abuso de esta libertad produzca en los casos determinados por la ley.

Posteriormente, en la **Declaración Universal de Derechos Humanos** (Asamblea General de la ONU, 10 de diciembre de 1948, París) surge la idea fundamental de reconocer y exaltar la dignidad humana, reconociendo derechos personales, políticos, económicos, sociales y culturales, que sólo se ven limitados por el reconocimiento de las libertades y derechos de los demás individuos. Por lo

[1] SOTO GAMA, Daniel. Principios Generales del Derecho a la Información. Consultable en http://www.infoem.org.mx/informeActividades/9b_5.pdf.

[2] Declaración de los Derechos del Hombre y del Ciudadano. Consultable en http://www.juridicas.unam.mx/publica/librev/rev/derhum/cont/30/pr/pr23.pdf

que hace al derecho a la información, este instrumento internacional expresa lo siguiente:

> ***Artículo 19.-*** Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de **investigar y recibir informaciones y opiniones, y el de difundirlas,** sin limitación de fronteras, por cualquier medio de expresión. [3]

Por otra parte, en el Pacto Internacional de Derechos Civiles y Políticos (del 16 de diciembre de 1966), respecto al derecho a la información, se establece:[4]

> ***Artículo 19.- 1.*** Nadie podrá ser molestado a causa de sus opiniones. ***2.*** Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. ***3.*** El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: ***a)*** Asegurar el respeto a los derechos o a la reputación de los demás; ***b)*** La protección de la seguridad nacional, el orden público o la salud o la moral pública.

Este Artículo obedece a las directrices establecidas por la Declaración Universal de Derechos Humanos. En este instrumento no se hace referencia explícita al derecho a la información, sin embargo, se reconocen cada una de las libertades que lo comprenden, tal como ocurre en la Declaración Universal.

Este instrumento incorpora la imposición al Estado de fijar expresamente en sus leyes las restricciones a las que estaría sujeta cualquiera de las libertades a que hace referencia, asegurando el derecho de terceros, así como la protección de la seguridad nacional, el orden público, la salud y moral pública.

La **Convención Americana de Derechos Humanos o Pacto de San José de Costa Rica**[5] (San José, Costa Rica 7 al 22 de noviembre de 1969) tuvo como propósito reafirmar el compromiso adquirido en la firma de otros instrumentos de derechos humanos, como la Declaración Universal de Derechos Humanos, por lo que los derechos esenciales del hombre no nacen por el reconocimiento del Estado al que pertenece, sino que se fundamentan en los atributos de la persona, por tanto, son inherentes a ella; de tal manera, toda persona puede disfrutar del ejercicio de sus derechos en cualquier estado donde se encuentre.

[3] Declaración Universal de Derechos Humanos. Consultable en http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/046/82/IMG/NR004682.pdf?OpenElement y http://www.un.org/es/documents/udhr/

[4] Pacto Internacional de Derechos Civiles y Políticos. Consultable en http://www2.ohchr.org/spanish/law/ccpr.htm.

[5] Convención Americana de Derechos Humanos. Consultable en http://www.oas.org/juridico/spanish/tratados/b-32.html.

El instrumento en estudio, en su artículo 13, concede la libertad de pensamiento y la libertad de expresión en todos los Estados que hayan ratificado dicha convención:

> ***Artículo 13.- 1.*** Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. ***2.*** El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: ***a)*** el respeto a los derechos o a la reputación de los demás, o ***b)*** la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

La importancia de dicho instrumento radica en su alcance, ya que no sólo se circunscribe a los gobernados de los estados parte, sino que se extiende su reconocimiento y protección a los extranjeros que se encuentran dentro del territorio de los estados parte.

Este precepto representó la unificación de criterios en la interpretación de los derechos fundamentales, principalmente en lo que se refiere al derecho a la información, ya que también coincide en no distinguir entre libertad de expresión y derecho a la información.

De acuerdo con la protección que otorga la Convención, el derecho a la libertad de pensamiento y de expresión comprende "no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de buscar, recibir y difundir informaciones e ideas de toda índole".

Al igual que los instrumentos internacionales de derechos humanos citados con antelación, la Convención en estudio establece el derecho de buscar y recibir información, por lo que protege el derecho de toda persona a solicitar el acceso a la información bajo el control del Estado. Consecuentemente, ampara el derecho de las personas a recibir información, y obliga al Estado a proporcionarla, de forma tal que la persona pueda tener acceso a conocer la información o recibir una respuesta fundamentada cuando, por algún motivo, el Estado pueda limitar el acceso a ésta para un caso concreto. De esta forma, el derecho a la libertad de pensamiento y de expresión contempla la protección del Derecho de Acceso a la Información bajo el control del Estado.

Fue hasta el año 2006 cuando se reconoció por primera vez el Derecho de Acceso a la Información como un derecho humano. El 8 de julio de 2005, la Comisión Interamericana de Derechos Humanos presentó una demanda ante

la Corte Interamericana de Derechos Humanos, el **caso Claude Reyes y otros**, la cual tenía como fundamento la negativa de una institución del Estado de Chile a brindar a las víctimas toda la información que requerían sobre un proyecto de deforestación con impacto ambiental en Chile. En este caso la Comisión sostuvo que la negativa, así como la falta de un recurso judicial efectivo para impugnarla, generaban la responsabilidad internacional del Estado por la violación del derecho a la libertad de pensamiento y de expresión y del derecho a la protección judicial. Por lo anterior, en la sentencia del 19 de septiembre de 2006, la Corte Interamericana reconoció al Derecho de Acceso a la Información como un derecho humano integrante del derecho a la libertad de pensamiento y de expresión, lo que implica la necesidad de garantizarlo a través de una protección adecuada, para que, de forma rápida y expedita, se pueda obtener su protección; de igual forma, se reconoce el deber de todas las autoridades públicas de hacer accesible la información sobre los asuntos de interés público, sujeta a limitaciones.[6]

2.2 Regulación del Derecho de Acceso a la Información

Los instrumentos internacionales expuestos en líneas anteriores dejaron a cada Estado parte de la interpretación doctrinal, legislativa y jurisdiccional del Derecho de Acceso a la Información, lo que dio la pauta para que, en distintas latitudes del mundo, se emitieran diversas leyes tendientes a dar cumplimiento al mandato internacional.

El primer antecedente internacional del Derecho de Acceso a la Información lo encontramos en una Real Ordenanza sueca denominada His Majesty's Gracious Ordinance Relating to Freedom of Writing and of the Press[7] de 1766, promovida por Anders Chydenius, en la que se regulan la libertad de prensa y el derecho de acceso a la documentación pública.[8]

Los postulados principales del referido cuerpo normativo señalaban que:

- Toda la información gubernamental debe ser conservada y catalogada.
- Toda la información deberá ser accesible por medio de las universidades y otros sitios públicos.

La suscripción de los distintos instrumentos internacionales dio lugar a la primera oleada internacional de generación de normas en materia de acceso a la información, a partir de la década de los ochenta del siglo XX.

[6] Corte Interamericana de Derechos Humanos. Claude Reyes y otros Vs. Chile. Sentencia del 19 de septiembre de 2006. Consultable en www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.doc.

[7] Björkstrand & Mustonen. The World's First Freedom of Information Act. Consultable en http://www.access-info.org/documents/Access_Docs/Thinking/Get_Connected/worlds_first_foia.pdf

[8] Ackerman y Sandoval. Leyes de acceso a la información en el mundo. Consultable en http://www.ifai.org.mx/Publicaciones/publicaciones

1ª oleada internacional de leyes en materia de transparencia y acceso a la información pública	
Año de aprobación	**País**
1982	Australia, Nueva Zelanda.
1983	Canadá.
1987	Austria, Filipinas.
1990	Italia.
1991	Holanda.
1992	Hungría.
1993	Ucrania, España, Portugal.
1994	Belice, Bélgica.
1996	Islandia, Lituania, Corea del Sur.
1997	Tailandia, Irlanda
1998	Israel, Letonia.
1999	República Checa, Albania, Georgia, Grecia, Japón, Liechtenstein, Trinidad y Tobago, Sudáfrica.

A partir del año 2000 se gesta una segunda oleada internacional de emisión de leyes en materia de acceso a la información, en la cual se incorpora México con la emisión de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Un factor que aceleró la emisión de reglas claras para el acceso a la información pública fue la demanda mundial de organismos internacionales como la OCDE, BM, FMI, ONU y la OEA, que consideraban a la información como una herramienta para combatir la corrupción en la administración pública y para darle certeza y un mejor clima a las inversiones y al intercambio comercial.

2ª oleada internacional de leyes en materia de transparencia y acceso a la información pública	
Año de aprobación	**País**
2000	Inglaterra, Bosnia y Herzegovina, Bulgaria, Lituania, Moldavia, Eslovenia, Estonia.
2001	Polonia, Rumania
2002	Panamá, Pakistán, México, Jamaica, Perú, Tayikistán, Uzbekistán, Zimbabwe, Angola
2003	Croacia, India, Kosovo, Armenia, Eslovenia, Turquía
2004	República Dominicana, Serbia, Suiza, Ecuador
2005	Azerbaiján, Alemania, Montenegro, Uganda
2006	Macedonia

Actualmente, más de 100 países tienen leyes específicas en materia de transparencia y acceso a la información, y varias naciones de los cinco continentes del mundo contemplan su pronta incorporación al marco regulatorio de este derecho fundamental.

De esta manera, la doctrina moderna, con sustento en los instrumentos internacionales referidos, ha reconocido al Derecho de Acceso a la Información como un derecho fundamental, que se incorpora en la agenda democrática de distintos países, incluido México, al erigirse sobre él la viabilidad de un sistema democrático que cumple una función vital: que los ciudadanos conozcan el quehacer, las decisiones y los recursos que erogan sus autoridades.

2.3 Evolución del Derecho de Acceso a la Información en México

En México, el derecho a la información se planteó por primera vez en el Plan Básico de Gobierno 1976-1982, en el que se estableció que el derecho de referencia se constituiría en una nueva dimensión de la democracia y una fórmula de respeto al pluralismo ideológico.

A partir de lo anterior, en el año de 1977, en el marco de la denominada "reforma política", se modificó el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, incorporándose por vez primera el Derecho de Acceso a la Información, al adicionarse la siguiente frase "…el derecho a la información será garantizado por el Estado…".

Esta adición dio lugar a un amplio debate sobre su contenido y alcance, el cual con el paso del tiempo ha sido redefinido en la evolución jurisprudencial que sobre el tema ha emitido la Suprema Corte de Justicia de la Nación.

El 15 de abril de 1985, la Segunda Sala de la Suprema Corte de Justicia de la Nación definió al Derecho de Acceso a la Información como una garantía política conferida a los partidos políticos para acceder a la información en manos del Estado.

Fue hasta junio de 1996 que la Suprema Corte de Justicia de la Nación le dio un nuevo sentido al Derecho de Acceso a la Información, al resolver la solicitud hecha por el Presidente de la República para que se investigaran los hechos acontecidos en el caso de Aguas Blancas, Guerrero. El cambio de interpretación consistió en darle el carácter de garantía individual, necesaria para que la sociedad contara con la información que le permitiera sustentar un régimen democrático y, desde ahí, determinar que se trataba de que sus miembros tuvieran la certeza de que las autoridades proporcionaran información de sus actividades para mantener una sociedad informada y apta para la democracia.

En esta decisión, la Suprema Corte de Justicia de la Nación consideró que el derecho a la información constituía una garantía individual, y que, por ende, los hechos en cuestión constituían una violación a las garantías individuales; esta postura se derivó del ejercicio, por parte del Alto Tribunal, de la facultad establecida en el segundo párrafo del artículo 97 de la Constitución.

En los años de 1997, 1999 y 2000 se emitieron una serie de resoluciones en las que se consideró al Derecho de Acceso a la Información como una garantía individual limitada sólo por los intereses nacionales, los de la sociedad y por el respeto a los derechos de terceros.

Fue hasta el año 2002 cuando se inició el proceso normativo tendiente a regular el Derecho de Acceso a la Información gubernamental en México. La alternancia política en el gobierno federal (año 2000) y la disminución de la credibilidad en el gobierno fueron factores que favorecieron la emergencia de las leyes de acceso a la información a nivel nacional y estatal.

En este desarrollo, las ONG's especializadas en temas vinculados al derecho de expresión y de información, académicos y medios de comunicación agrupados fueron activo motor social que impulsó el surgimiento de la primera Ley de Transparencia y Acceso a la Información Pública Gubernamental en el país.

En este contexto, el denominado Grupo Oaxaca se convirtió en el principal gestor del proyecto de regulación del derecho fundamental a la información.

Este grupo fue integrado por periodistas y especialistas en el tema, quienes contribuyeron para colocar al Derecho de Acceso a la Información en la agenda pública del país, además de que impulsaron la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en el año 2002[9].

La emisión de dicha Ley dio la pauta para que, de 2002 a 2007, los treinta y un estados de la República y el Distrito Federal expidieran sus respectivas leyes adjetivas que garantizan el Derecho de Acceso a la Información Pública.

2002 (6)	2003 (8)	2004 (9)	2005 (6)	2006 (2)	2007(2)
Jalisco	Nuevo León	México	Sonora	Oaxaca	Tabasco
Sinaloa	Durango	Quintana Roo	Campeche	Chiapas	Hidalgo
Federal	Colima	Yucatán	Baja California		
Aguascalientes	San Luis Potosí	Veracruz	Baja California Sur		
Michoacán	Distrito Federal	Nayarit	Guerrero		
Queretaro	Guanajuato	Zacatecas	Chihuahua		
	Morelos	Tlaxcala			
	Coahuila	Puebla			
		Tamaulipas			

2.4 Una reforma constitucional

Para principios del año 2007, todos los estados del país contaban con una ley en materia de transparencia y acceso a la información. Sin embargo, existían variaciones significativas en los criterios contenidos en esas leyes para el ejercicio del Derecho de Acceso a la Información, lo que significó que los requisitos para ejercitar el derecho fueran distintos, dependiendo de la entidad federativa de que se tratara.

En algunos estados se requería, por ejemplo, que la persona que presentaba la solicitud fuera residente de ese estado; en otros estados, se imponían diversas limitaciones a las solicitudes, o bien existían diferencias importantes en la información que podía ser reservada. Aun y cuando se trataba del mismo derecho, el ejercicio de éste se sujetaba a condiciones diferentes.

Ante tal problemática, un grupo de gobernadores presentó al Congreso de la Unión un documento conocido como la "Iniciativa Chihuahua"[10], en la que

[9] Sobre este tema puede ver:
- ESCOBEDO DELGADO, Juan Francisco. Movilización de opinión pública en México: el caso del Grupo Oaxaca y de la Ley Federal de Acceso a la Información Pública. Consultable en Derecho Comparado de la Información http://www.juridicas.unam.mx/publica/librev/rev/decoin/cont/2/art/art3.pdf
- ESCOBEDO DELGADO, Juan Francisco. La invención de la Transparencia. Páginas 34-54. Consultable en http://www.resi.org.mx/icainew/images/Biblioteca/Publicaciones_ICAI/La%20Invencion%20de%20la%20Transparencia.pdf

[10] La iniciativa fue elaborada por los gobernadores de los Estados de Aguascalientes, Chihuahua, Veracruz, Zacatecas y el

se propuso adicionar al artículo 6° de la Constitución Política de los Estados Unidos Mexicanos un segundo párrafo, en el cual se incorporaron los criterios mínimos para ejercer el Derecho de Acceso a la Información, lo que impactó el diseño de las leyes de transparencia y acceso a la información pública del país.

De esta manera, en el dictamen de aprobación de la Cámara de Diputados, se reconoció que "… el desarrollo del derecho de acceso a la información no ha estado exento de problemas, resistencias y deformaciones. Quizás la dificultad más importante es la heterogeneidad con la que se ha legislado y con la que se ejerce hoy mismo en las entidades y en las instituciones de la República… La rutina democrática que posibilita pedir información a los gobiernos sin limitaciones, luego de 33 leyes de transparencia en la Federación y los estados, ha adquirido las más variadas tonalidades, pues los procedimientos y los arreglos institucionales, los límites, la apertura, la tecnología disponible y los documentos accesibles son muy distintos, por tanto la pregunta obligada es: ¿puede un derecho fundamental tener tantas versiones como gobiernos, jurisdicciones administrativas y soberanías? ¿Puede un derecho diferenciar a los mexicanos de modo tan subrayado, dependiendo de la entidad federativa, del lugar de residencia o del nacimiento de una persona?"[11].

La respuesta a dichos planteamientos, sin duda alguna, fue NO, por lo que ante la disparidad existente entre las distintas leyes de acceso a la información, se aprobó la incorporación de un párrafo segundo al artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, en el cual se establecen los principios que rigen al Derecho de Acceso a la Información Pública gubernamental en todo el país.

De esta manera, el 20 de julio de 2007 se publicó dicha reforma en el Diario Oficial de la Federación, la cual marca un antes y un después en el tema de transparencia y acceso a la información pública en México[12], al incorporar los aspectos mínimos que deben contener todas las leyes que en la materia se expidan a nivel nacional.

La reforma referida incorporó al artículo 6º Constitucional un párrafo segundo del que se desprende lo siguiente:

> Artículo 6o. La manifestación de las ideas no será objeto de ninguna

entonces Jefe de Gobierno del Distrito Federal.

[11] Véase Dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública con Proyecto de Decreto que reforma el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos en Gaceta Parlamentaria, Cámara de Diputados, número 2207–II, martes 6 de marzo de 2007. Publicado en http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum_crono.htm

[12] CARBONELL, Miguel. La Reforma Constitucional en Materia de Transparencia: RETOS Y PERSPECTIVAS. Consultable en http://www.ceaip-zac.org/datos/cultura/REVISTAS/carbonel.pdf .

> 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:

La **fracción I** del párrafo segundo establece:

> 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.

De la citada fracción se desprenden tres aspectos relevantes[13]:

- Establece el principio de publicidad de la información, que garantiza el acceso a la información en posesión de autoridades, entidades, órganos y organismos que integran los distintos niveles de gobierno; de manera que **toda la información gubernamental es considerada como un bien público,** rompiendo con la discrecionalidad en el manejo de la información con la que contaban los funcionarios públicos. Este principio supone un nuevo valor que debe formar parte de la función pública por lo que hace a la publicidad de sus actos.

- **La reserva temporal** de la información como excepción a la publicidad de ésta, la cual debe estar determinada por disposición de ley. Por ello, la reserva de información debe demostrarse y sustentarse con argumentos objetivos, de manera clara y contundente, que acrediten que la divulgación de cierta información genera una alta probabilidad de dañar un interés público protegido.

- Establece el principio de **máxima publicidad,** el cual orienta la forma de interpretar y aplicar la norma, para que en caso de duda razonable entre la publicidad o reserva de la información, se opte por la publicidad de ésta.

En la **fracción II** se establece:

> 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.

[13] LÓPEZ-Ayllón, Sergio. El acceso a la información como un derecho fundamental: la reforma al artículo 6º de la Constitución mexicana. Consultable en http://www.ifai.org.mx/Publicaciones/publicaciones.

En dicha fracción se incorpora una segunda limitación al Derecho de Acceso a la Información, que se refiere a la **protección de la vida privada y de los datos personales,** aspectos que no están sujetos al principio de publicidad, al poner riesgo otro derecho fundamental, que es el de la intimidad y la vida privada, por lo que los términos de la protección y las excepciones a este derecho se determinaran por mandato de ley, siendo posible considerar que cierta información privada o datos personales que adquieran un valor público podrán ser divulgados a través de los mecanismos que al efecto determine la ley; un ejemplo son los datos contenidos en los registros públicos de la propiedad o los salarios de los funcionarios públicos.

La **fracción III** prevé lo siguiente:

> 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.

Conforme a esta fracción, el ejercicio del **Derecho de Acceso a la Información no puede estar condicionado a requerir al interesado identificación alguna, ni acreditación de un interés o justificación de la utilización de la información,** por lo que no se puede establecer condiciones que permitan a la autoridad, de manera discrecional, juzgar sobre la legitimidad del solicitante o del uso de la información.

En el caso de datos personales, únicamente se requerirá acreditar la identidad de su titular para su acceso y la procedencia de su rectificación, en su caso.

También establece el **principio de gratuidad,** tanto en el ejercicio del Derecho de Acceso a la Información como en el de acceso o rectificación de los datos personales. Dicho principio se refiere a la gratuidad de los procedimientos de acceso cuyo costo debe ser cubierto por los órganos del Estado, y, eventualmente, el único cobro admisible es el de recuperación de los materiales de reproducción de la información (fotocopias, respaldos, discos compactos, gastos de envío, etc.).

En la **fracción IV** se prevé lo siguiente:

> 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.

Aquí se establecen las bases operativas que deberán incorporar las leyes para el ejercicio del Derecho de Acceso a la Información. El primer aspecto es el

desarrollo de **procedimientos de acceso** que permitan a cualquier persona realizar y obtener de manera expedita el acceso a la información, a sus datos personales o a la rectificación de éstos. Ante la eventual negativa de acceso o la entrega de información incompleta, las leyes deberán desarrollar un mecanismo de impugnación expedito, del cual tendrá conocimiento un órgano u **organismo especializado** e imparcial. Con lo anterior se garantiza el ejercicio del derecho de acceso a la información.

El órgano u organismo especializado que conoce de los **medios de impugnación** deben gozar de:

- Especialización, para garantizar que los juzgadores tendrán el conocimiento necesario para valorar adecuadamente los casos que se presenten.

- Imparcialidad, con lo que se busca asegurar que, tanto en la integración como en la operación, los órganos u organismos no responderán a consignas directas o indirectas de los órganos de autoridad y que actuarán de manera profesional y objetiva.

- Autonomía:

  Operativa, que consiste en la administración responsable con criterios propios.

  De gestión presupuestaria, que se refiere a la aprobación de sus proyectos de presupuesto, el cual deberá ejercerse con base en los principios de eficacia, eficiencia y transparencia, sujetándose a la normatividad, la evaluación y el control de los órganos correspondientes; autorizar adecuaciones y determinar los ajustes que correspondan en su presupuesto, en caso de disminución de ingresos, atendiendo a sus competencias conforme a la Ley.

  De decisión, que supone una actuación basada en la ley y en la capacidad de un juicio independiente debidamente fundado y motivado.

La **fracción V** dispone:

> 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.

Esta fracción establece, de manera específica, la obligación de los órganos e instituciones del estado de contar con **archivos** administrativos, que

documenten sus actividades, faciliten una mejor gestión y aseguren una adecuada rendición de cuentas y la localización fácil y expedita de los documentos que se soliciten.

Además, incorpora la obligación de generar y publicar en medios electrónicos sus **indicadores de gestión,** así como informar sobre el uso y destino de los recursos públicos otorgados a cada uno de los sujetos obligados.

Por otra parte, en la **fracción VI,** se establece:

> 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.

Conforme a esta fracción, el legislador emitirá las leyes adjetivas que 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, estas últimas con independencia de su naturaleza pública o privada, los partidos políticos y otras instituciones de interés público, así como organizaciones no gubernamentales, sociedades, asociaciones y fundaciones, entre otros, lo cual debe ser objeto de transparencia.

Si bien dichas personas no se consideran sujetos obligados, la entrega de recursos públicos las sujeta a presentar informes y documentación probatoria del uso y destino de los recursos del erario que les son entregados, es decir, les sujeta a la rendición de cuentas.

Finalmente, en la **fracción VII** se prevé:

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

Esta fracción incorpora la imposición de **sanciones** ante la inobservancia a las disposiciones contenidas en las leyes de acceso a la información; por lo tanto, las legislaciones federales y estatales deben regular y definir las conductas de los servidores públicos que ameriten sanción, así como las autoridades a cargo de su aplicación.

Por otra parte, el constituyente, en los artículos Segundo y Tercero transitorios, estableció aspectos esenciales para el correcto ejercicio del Derecho de Acceso a la Información, al señalar, en el primero de ellos, el plazo de un año para que se reformaran las leyes en materia de transparencia y acceso a la información pública conforme al nuevo marco constitucional. En tanto que el artículo

Tercero incorporó la obligación de los distintos sujetos obligados para que cuenten con sistemas electrónicos que faciliten el acceso a la información, los cuales se debían implementar dos años después de la entrada en vigor de la reforma.

2.5 El caso del Distrito Federal

En el Distrito Federal, el camino recorrido en el tema de la transparencia y el acceso a la información no ha estado libre de obstáculos, dificultades y resistencias.

El proceso de institucionalización del derecho a la información tiene su primer antecedente el 7 de diciembre de 2001, momento en que el diputado José Luis Buendía Hegewisch, del Partido Democracia Social, presentó en la Asamblea Legislativa una iniciativa de la Ley de Transparencia y Acceso a la Información Pública para el Distrito Federal, en la cual se garantizaba el Derecho de Acceso a la Información, tanto de particulares como de las autoridades. En dicha iniciativa se incorporaron los siguientes aspectos:

- La creación de un órgano garante denominado Consejo de Información del Distrito Federal, integrado por 3 consejeros ciudadanos, el Secretario de Gobierno del Distrito Federal, el Presidente de la Comisión de Gobierno de la Asamblea Legislativa del Distrito Federal, el Presidente del Tribunal Superior de Justicia del Distrito Federal, el Presidente de la Comisión de Derechos Humanos del Distrito Federal y 3 representantes de los medios de comunicación.

- Preveía a la información reservada como excepción al acceso a la información, sin ser muy específica.

- Establecía un plazo de respuesta a las solicitudes de información pública de 10 a 15 días hábiles, sin ser puntual en cada caso.

- Reconocía distintos medios de impugnación (ante el Consejo de Información del Distrito Federal y ante los órganos de control interno).

Fue hasta el 18 de marzo de 2003 cuando se aprobó por mayoría de las dos terceras partes de los integrantes presentes de la Asamblea Legislativa del Distrito Federal la primera Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, que fue publicada en la Gaceta Oficial del Distrito Federal el 8 de mayo del mismo año, y con la cual se mantenían algunos de los puntos de la iniciativa de ley señalada con antelación, de tal manera que se limitaba el ejercicio del Derecho de Acceso a la Información al establecer:

- Las solicitudes de acceso a la información debían ser presentadas físicamente ante el Ente Público.
- La necesidad de acreditar la identidad para ejercitar el Derecho.
- La creación como órgano garante al Consejo de Información Pública del Distrito Federal, que por su compleja estructura dificultaba la defensa oportuna del derecho[14].
- Los entes podían emitir acuerdos clasificatorios generales de aquella información que consideraran reservada o confidencial, lo que dio lugar a la clasificación indiscriminada de información de naturaleza pública[15].

El 16 de diciembre de 2003 se publicó la primera reforma a la LTAIPDF en la Gaceta Oficial del Distrito Federal, en la que se derogan, adicionan y reforman diversos contenidos de la LTAIPDF, que, sin duda, seguía siendo sumamente deficiente.

Ante la constante práctica de clasificar la información por parte de los entes, el Jefe de Gobierno del Distrito Federal emitió un acuerdo en el que se estableció como pública toda la información que detentaba la administración pública del Distrito Federal, de conformidad con lo dispuesto en los artículos 23 y 24 de la LTAIPDF; de igual forma, abrogó todos los Acuerdos emitidos por los Entes Públicos que clasificaban la información[16]. Dicho acuerdo fue publicado en la Gaceta Oficial del Distrito Federal el 18 de marzo de 2005.

El 28 de octubre de 2005 se publicó, en la Gaceta Oficial del Distrito Federal, el decreto por el que se reformaron, derogaron y adicionaron diversas disposiciones de la Ley, que, en su conjunto, constituyeron una renovación en materia de garantías, procedimientos y funciones, al introducir modificaciones y adiciones sustantivas, que empezaron a colocar a esta Ley a la vanguardia de los instrumentos jurídicos en la materia a nivel nacional.

En esta Ley se superaron los obstáculos señalados en la Ley anterior, al incorporarse los siguientes aspectos:

- Reducción del plazo máximo de reserva de 20 a 12 años.

[14] El Consejo de Información Pública del Distrito Federal se integraba con 3 representantes de la Administración Pública del Distrito Federal designados por el Jefe de Gobierno, 4 diputados designados por la Asamblea Legislativa del Distrito Federal, 3 integrantes del Tribunal Superior de Justicia del Distrito Federal, 3 representantes de la sociedad civil y un representante de cada uno de los 5 órganos autónomos del Distrito Federal.

[15] Un claro ejemplo de la falta de transparencia en el Distrito Federal fue la clasificación por parte del FIMEVIC de la información de la construcción del 2º piso del Periférico. Véase 5. Claroscuros de la TRANSPARENCIA en el D.F. Horizontes en el escrutinio de la gestión pública. Consultable en http://www.infodf.org.mx/web/index.php?option=com_wrapper&Itemid=329.

[16] Consultable en http://www.consejeria.df.gob.mx//uploads/gacetas/marzo05_18_33bis.pdf.

- Inclusión de la obligación de generar versiones públicas.
- Creación del Instituto de Acceso a la Información Pública del Distrito Federal (INFODF), el cual se conformó por cinco comisionados ciudadanos, que aún conservaba la presencia de consejeros institucionales, con derecho a voz y no a voto.
- Inclusión, dentro del marco interpretativo de la Ley, de los instrumentos internacionales suscritos por México, con lo que se garantizó el cumplimiento de estándares internacionales en la materia.
- Establecimiento de la presentación de solicitudes de información a través de medios electrónicos.
- Eliminación del requisito de presentar una identificación oficial para la procedencia y tramitación de las solicitudes de información.
- Eliminación de la atribución de los entes para emitir acuerdos clasificatorios.
- Obligación, para los sujetos obligados, de entregar gratuitamente la información en caso de no responder al solicitante dentro del plazo legal establecido para ello.
- El órgano garante quedo como único para la interposición de recursos.
- Inclusión de la prueba de daño.

Es así como el Distrito Federal, después de poner a prueba su legislación, pasó de contar con una de las peores leyes de transparencia y acceso a la información, a una de las mejores leyes en el país, al colocarse en el segundo lugar del ranking nacional.

A esta última reforma le siguieron las siguientes modificaciones, publicadas en la Gaceta Oficial del Distrito Federal:

- El 23 de diciembre de 2005 se indicó que la designación de Comisionados Ciudadanos debía realizarse a más tardar el 31 de enero de 2006.
- El 31 de enero de 2006 se emitió una reforma en la que se amplió el periodo de designación de Comisionados hasta el 31 de marzo de 2006.

El 31 de marzo del 2006, entró en funciones el Instituto de Acceso a la Información Pública del Distrito Federal, lo que agilizó los mecanismos de defensa del Derecho de Acceso a la Información.

La siguiente reforma se publicó en la Gaceta Oficial del Distrito Federal el 29 de mayo de 2006; en ella se ciudadanizó plenamente el Órgano Garante, al excluir la participación de los consejeros institucionales en sus sesiones institucionales.

De igual forma, el 5 de enero de 2007 se publicó una nueva reforma a la LTAIPDF, con la cual se perfeccionó su contenido, que la siguieron posicionando como una de las mejores leyes en la materia.

Como consecuencia de la reforma al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, publicada el 20 de julio de 2007, el INFODF presentó a los legisladores una propuesta de reforma que pretendía armonizar la LTAIPDF con los ejes rectores del 6º Constitucional, atendiendo el modelo de ley que habían integrado investigadores de la UNAM y del CIDE, de manera conjunta con los órganos garantes del país, en un documento denominado Código de Buenas Prácticas y Alternativas para el Diseño de Leyes de Transparencia y Acceso a la Información Pública en México[17].

Dicha propuesta fue retomada por los legisladores para su estudio y elaboración de una nueva Ley, la cual fue publicada en la Gaceta Oficial del Distrito Federal el 28 de marzo del 2008.

En ese mismo año se emitieron leyes especializadas en materia de datos personales y archivo, como elementos sustantivos que fortalecen el marco normativo en materia de transparencia y acceso a la información.

De esta forma, el Distrito Federal no sólo atendió el ordenamiento constitucional de actualizar su norma especial e incorporar las mejores prácticas en su construcción normativa, sino que, además, dotó de dos leyes especiales que le permiten contar con el mejor marco normativo para dar acceso a la información gubernamental, proteger los datos personales en manos del sector gubernamental y de los partidos políticos y ordenar y administrar sus archivos.

La nueva Ley de Transparencia y Acceso a la Información Pública del Distrito Federal incorporó los siguientes aspectos:

- Los partidos políticos se consideran como sujetos obligados directos al cumplimiento de la LTAIPDF.

[17] Esta propuesta, producto de un ejercicio de consulta y consenso, expone, en un formato propio de un instrumento legislativo, las mejores prácticas en materia de acceso a la información y protección de datos personales, así como alternativas concretas para el diseño de las leyes de acceso a la información pública en México, todo ello de manera congruente con los principios y bases que contiene el texto reformado del artículo 6° constitucional. El Código desarrolla, así, una serie de prácticas que pretenden servir como un marco de referencia para el diseño de las legislaciones en materia de transparencia y acceso a la información pública. Consultable en http://www.ifai.org.mx/Publicaciones/publicaciones

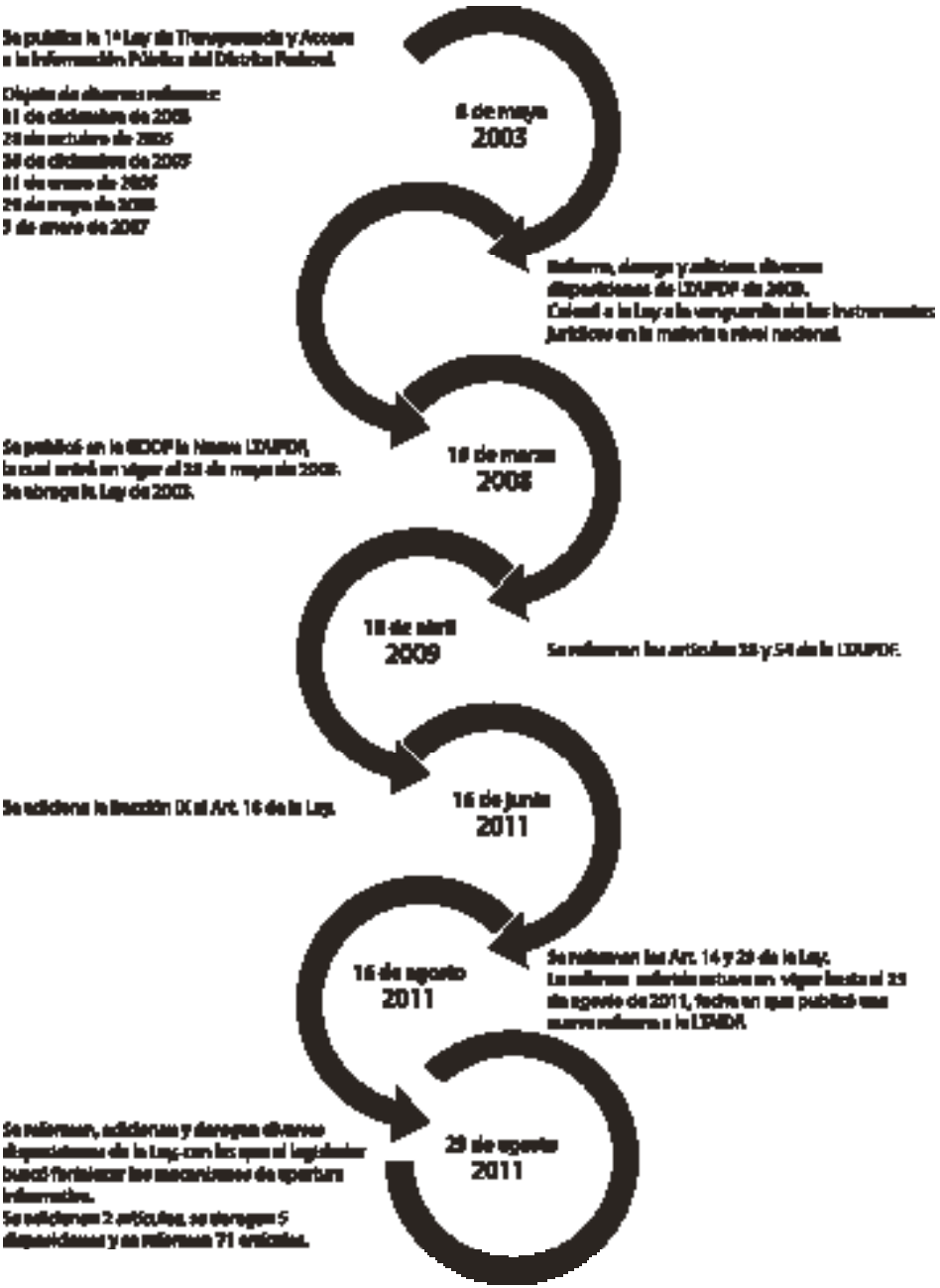
- La actualización trimestral de la información considerada como pública de oficio.
- Toda persona moral (organizaciones de la sociedad civil, sindicatos o cualquier otra análoga) que recibe recursos públicos por cualquier concepto, con excepción de las cuotas sindicales, debe proporcionar a los entes públicos que les otorgó los recursos, la información relativa al uso, destino y actividades que realiza con ellos.
- El principio de máxima publicidad.
- La obligación para los entes de publicar sus indicadores de gestión.
- El plazo de cinco días para la entrega de información pública de oficio.
- La reducción del plazo de 45 a 40 días para resolver recursos.
- El establecimiento de tres procedimientos de atención de recursos de revisión.
- La incorporación de la figura de la Denuncia por incumplimiento a la publicación de información considerada como pública de oficio.

Dicha Ley ha sido objeto de diversas reformas y adiciones:

- La primera de ellas fue publicada en la Gaceta Oficial del Distrito Federal el 13 de abril del 2009, en la que se reformó el tercer párrafo del artículo 36 y el primer párrafo de su artículo 54, para armonizar la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal con la Ley que regula el uso de la tecnología para la seguridad pública, por lo que hace a la restricción al acceso a la información.
- La segunda reforma fue publicada en la Gaceta Oficial del Distrito Federal el 16 de junio del 2011, en ésta se adicionó la fracción IX al artículo 18, referente a las obligaciones de transparencia específicas conferidas a los Órganos Político Administrativos, dentro de las cuales se incorporó la obligación de publicar los montos que ejercen estos Órganos, el nombre y ubicación de los mercados de cada demarcación y el padrón de locatarios.
- Una reforma que no se debe de descartar, es la publicada el 16 de agosto de 2011 en la Gaceta Oficial del Distrito Federal, en la que se reformaron los artículos 14, primer párrafo, y 28 de la Ley, en la cual se preveía la obligación de los Entes Obligados de habilitar redes sociales de internet. Sin embargo, su vigencia fue efímera, pues en la reforma del 29 de agosto

de 2011 se modificó el contenido de ambos artículos. Sobre esta reforma se debe señalar que incidió en la Ley de Firma Electrónica y en la Ley Orgánica de la Administración Pública, ambas del Distrito Federal, en donde quedó firme la habilitación de los entes para hacer uso de redes sociales para información sobre trámites y servicios y también se habilitó al gobierno para el desarrollo de su portal interactivo.

La última reforma fue publicada en la Gaceta Oficial del Distrito Federal el 29 de agosto del 2011; ésta es la tercera reforma significativa de la LTAIPDF, la cual adiciona dos artículos, se derogan cinco disposiciones y se reforman 71 artículos, elementos que revisaremos en nuestro siguiente apartado.


Se publica la 1ª Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.
Objeto de diversas reformas:
31 de diciembre de 2003
28 de octubre de 2005
30 de diciembre de 2005
31 de enero de 2006
29 de mayo de 2006
5 de enero de 2007
6 de mayo 2003
Reforma, adiciona y adiciona diversas disposiciones de LTAIPDF de 2003. Creación de la Ley y la vanguardia de los instrumentos jurídicos en la materia a nivel nacional.
Se publicó en la GODF la Nueva LTAIPDF, la cual entró en vigor el 28 de mayo de 2008. Se abroga la Ley de 2003.
18 de marzo 2008
18 de abril 2009
Se reformaron los artículos 38 y 54 de la LTAIPDF.
Se adiciona la fracción IX al Art. 16 de la Ley.
16 de junio 2011
16 de agosto 2011
Se reformaron los Art. 14 y 29 de la Ley. La reforma señalada estuvo en vigor hasta el 25 de agosto de 2011, fecha en que publicó una nueva reforma a la LTAIPDF.
Se reformaron, adicionan y derogan diversas disposiciones de la Ley con los que el legislador buscó fortalecer los mecanismos de apertura informativa.
Se adicionan 2 artículos, se derogan 5 disposiciones y se reformaron 71 artículos.
29 de agosto 2011

Resumen

El acceso a la información pública es un elemento fundamental que incide en la construcción democrática de nuestro país, al establecer los mecanismos que permiten mejores condiciones para la participación de las personas y dotarla de información que incide en la toma de decisiones.

Es importante resaltar que no basta con que haya un reconocimiento explícito del derecho a la información, pues estas premisas deben traducirse en obligaciones de la autoridad y en procedimientos que garanticen el derecho de las personas para acceder a la información.

La transparencia exige, para su adecuada materialización, un marco jurídico que garantice el derecho y que regule elementos mínimos.

La formulación y publicación de las leyes de transparencia en nuestro país evidenció un proceso heterogéneo y paulatino en la emisión de legislaciones en la materia. Con la reforma del artículo 6º Constitucional, se homogeneizó el contenido de las leyes de acceso a la información, tanto a nivel federal como de los estados de la República, por lo que todas las leyes de la materia fueron reformadas para incorporar en ellas los ejes rectores que hoy en día reconoce la Constitución Política de los Estados Unidos Mexicanos.

La evolución progresiva de la Ley en el Distrito Federal ha perfeccionado, en cada reforma, los mecanismos para que la gente pueda ejercer su derecho a la información y mejorar sus medios de defensa y garantías, lo que ha posicionado a esta Entidad como la mejor armada normativamente para atender este derecho fundamental.

La transparencia en el gobierno debe construirse cuidadosamente, con una visión de largo plazo que asuma, al mismo tiempo, objetivos legales, reglamentarios, políticos, organizacionales, educativos, culturales dentro y fuera de las instituciones de gobierno, y ello queda reflejado en la evolución normativa que se ha venido gestando.

3. Marco Conceptual

En este apartado se presentan los conceptos y definiciones que se encuentran estrechamente vinculados con los temas de transparencia y acceso a la información pública.

3.1 Rendición de Cuentas

La rendición de cuentas es entendida como la obligación de todos los servidores públicos y partidos políticos de informar sobre sus acciones y justificarlas en público: "qué hice y por qué lo hice"; incluida la posibilidad de que sean sancionados; es decir, "… la rendición de cuentas involucra por tanto el derecho a recibir información y la obligación correspondiente de divulgar todos los datos necesarios. También implica, el derecho a recibir una explicación y el deber correspondiente de justificar el ejercicio del poder…"[18].

Para algunos estudiosos del tema, la rendición de cuentas involucra dos tipos de relación:

- La rendición de cuentas horizontal, que se refiere a las relaciones de control entre los órganos del Estado, es decir, se gesta en una relación igualitaria.
- La rendición de cuentas vertical, que se refiere a la relación de control de la sociedad hacia el Estado, la cual se basa en la capacidad de los ciudadanos para vigilar, interpelar y sancionar a servidores públicos.

3.2 Transparencia

Es la práctica permanente de colocar la información en la vitrina pública, para que cualquiera pueda revisarla, analizarla y, en su caso, utilizarla como fundamento de sanción; lo que implica, para las organizaciones públicas, un cambio cultural.

3.3 Información Pública

Es todo archivo, registro o dato contenido en cualquier medio o documento que se encuentre en poder de los distintos órganos de gobierno, o que, en ejercicio de sus atribuciones, tengan la obligación de generar o administrar y que no encuadre en los supuestos de información de acceso restringido.

3.4 Derecho de Acceso a la Información Pública

Es la prerrogativa de toda persona para acceder a la información generada, administrada o en poder de los distintos órganos de gobierno, la cual no podrá ser negada, salvo las excepciones previstas por la Ley.

[18] SCHEDLER, Andreas. ¿Qué es la rendición de cuentas? Cuadernos de Transparencia 03. Consultable en http://www.ifai.org.mx/publicaciones/cuadernillo3.pdf

4. Ley de Transparencia y Acceso a la Información Pública del Distrito Federal

En este apartado se abordara el contenido de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, conforme al texto de la última reforma publicada en la Gaceta Oficial del Distrito Federal el 29 de agosto del 2011.

El contenido de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (LTAIPDF) se distribuye en cuatro títulos, diez Capítulos y 99 artículos.

4.1 Disposiciones de carácter general

La LTAIPDF tiene por objeto transparentar el ejercicio de la función pública, garantizar el efectivo acceso de toda persona a la información pública en posesión de los órganos Ejecutivo, Legislativo, Judicial y autónomos, así como de cualquier entidad, organismo u organización que reciba recursos públicos del Distrito Federal; por lo tanto, en ella se establecen mecanismos de acceso a la información que favorecen la rendición de cuentas y la transparencia.

En este instrumento normativo se incorporan los principios rectores del segundo párrafo del artículo 6° Constitución Política de los Estados Unidos Mexicanos, al establecer:

- Que la información generada, administrada o en posesión de los Entes Obligados del Distrito Federal es un bien de dominio público accesible a cualquier persona (artículo 3), por lo que debe estar a disposición, con excepción de aquella que tenga el carácter de acceso restringido.
- Que el acceso a la información no se encuentra sujeto a la acreditación de derechos subjetivos, interés jurídico o razones que justifiquen el requerimiento (artículo 8).
- Los Entes Obligados a dar cumplimiento a la LTAIPDF de manera directa e indirecta (artículo 4 y 30).
- Las causales de reserva temporal de la información (artículo 37).
- El principio de máxima publicidad como principio rector del acceso a la información y de los procedimientos (artículos 2, 4 fracción XII, y 45).
- La protección de los datos personales y de la vida privada, por lo que

todo lo relacionado con dichos temas se estará a lo previsto en la Ley de Protección de Datos Personales para el Distrito Federal (artículo 8 y 38).

- El principio de gratuidad de la información (artículos 9, 45 y 48).
- Mecanismos de acceso que permiten a cualquier persona obtener información pública de los Entes Obligados (artículos 45 a 57).
- Los medios de impugnación (artículos 32, 71, 76 a 92).
- Al Instituto de Acceso a la Información y Protección de Datos Personales del Distrito Federal como órgano garante del Derecho de Acceso a la Información (artículo 63).
- Que todos los entes deberán proporcionar a través de medios electrónicos sus principales indicadores de gestión, así como información sobre sus actividades. (artículos 13 a 32).
- Un capítulo de responsabilidades por inobservancia de la LTAIPDF (artículo 93 y 94).

En la vigente Ley se positiviza el **Derecho a la Información como un derecho fundamental,** el cual se encuentra reconocido en el artículo 6º Constitucional, al establecer mecanismos de protección que garantizan plenamente dicho derecho.

También prevé que el derecho a la información comprende las facultades de difundir, investigar y recabar (o recibir) información pública, las cuales consisten en:

- **Investigar,** implica la posibilidad de que cualquier persona pueda acceder y conocer la información que generan los distintos Entes Obligados.
- **Difundir,** es la potestad que toda persona tiene de dar a conocer la información de la cual se allega a través del ejercicio de su derecho a la información, así como su opinión sobre ella.
- **Recabar** (o recibir) información, implica la posibilidad de todo individuo de obtener libremente información, sin restricciones o negativas injustificadas, de acuerdo con sus necesidades e intereses personales, lo cual le garantiza la obtención de un bien jurídico: información.

Un elemento relevante de las reformas a la LTAIPDF es lo previsto en su artículo 5, que establece que son responsabilidades de los Entes Obligados: facilitar la

participación de las personas en la vida política, económica, social y cultural del Distrito Federal; para lo cual deberán difundir entre los habitantes de dicha entidad, el contenido de la LTAIPDF, además de contribuir al fortalecimiento de espacios de participación social, que fomenten la interacción entre la sociedad y los propios entes en temas de transparencia, acceso a la información pública y rendición de cuentas.

Así mismo, el artículo 12 de la LTAIPDF establece las obligaciones que, de manera general, deben cumplir los sujetos obligados, entre las cuales se encuentran las siguientes:

- **Garantizar** que la información que se publica en los portales de internet de los entes sea fácilmente identificable, accesible y cumpla con los requerimientos de organización establecidos en los Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer los Entes Obligados en sus portales de Internet, aprobados el 16 de noviembre de 2011.

- **Asegurar la protección de los datos personales** en términos de la Ley de Protección de Datos Personales para el Distrito Federal y demás normatividad aplicable.

- **Capacitar y actualizar de manera permanente a sus servidores públicos,** en coordinación con el INFODF, sobre los temas de cultura de accesibilidad y apertura informativa a través de cursos, talleres, seminarios, y cualquier otra forma de enseñanza que consideren pertinente (artículo 33). Es importante destacar que, en la práctica, no basta con el conocimiento del marco normativo que rige la materia, toda vez que es necesario el cambio de actitud de los servidores públicos, para adoptar la transparencia y el acceso a la información como un valor y no simplemente como una obligación.

- **Promover y fomentar una cultura de la información** a través de medios impresos, procurando el uso de documentos y expedientes electrónicos, que facilitan el acceso a la información pública.

- **Crear y hacer uso de sistemas de tecnología avanzados** y adoptar las nuevas tecnologías de la información, para que las personas consulten información de manera directa, sencilla y rápida.

- Una de las más importantes es **documentar todos los actos** que deriven del ejercicio de las atribuciones que le son conferidas, a fin de garantizar plenamente el acceso a la información.

Es importante destacar que la LTAIPDF no sólo garantiza el acceso a la información pública contenida en documentos, sino que también permite conocer información relacionada con el funcionamiento y actividades que desarrollan los distintos Entes Obligados, con excepción de aquella que sea de acceso restringido (artículo 26).

4.2 Entes Obligados

En el artículo 4, fracción V, la LTAIPDF reconoce como Entes Obligados directos a su cumplimiento a:

- Órgano Ejecutivo: Jefatura de Gobierno del Distrito Federal, dependencias, órganos desconcentrados, órganos político administrativos (16 delegaciones políticas), entidades de la administración pública.
- Órgano Legislativo: Asamblea Legislativa del Distrito Federal y la Contaduría Mayor de Hacienda de la Asamblea Legislativa del Distrito Federal.
- Órgano Judicial: Tribunal Superior de Justicia del Distrito Federal y el Consejo de la Judicatura del Distrito Federal.
- Órganos Electorales: Tribunal Electoral del Distrito Federal y el Instituto Electoral del Distrito Federal.
- Órganos Autónomos: Instituto de Acceso a la Información y Protección de Datos Personales del Distrito Federal, Universidad Autónoma de la Ciudad de México, Comisión de Derechos Humanos del Distrito Federal, Tribunal de lo Contencioso Administrativo del Distrito Federal y la Junta de Conciliación y Arbitraje del Distrito Federal.
- Otros: Fideicomisos y fondos públicos; partidos políticos, y los que la legislación local reconozca como de interés público.

Por lo que hace a los partidos políticos, éstos se reconocen como sujetos obligados directos en materia de transparencia y acceso a la información en los términos de la LTAIPDF y el Código de Instituciones y Procedimientos Electorales del Distrito Federal; por lo que la información que administren, resguarden o generen en el ejercicio de sus funciones se sujeta al principio de máxima publicidad. Ante incumplimientos a las obligaciones que les son conferidas en materia de transparencia y acceso a la información, el INFODF –como órgano garante- dará vista al Instituto Electoral del Distrito Federal para que determine las acciones que resulten procedentes (artículos 4, 19 BIS y 31).

De igual forma, reconoce como Entes Obligados indirectos a las personas morales, organizaciones de la sociedad civil, a los sindicatos o cualquier otra que reciban recursos públicos por cualquier concepto, quienes deberán proporcionar a los Entes Obligados de los que los reciban, la información relativa al uso, destino y actividades que realicen con tales recursos (artículo 30). Por lo que hace a este punto, se abre una área de oportunidad para los Entes Obligados (directos e indirectos) de dar a conocer los documentos probatorios que sustenten el ejercicio de los recursos.

4.3 Principios rectores del acceso a la información

La LTAIPDF establece que los Entes Obligados, en su relación con los solicitantes de información, se deben regir por los siguientes principios (artículo 2):

- **Principio de legalidad:** Los actos de los Entes Obligados deben estar debidamente fundados y motivados, por lo que su actuar debe apegarse a lo dispuesto en la normativa vigente; por tanto, sólo pueden hacer aquello que le sea expresamente facultado.

- **Principio de información:** Toda la información en posesión de los Entes Obligados es pública y toda persona puede acceder a ésta, con excepción de aquella que tenga el carácter de acceso restringido. Esto implica el deber de los entes de producir (generar) y administrar adecuadamente la información (incluso sistematizarla), de manera tal que permita documentar la actuación pública y mejorar la calidad de los registros y archivos públicos.

- **Principio de imparcialidad:** Toda persona está en posibilidad de someterse a las normas que rigen el procedimiento de acceso a la información pública en igualdad de condiciones. Las autoridades deben actuar sin ninguna clase de discriminación entre las personas, otorgándoles tratamiento y tutela igualitarios frente al procedimiento, resolviendo de manera objetiva y conforme a la normatividad.

- **Principio de celeridad:** Los procedimientos de acceso a la información pública deben ser sencillos y expeditos, lo que implica que no se regulen formalidades innecesarias y que la atención de los procedimientos debe ser breve, cumpliendo con las formalidades y garantías que debe seguir todo proceso.

- **Principio de certeza jurídica:** Las acciones que efectúen los Entes Obligados, deben ser completamente verificables, fidedignas y confiables. Esto es, que una vez que se ha resuelto sobre una situación, habiéndose

considerado todos los factores que ello implica, la decisión adoptada no va a cambiar (cosa juzgada).

- **Principio de veracidad:** Se refiere a la autenticidad de la información sustentada en los archivos de los Entes Obligados. Esto significa que la información que se entregue sea verificable y cierta.

- **Principio de transparencia:** Implica la voluntad de los entes de dar a conocer sus actos para su escrutinio público.

- **Principio de máxima publicidad:** Consiste en que los Entes Obligados expongan la información que poseen al escrutinio público y, en caso de duda razonable respecto a la restricción a la información, se optará por su publicidad.

4.4 Objetivos de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal

La LTAIPDF tiene los siguientes objetivos (artículo 9):

- Proveer lo necesario para que toda persona pueda tener acceso a la información pública gubernamental, mediante procedimientos sencillos, expeditos y gratuitos; para lo cual se establecen los procedimientos de presentación y atención de solicitudes de acceso a la información. Así como los medios de impugnación que resultan procedentes (revisión, revocación, reconsideración y denuncias por incumplimiento a las obligaciones de transparencia).

- Optimizar el nivel de participación comunitaria en la toma de decisiones, y en la evaluación de las políticas públicas, para lo cual se establecen espacios de interlocución entre los Entes Obligados y la sociedad, a fin de estimular dicha participación y la promoción del Derecho de Acceso a la Información.

- Garantizar el principio democrático de publicidad de los actos del Gobierno del Distrito Federal, transparentando el ejercicio de la función pública, a través de un flujo de información oportuno, verificable, inteligible, relevante e integral, de manera que cualquier persona puede valorar el desempeño de los distintos órganos de gobierno y la aplicación de recursos públicos.

- Mejorar la organización, clasificación y manejo de documentos en posesión de los Entes Obligados.

- Promover y fomentar una cultura de transparencia y acceso a la información pública.

Resumen

La LTAIPDF otorga el Derecho de Acceso a la Información Pública a todas las personas, del cual nadie puede ser excluido al ser un derecho fundamental establecido en la Constitución Política de los Estados Unidos Mexicanos.

La finalidad de la LTAIPDF es transparentar el ejercicio de la función pública, garantizar el efectivo acceso de toda persona a la información pública en posesión de los órganos locales: Ejecutivo, Legislativo, Judicial y autónomos, así como de cualquier entidad, organismo u organización que reciba recursos públicos del Distrito Federal.

La información que generan, administran o está en posesión de los entes públicos del Distrito Federal se considera como un bien del dominio público.

Para solicitar información pública no es necesario que la persona interesada justifique o demuestre las razones que tiene para pedir la información.

Nuestros datos personales no pueden ser divulgados sin nuestro permiso y tenemos derecho antes que nadie a saber qué información se tiene sobre nosotros.

Los entes públicos deben proporcionar la información pública que solicitamos de manera verbal, escrita, por medio electrónico o cualquier otro en el que se encuentre.

Los servidores públicos pueden ser sancionados por la pérdida, destrucción, modificación, alteración u ocultamiento de los documentos, archivos, registros o datos en que se contenga la información pública.

4.5 Información pública de oficio

Uno de los capítulos más importantes de la LTAIPDF, es el relativo a la transparencia y publicidad de los actos de los Entes Obligados, en el cual se establece la divulgación por Internet de información definida como pública de oficio, entendida como aquella información que es de interés general para todas las personas, cuyo acceso no dependa de una solicitud expresa, lo que habilita la apertura informativa del gobierno.

De tal manera, la LTAIPDF incorpora la obligación de los entes de contar con un portal de Internet en el cual se debe incluir un apartado de fácil identificación y acceso, en el que se publique la información que de manera oficiosa debe darse a conocer, debiendo, además, incluir buscadores temáticos que faciliten la localización de la información (artículo 28). En dicho apartado, los entes

deben publicar la información de manera actualizada, para que cualquier persona pueda revisarla, analizarla y usarla para los fines que le convengan, dentro del marco de la legalidad.

A fin de dar a conocer la información con la que cuentan los Entes Obligados, al inicio de cada año (enero de cada año) éstos deben publicar, en sus respectivos sitios de Internet y en los medios que estimen necesarios, un listado de la información que detentan por rubros generales, especificando el ejercicio al que corresponde (año), medios de difusión y lugares en donde se pondrá a disposición de los interesados, con excepción de aquella información considerada como de acceso restringido, en su modalidad de reservada o confidencial (artículo 13).

De esta manera, la información deberá estar debidamente clasificada y ordenada mediante criterios uniformes que faciliten su manejo y comprensión, con lo que se permite a los interesados identificar rápidamente el tipo de información que se encuentra disponible en cada ente, dónde puede encontrarse y el área encargada de su custodia.

La LTAIPDF incluye el catálogo de información considerada como pública de oficio y que deben publicar de manera obligatoria los entes en sus portales de Internet (artículo 14), el cual se complementa con la información específica que deben publicar el órgano Ejecutivo, Legislativo, Judicial, delegaciones, fideicomisos y fondos, Instituto y Tribunal Electoral del Distrito Federal, partidos políticos, Comisión de Derechos Humanos del Distrito Federal, Universidad Autónoma de la Ciudad de México y el INFODF (artículos 15 a 22).

Con el fin de homologar los contenidos de información que se deben publicar en los portales de Internet, en el rubro de información pública de oficio, así como la presentación de ésta, el INFODF ha expedido los siguientes instrumentos:

- Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer los Entes Obligados en sus portales de Internet.

- Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer en sus portales de la Internet los Partidos Políticos en el Distrito Federal.

En estos instrumentos se describen los criterios, tanto de contenido como de forma, de la publicación de la información de oficio, así como sus periodos de actualización.

4.5.1 Información pública de oficio genérica

El artículo 14 de la LTAIPDF establece el catálogo de información pública de oficio que deben publicar de manera obligatoria todos los Entes Obligados, dentro de la cual se encuentra la siguiente:

- **Marco normativo aplicable:**

  Deberá incluir:

  - Acceso a la gaceta oficial del Distrito Federal.
  - Decreto de creación.
  - Leyes, códigos, reglamentos, reglas de procedimiento, manuales administrativos, políticas y demás normatividad que emita y que se encuentre vigente.
  - El vínculo a cada uno de dichos documentos.

En este apartado los sujetos obligados pueden incluir elementos que permitan identificar fácilmente cada instrumento normativo.

- **Remuneración de todos los servidores públicos.**

  Deberá incluir:

  - Datos de todos los trabajadores del Ente Obligado: técnico-operativos, de base, de confianza, los contratados por honorarios asimilados a salarios o prestadores de servicios profesionales, eventuales o cualquier otra denominación de contratación.

- **Presupuesto**

  Deberá incluir:

  - Presupuesto (general, por programas o resultados y por capítulo), informes (trimestrales, de avance, anuales de cuenta pública, estados financieros y presupuestales), ingresos (ordinarios, extraordinarios y autogenerados), gastos (comunicación social), recursos autogenerados.

- **Recomendaciones emitidas al ente por la CDHDF:**

  Deberá incluir:

- Relación de recomendaciones de la CDHDF, de manera cronológica y por tipo de recomendación.

- **Convenios**

  Deberá incluir:

  - Información relativa a los convenios institucionales de todo tipo, celebrados por el Ente Obligado con organismos de la sociedad civil organizada y/o con instituciones públicas y privadas.

- **Concesiones, licencias, permisos y autorizaciones:**

  Deberá incluir:

  - Datos de cada instrumento como el nombre o razón social del titular, el concepto, la vigencia, los bienes, servicios y/o recursos públicos que se aprovecharán o, en su caso, señalar que no hay aprovechamiento de bien alguno.

Es de señalarse que los entes no están obligados a publicar el total de información descrita en el artículo 14 de la LTAIPDF, pues, de acuerdo con las atribuciones que les son conferidas, no la pueden generar, motivo por el cual en los rubros que no les sean aplicables deberán informar dicha circunstancia de manera fundada y motivada, con el objeto de que el Instituto verifique y apruebe de forma fundada y motivada las fracciones aplicables a cada ente.

4.5.2 Información pública de oficio específica

La **información específica** que debe publicar cada Ente Obligado se encuentra listada en los artículos 15 a 22, tal como se muestra a continuación:

- **Poder Ejecutivo** (artículo 15):

  La Procuraduría General de Justicia y la Secretaría de Seguridad Pública del Distrito Federal deben publicar:

  - Estadísticas e índices delictivos, así como los indicadores de la procuración de justicia.

  La Secretaría de Desarrollo Urbano y Vivienda debe publicar:

  - Los usos de suelo, para lo cual podrá incluir mecanismos que permitan la consulta de mapas y planos la localización de cada predio del Distrito Federal y su respectivo tipo de uso de suelo.

La Secretaría de Finanzas debe publicar:

- Sistema electrónico de consulta de cobro de impuestos, servicios, derechos y aprovechamientos, así como el total de las cantidades recibidas por estos conceptos.

Todos los Entes Obligados de la administración pública centralizada que posea la siguiente información deben publicar:

- Relación de constancias, certificados, permisos, licencias, autorizaciones, registro de manifestaciones y dictámenes de las obras que se llevan a cabo en cada una de las delegaciones, que permita conocer el estado, situación jurídica y modificaciones de cualquier índole de cada predio.

- **Poder Legislativo** (Art.16)

  La Asamblea Legislativa debe publicar:

  - Nombres, fotografía y currículo de los actuales 66 diputados en funciones, así como las comisiones y comités a los que pertenecen.
  - Los recursos económicos que, de conformidad con el Reglamento para el Gobierno Interior de la Asamblea Legislativa del Distrito Federal, entrega el Órgano Legislativo a los diputados independientes, grupos parlamentarios o coaliciones, así como los informes que éstos presenten sobre su uso y destino.

  La Contaduría Mayor de la Asamblea Legislativa debe publicar:

  - Los dictámenes de cuenta pública, así como los estados financieros y demás información que los órganos de fiscalización superior utilizan para emitir dichos dictámenes.

- **Poder Judicial** (artículo 17):

  El Tribunal Superior de Justicia del Distrito Federal, el Tribunal de lo Contencioso Administrativo y la Junta Local de Conciliación y Arbitraje deben publicar:

  - Acuerdos y resoluciones del Pleno.
  - Resoluciones o laudos judiciales y administrativos resueltos por jueces y magistrados que hayan causado estado.

El Consejo de la Judicatura del Distrito Federal debe publicar:

- Datos estadísticos anuales de sus actuaciones (información anual sobre las actuaciones de sus áreas sustantivas, el Pleno, la Secretaría General, la Comisión de Disciplina Judicial, la Visitaduría Judicial, la Contraloría y la Comisión de Administración y Presupuesto), sesiones, acuerdos expedidos, jueces ratificados, Jueces de nuevo ingreso, amparos tramitados por tipo, expedientes recibidos, auditorías realizadas, sanciones, etc.
- Resoluciones del órgano de control interno que hayan causado estado.

La Junta Local de Conciliación y Arbitraje debe publicar:

- Información de los contratos colectivos de trabajo que, en ejercicio de sus funciones, ha recibido en depósito, pudiendo dar a conocer número de expediente, denominación o nombre del sindicato, nombre de los dirigentes, número de trabajadores, fecha de depósito, etc.
- Boletín laboral, debiendo incluir la fecha de publicación y el vínculo al documento.
- Base de datos que contenga el registro de todas las asociaciones sindicales locales, patronales y de trabajadores, pudiendo incluir el número de registro, nombre o denominación del sindicato, fecha en la que se otorgó el registro, domicilio, tipo de sindicato (trabajadores de la industria, manufactura, gremial, etcétera) estatuto (reglamento interior).

- **Las delegaciones** (Art.18)

  - Información sobre el presupuesto que destinarán al rubro de mercados, así como el padrón de locatarios, nombre y ubicación de los mercados públicos en su demarcación territorial.

    - Presupuesto destinado a mercados públicos asignado y ejercido.

    - Relación de mercados públicos: nombre del mercado y domicilio.

    - Padrón de locatarios.

- **Los fideicomisos y fondos** (Art.18 BIS)

  - Los documentos y datos que los identifiquen, tales como: contrato o decreto de creación, el nombre del servidor público y de la persona física o moral que represente al fideicomitente, al fiduciario y al fideicomisario.
  - Información desglosada respecto de los recursos económicos recibidos para el ejercicio de las funciones que legalmente le corresponden por subsidios, donaciones, transferencias, aportaciones o subvenciones, ya sea en dinero o en especie, especificando los datos, tanto locales como federales. Asimismo, se detallará el uso y destino final de dichos recursos.
  - Las modificaciones que, en su caso, sufran los contratos o decretos de creación del fideicomiso o del fondo público, señalando el vínculo al documento del contrato o decreto de creación, fecha de modificación del contrato o decreto; así como el documento del contrato o decreto modificado.
  - Causas y motivos por los que se inicia el proceso de extinción del fideicomiso o fondo, especificando de manera detallada los recursos financieros destinados para tal efecto.

- **Instituto Electoral y Tribunal Electoral** (Art.19)

  El Instituto Electoral debe publicar:

  - Los informes entregados por las instituciones políticas sobre el origen, destino y monto de los ingresos que reciban por cualquier modalidad de financiamiento, así como su empleo y aplicación, de conformidad con lo establecido en el Código de Instituciones y Procedimientos Electorales del DF vigente, y con base en los reglamentos y normas de fiscalización aprobados para el efecto. Estos informes se publicarán una vez concluidos los procesos de fiscalización, en su caso, se deberá incluir una leyenda que especifique que se encuentran en proceso de revisión o especificar cuál es la periodicidad que corresponde a cada uno de los tipos de informes que son: informes anuales sobre el origen, monto y destino de los recursos, informes de selección interna de candidatos (de precandidatos ganadores y de precandidatos perdedores), informes de campaña y, finalmente, Informes trimestrales de avance del ejercicio.

El Tribunal Electoral debe publicar:

- Información y documentos relativos a las sentencias que hayan causado ejecutoria y que sean resultado del ejercicio de sus funciones, de conformidad con lo establecido en el Código de Instituciones y Procedimientos Electorales del Distrito Federal, la Ley Procesal Electoral para el Distrito Federal y la demás normatividad relativa.

- **La Comisión de Derechos Humanos del Distrito Federal** (Art.20)
  - Deberá publicar la información y documentos relativos a las recomendaciones emitidas en ejercicio de sus facultades establecidas en la Ley de la Comisión de Derechos Humanos del Distrito Federal vigente.
- **La Universidad Autónoma de la Ciudad de México** (Art.21)
  - Deberá publicar toda la información relacionada con sus procedimientos de admisión.
- **El INFODF** (Art.22)
  - Deberá publicar los resultados de los recursos de revisión interpuestos ante el INFODF contra los actos y resoluciones dictados por los Entes Obligados con relación a las solicitudes de acceso a la información, organizados por ejercicio, en orden progresivo, y el vínculo a la resolución emitida.
  - Asimismo, deberá publicar las estadísticas sobre los recursos de revisión por Ente Obligado, en donde, por lo menos, se proporcionen: número de recursos, sentido de la resolución, cumplimiento de la resolución.

Para facilitar el acceso a la información considerada como pública de oficio, la LTAIPDF establece las siguientes obligaciones:

- Poner a disposición de las personas la información de tal manera que facilite su uso y comprensión.
- Asegurar la **calidad, veracidad, oportunidad y confiabilidad** de la información.
- Dar acceso a la información mediante **bases de datos que permitan la búsqueda y extracción de información.**

- Disponer de un respaldo con todos los registros electrónicos e impresos que contengan la información definida como publica de oficio, para que cualquier persona los pueda consultar.

Con el objeto de evitar la publicación de información incompleta, inteligible o no actualizada, en la LTAIPDF se establece un periodo de **actualización** trimestral de la información pública de oficio, no obstante, en los Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer los Entes Obligados en sus portales de Internet (aprobados el 16 de noviembre de 2011) se determina de manera precisa el periodo de actualización de cada rubro de información.

Cabe señalar que los contenidos de información definidos como información pública de oficio no son limitativos, por lo que los entes pueden publicar de manera adicional toda aquella información que consideren relevante y de interés de las personas.

4.6 De los órganos de control interno

La LTAIPDF también establece obligaciones especiales a los **órganos internos de control** de cada uno de los entes, por lo que hace a (artículo 27):

- La publicación de todas las vistas dadas por el INFODF, derivadas del incumplimiento de las obligaciones señaladas en la LTAIPDF, incluyendo el motivo que las originó y el seguimiento que se les dé.

- La publicidad de los resultados de las auditorías concluidas al ejercicio presupuestal que de cada sujeto obligado realicen el órgano de control interno y la Contaduría Mayor de Hacienda de la Asamblea Legislativa del Distrito Federal, los cuales serán proporcionados a solicitud de parte, debiendo señalar la etapa del procedimiento y los alcances legales de éstos.

- Con relación a las solventaciones o aclaraciones derivadas de las auditorías concluidas, se establece la obligación para los Entes Obligados de proporcionarlas previa solicitud.

4.7 Transparencia Ciudadana

Ante la demanda social de apertura general de la información que responda, de manera anticipada, a temas de interés de las personas, el legislador incorporó, en el artículo 28 de la LTAIPDF, una nueva obligación a los Entes Obligados consistente en contar en sus portales de Internet con un concepto de portal ciudadano o de transparencia ciudadana, en donde se publique información

relevante para el interesado, atendiendo de manera anticipada a la demanda de información.

La publicación de los portales ciudadanos tiene por objeto dar publicidad a las actividades más sobresalientes de los Entes Obligados, los cuales se distinguen por servir a la gente al proporcionar información focalizada pensada en ella, generadora de conocimiento veraz y oportuno sobre lo que se están haciendo en todos los campos de actuación de los Entes Obligados.

De esta manera, se genera un nuevo espacio de oportunidad para dar a conocer información útil, ciudadanizando la información que puede generar beneficios sociales específicos y que se anticipa al interés de la sociedad. Este es un espacio para establecer comunicación directa con las autoridades, a fin de que el usuario del portal obtenga respuestas a información de eventos relevantes en marcha o por venir, permitiendo tomar decisiones oportunas a la par.

De igual forma, se facilita la comprensión de la información al utilizar un lenguaje ciudadano y no técnico.

En los portales ciudadanos se debe publicar información de manera distinta y complementaria a la información de oficio que, de manera obligada, deben publicar los entes públicos en sus portales de Internet. Se trata de publicar información integrada de manera que contenga, en un nuevo producto, todos los elementos asociados que permitan entender el quehacer gubernamental.

La información que se publique en los portales ciudadanos o de transparencia debe responder preguntas fundamentales, como pueden ser: ¿Qué debo saber sobre determinado tema? ¿Qué impacto tiene en mi vida cotidiana? ¿Qué puedo hacer al respecto? ¿Qué hace el Gobierno del Distrito Federal sobre este tema? ¿Cuál es o ha sido el comportamiento de un problema o actividad relevante?

Con la publicación de portales ciudadanos se amplían los beneficios de la transparencia a la sociedad.

- Portal de Medio Ambiente: **http://www.sma.df.gob.mx/sma/index.php**
- Portal Ciudadano del Gobierno del Distrito Federal: **http://www.df.gob.mx/**
- Portal de Obras Públicas que se están ejecutando: **http://www.obrasenmiciudad.df.gob.mx/**

- Portal de Programas Sociales del Gobierno del Distrito Federal: **http://www.redangel.df.gob.mx/index.php?option=com_content&view=article&id=66&Itemid=56**

- Portal del Presupuesto Ciudadano de la Secretaria de Finanzas del Gobierno del Distrito Federal: **http://www.finanzas.df.gob.mx/pciudadano/**

Resumen

En este apartado se abordaron tres de las obligaciones fundamentales de los Entes Obligados:

- Publicar cada año un listado por rubros generales de la información que generan o tienen bajo su custodia.

- Publicar y mantener actualizada, de forma impresa y en sus respectivos sitios de Internet, la información definida como pública de oficio (general y específica).

- La apertura informativa que responda, de manera anticipada, a temas de interés de las personas, a partir de la publicación de portales ciudadanos o de transparencia ciudadana en donde se publique información relevante para el interesado, atendiendo de manera anticipada a la demanda ciudadana de información.

4.8 De la organización interna de los Entes Obligados en materia de transparencia y acceso a la información

En términos de la LTAIPDF, todos y cada uno de los Entes Obligados deben contar al interior de su organización con una oficina de información pública y un comité de transparencia, los cuales constituyen instancias fundamentales en el ejercicio del Derecho de Acceso a la Información. Por lo anterior, es necesario analizar las atribuciones que les son conferidas así como su funcionamiento.

4.8.1 Oficina de Información Pública (OIP)

La oficina de información pública es la unidad administrativa que funge como vínculo entre los distintos Entes Obligados y los solicitantes que deseen conocer información pública que generan, administran o detentan dichos entes, por lo que debe asesorar y orientar de manera sencilla, comprensible y accesible a los solicitantes sobre:

- La elaboración de solicitudes de información.

- Trámites y procedimientos que deben realizarse para solicitar información.

- Las instancias a las que pueden acudir a solicitar orientación, consultas o interponer quejas sobre la prestación del servicio.

La LTAIPDF define a la OIP como la unidad administrativa receptora de las peticiones ciudadanas de información, a cuya tutela estará el trámite de las mismas, conforme al reglamento de esta Ley (artículo 4, fracción XIII).

Las atribuciones conferidas a las OIP's se encuentran definidas en el artículo 58 de la LTAIPDF, dentro de las cuales se encuentran:

- La principal y más importante es la recepción, registro y atención de las solicitudes de información presentadas ante el Ente Obligado.

- Tramitar el procedimiento de acceso a la información en los términos definidos en la LTAIPDF, así como realizar las notificaciones correspondientes.

- Mantener actualizada la información definida como publica de oficio, actividad que debe realizar de manera conjunta con todas las unidades administrativas que cuenten con la información, atendiendo los plazos de actualización previstos en los Criterios y metodología de evaluación de la información pública de oficio que deben dar a conocer los Entes Obligados en sus portales de Internet, aprobados el 16 de noviembre de 2011.

- Informar de manera trimestral, a su comité de transparencia, el registro de las solicitudes, su trámite, los costos y los resultados de la atención de éstas.

- Al ser sólo el vínculo con los solicitantes de información, a fin de garantizar el acceso a la información pública que les sea solicitada, así como la protección de información de acceso restringido, puede requerir la opinión técnica de las unidades administrativas que estime convenientes, con el objeto de brindar de mejores elementos de convicción para justificar adecuadamente la clasificación de información, antes de someterla a consideración del comité de transparencia.

- Presentar al comité de transparencia las propuestas de clasificación de información realizadas por las unidades administrativas, siendo dichas unidades las que deben aportar los elementos objetivos que den sustento a la clasificación de la información.

Otra obligación conferida a las oficinas de información pública es la de poner a disposición de las personas interesadas equipo de cómputo, que les permita obtener la información de su interés, mediante su consulta o mediante impresiones, las cuales se expedirán previo pago de derechos por concepto de reproducción de la información.

Si bien la OIP es la unidad administrativa encargada de tramitar y atender las solicitudes de información que les sean presentadas, de conformidad con la LTAIPDF no está obligada a dar trámite a las solicitudes que resulten ofensivas, por lo que podrá tenerlas por no presentadas.

4.8.2 Comité de Transparencia

El comité de transparencia es una instancia de decisión creada en todos los Entes Obligados para analizar y decidir sobre diversos aspectos que intervienen en el proceso de acceso a la información pública y en el cumplimiento de las obligaciones de transparencia de cada ente.

Su propósito es asegurar que todas las acciones en materia de transparencia y acceso a la información de los entes se apeguen a la legislación vigente, así como crear una cultura de transparencia al interior de los entes.

De acuerdo con la LTAIPDF, el Comité de Transparencia es competente para (artículo 61):

- Revisar la propuesta de clasificación de la información presentada por la oficina de información pública del Ente Obligado, a fin de confirmar, modificar o revocar la clasificación; de resultar procedente puede determinar la elaboración de la versión pública de la información solicitada. De igual forma, debe suscribir las declaraciones de inexistencia de la información y, en su caso, ordenar la generación de la información, siempre y cuando sea posible. De esta manera se evita la discrecionalidad de las respuestas, ya que no basta con que el titular de la unidad administrativa responda que la información es de acceso restringido.

- En caso de que la información que le sea solicitada a un Ente Obligado no sea localizada, el Comité deberá tomar las medidas necesarias para su localización y resolver en consecuencia.

- Establecer la o las oficinas de información que sean necesarias y vigilar el efectivo cumplimiento de las funciones de éstas, a fin de facilitar y garantizar el Derecho de Acceso a la Información.

- Capacitar y actualizar a los servidores públicos adscritos a la o las oficinas de información pública en materia de transparencia y acceso a la información.

- Elaborar y enviar al INFODF la información necesaria para la elaboración del informe del Instituto, el cual se integrará con la información que proporcione la oficina de información pública y todas las unidades administrativas.

4.9 Procedimiento de acceso a la información

En este apartado se abordará el procedimiento de acceso a la información ante las oficinas de información pública de los Entes Obligados; dicho procedimiento se encuentra descrito en el Capítulo I del Título Segundo de la LTAIPDF, el cual comprende del artículo 45 al 57.

En primer lugar, es necesario exponer los principios en los que se sustenta el proceso de acceso a la información pública, para, posteriormente, abordar lineamientos, criterios, requisitos, tiempos de respuesta, excepciones y costos que regulan el ejercicio del Derecho de Acceso a la Información Pública, tanto en lo que corresponde al solicitante como en lo que compete a los Entes Obligados.

4.9.1 Principios rectores del procedimiento de acceso a la información

El procedimiento para el ejercicio del Derecho de Acceso a la Información Pública se rige por los siguientes principios (artículo 45):

Máxima publicidad

Se refiere al hecho de que toda información que tenga en su poder un Ente Obligado debe considerarse como información pública y, por lo mismo, debe estar a la disposición de todas las personas para su consulta, salvo que se encuentre en alguno de los casos de excepción. También refiere que los entes deben exponer al escrutinio público la información que poseen y, en caso de que haya duda entre la publicidad o reserva de la información, deberán favorecer inequívocamente su publicidad.

Simplicidad y rapidez

Se refiere a que los procedimientos para acceder a la información pública deben estar diseñados para garantizar que cualquier persona pueda, libremente y de manera sencilla, clara y expedita, ejercer su Derecho de Acceso a la Información Pública y sin condicionamientos de ninguna índole.

Gratuidad del procedimiento

La gratuidad del Derecho de Acceso a la Información Pública significa que, por ningún motivo, los entes públicos pueden cobrar a las personas por la asesoría, recepción de solicitud, realización del trámite, búsqueda de la información y entrega de ésta, lo que garantiza que todas las personas estén en posibilidades de ejercer estos derechos.

Costo razonable por la reproducción

Los medios de reproducción de la información y su envío deben tener un costo razonable para el solicitante, nunca la información. Es decir, el solicitante debe cubrir un costo razonable cuando requiera que la información se le entregue en materiales como CD, disquetes, casetes, copias simples o certificadas, entre otros, y, en su caso, el envío de la información a su domicilio por medio de mensajería.

Libertad de información

Esta es una garantía fundamental de cualquier régimen democrático; es el principal fundamento sobre el que se basa el Derecho de Acceso a la Información tutelado por la LTAIPDF, se relaciona con el derecho de todo individuo a informarse, informar y ser informado.

Buena fe del solicitante

El servidor público no deberá calificar la intención de las personas al ejercer su Derecho de Acceso a la Información; esto quiere decir que no debe importar la intencionalidad que las personas tienen al momento de presentar su solicitud de información. Este principio parte de un voto de confianza al interesado en cuanto a los propósitos de su solicitud. La normatividad establece que toda persona tiene derecho a solicitar información sin necesidad de sustentar justificación o motivación alguna, siempre que no sea expresamente de acceso restringido (artículo 45), por lo que queda a responsabilidad del interesado la intencionalidad de su petición.

4.9.2 Orientación y asesoría a los particulares

Los servidores públicos de los sujetos obligados deben facilitar a las personas el acceso a la información, por lo que debe ser orientada y asesorada respecto de los requisitos, procedimientos, tiempos, utilización de los medios electrónicos y, en general, todo aquello que se relacione con el ejercicio del Derecho de Acceso a la Información Pública, de tal manera que las personas tengan el mayor auxilio en el proceso y obtención de la información que requieren.

4.9.3 Del procedimiento de acceso a la información pública

Una cuestión fundamental para un efectivo ejercicio del Derecho de Acceso a la Información Pública es el establecimiento de un procedimiento sencillo y expedito, el cual puede ser iniciado por cualquier persona, sin necesidad de que sea especialista en la materia.

4.9.4 Instancia ante la que se presenta la solicitud

La solicitud de información se debe presentar ante la oficina de información pública de los Entes Obligados, por escrito material (en papel) ante la propia OIP, por correo electrónico, a través del sistema electrónico INFOMEX, de manera verbal, ya sea en persona (cuando la índole del asunto lo permita) o a través del sistema telefónico "TEL-INFODF", instrumentado por el INFODF.

4.9.5 Requisitos

Los solicitantes, al momento de presentar una solicitud de acceso a la información, deben cumplir los siguientes requisitos (artículo 47):

- Datos de identificación del ente a quien se dirige la solicitud.
- Descripción clara y precisa de los datos e información que solicita.
- El medio para recibir la información y notificaciones, el cual puede ser domicilio, correo electrónico, INFOMEX, correo certificado, fax o, en su caso, el solicitante puede acudir directamente a las instalaciones de la propia OIP. En el caso de que el solicitante no señale medio para oír y recibir notificaciones, éstas se realizarán por lista que se fije en los estrados de la oficina de información pública del Ente Obligado que corresponda.
- La modalidad de acceso a la información, la cual puede ser mediante consulta directa, copias simples, certificadas o cualquier otro tipo de medio electrónico. La información deberá ser proporcionada de manera electrónica siempre y cuando se tenga digitalizada y sin que ello implique su procesamiento.

  Si bien el solicitante puede elegir la modalidad de acceso a la información, el Derecho de Acceso a la Información se tendrá por satisfecho cuando se ponga a su disposición en el estado en que se encuentre en los archivos de los entes, circunstancia que debe ser informada al solicitante fundando y motivando el cambio de modalidad (artículo 11).

De manera opcional, los solicitantes podrán proporcionar datos que permitan definir su perfil como requirentes de información, sin identificarlo y únicamente con fines estadísticos. Esta información será proporcionada por el solicitante si lo desea y en ningún caso podrá ser un requisito para la procedencia de la solicitud.

4.9.6 Prevención

En caso de que la OIP identifique que la solicitud no es precisa o no cumple con los requisitos señalados en el apartado anterior, deberá prevenir al solicitante por escrito, en un plazo no mayor a 5 días hábiles a partir de la recepción de la solicitud, para que éste, en un plazo igual de 5 días hábiles, complemente o aclare su solicitud.

Para el caso de que el particular haya presentado vía solicitud de acceso a la información una relativa a datos personales, la oficina de información pública deberá prevenir al solicitante sobre el alcance de la vía elegida y los requisitos exigidos por la Ley de Protección de Datos Personales del Distrito Federal.

Si el solicitante no desahoga la prevención que le sea formulada, ésta se tendrá por no presentada, circunstancia que deberá ser notificada al solicitante.

4.9.7 Canalización de solicitudes

Si la solicitud es presentada ante un ente que no es competente para atender la solicitud de información, la OIP receptora deberá comunicar dicha circunstancia al solicitante y orientarle respecto al ente que, considere, es competente para su atención; y en un plazo no mayor de cinco días hábiles, deberá remitir la solicitud a la oficina de información pública que corresponda (a través del sistema INFOMEX, correo electrónico o cualquier otro medio).

En caso de que la solicitud sea presentada ante un Ente Obligado que, teniéndola, sólo cuente con atribuciones sobre ésta para su resguardo en calidad de archivo de concentración o histórico, la oficina receptora orientará al solicitante, y en un plazo no mayor de cinco días hábiles, deberá canalizar la solicitud a la OIP que corresponda (un claro ejemplo es la Oficialía Mayor del Distrito Federal que concentra y resguarda, por disposición de Ley, los documentos que las dependencias, unidades administrativas y órganos desconcentrados le remiten).

4.9.8 Orientación

En caso de que el Ente Obligado sea parcialmente competente para atender la solicitud de información que le sea planteada, dará respuesta a la solicitud por lo que toca a sus atribuciones y orientará al solicitante para que presente su solicitud ante el ente que considere competente para atender el resto de la solicitud, debiendo informar los datos de contacto de la oficina de información pública del ente competente para atender la solicitud (nombre, domicilio de la OIP, correo electrónico).

4.9.9 Procedimiento

Una vez que se tiene por presentada la solicitud, la OIP gestionará la solicitud ante las unidades administrativas del ente que puedan atender la solicitud de información. Concluida la gestión interna de la solicitud, el ente deberá dar respuesta al solicitante proporcionando la información requerida o negando su entrega, en un plazo no mayor a 10 días hábiles, contados a partir de que se tenga por recibida la solicitud o se tenga por desahogada la prevención.

En caso de que el solicitante deba hacer un pago por la entrega de la información, el ente deberá generar el recibo de pago correspondiente, en el que se señale el monto a cubrir y la institución ante la cual se debe realizar el pago. Realizado el pago por parte del solicitante, la entrega de la información se realizará en un plazo máximo de tres días hábiles posteriores a la comprobación del pago.

El ente puede solicitar una ampliación del plazo hasta por 10 días hábiles más en función del volumen o la complejidad de la información, debiendo fundar y motivar debidamente las razones que originan dicha prórroga, lo cual deberá ser notificado al solicitante antes de que venza el primer plazo.

Cuando la solicitud tenga por objeto información considerada como pública de oficio, ésta deberá ser entregada en un plazo no mayor a cinco días hábiles, el cual no es prorrogable. En el caso de que el solicitante requiera información pública de oficio y el Ente Obligado no la tenga digitalizada, deberá entregarla sin ningún costo al solicitante.

Si la solicitud de información tiene por objeto, tanto información pública como información pública de oficio, se considerará como una solicitud mixta y el plazo máximo de respuesta será de 10 días hábiles.

Si el ente no entrega la información una vez concluido el plazo de respuesta, deberá hacerlo en un periodo no mayor a 10 días hábiles posteriores al vencimiento del plazo de respuesta, sin cargo alguno para el solicitante y atendiendo la respuesta en sentido afirmativo en todo lo que le favorezca, excepto cuando la solicitud verse sobre información de acceso restringido.

4.9.10 Del pago de derechos

Al respecto, la LTAIPDF establece que las solicitudes de acceso a la información pública serán gratuitas, no así la reproducción de la información solicitada. Debido a ello, habilita al ente a realizar el cobro de derechos, de acuerdo con lo que se establezca en el Código Fiscal del Distrito Federal. Asimismo, se especifica que los costos de reproducción de la información solicitada se

cobrarán al solicitante antes de la entrega de la información y se calcularán atendiendo a:

- El costo de los materiales utilizados en la reproducción de la información.
- El costo de envío.
- La certificación de documentos, cuando proceda.

La LTAIPDF exhorta a los entes para que reduzcan al máximo los costos de reproducción de la información, por lo que, por disposición de ley, los entes deben procurar documentar la información que generan de manera electrónica.

Una práctica que se ha dado es la adopción de acuerdos en los que distintos entes han optado por digitalizar información que no detentan en esa modalidad, hasta por una determinada cantidad de hojas.

4.9.11 Caducidad del trámite

Si después de 30 días hábiles de haberse emitido la respuesta, el interesado, por cualquier circunstancia, no concluye el trámite y/o no recibe la información, ya sea porque no realiza el pago correspondiente, no es localizado en el lugar que señaló para recibirla y/o no acude a la OIP a recogerla, el trámite se considerará como caduco, por lo que el solicitante no podrá reclamar la información posteriormente. En estos casos, los entes deberán notificar el acuerdo correspondiente.

Es de destacarse que las solicitudes de acceso a la información y las respuestas que se les dé son públicas, por lo que los entes deben poner a disposición de cualquier persona dicha información.

Así mismo, la OIP debe informar a los solicitantes su derecho de impugnar la respuesta a su solicitud cuando se considere que es ambigua o imparcial, o cuando no se está de acuerdo con la respuesta otorgada a su solicitud. Esto mediante la presentación de un "recurso de revisión" ante el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Resumen

El acceso a la información atiende a los principios de: máxima publicidad, simplicidad y rapidez, gratuidad del procedimiento, costo razonable por la reproducción, libertad de información, buena fe del solicitante, y orientación y asesoría a los particulares.

Todos los entes públicos deben contar con una "oficina de información pública (OIP)", que es la encargada, entre otras funciones, de recibir las solicitudes de información, asesorar a los solicitantes y llevar a cabo los procedimientos para su atención.

Para garantizar el ejercicio del Derecho de Acceso a la Información, la LTAIPDF establece el procedimiento que deberá seguirse ante los distintos Entes Obligados.

El procedimiento inicia con la presentación de la solicitud de información ante la OIP de los Entes Obligados, por escrito material (en papel), correo electrónico, en forma verbal, ya sea en persona (cuando la índole del asunto lo permita) o vía telefónica a través del sistema telefónico "TEL-INFODF" implementado por el INFODF.

La solicitud debe cumplir con los requisitos establecidos en el artículo 47 de la LTAIPDF, que permiten una comunicación ágil entre el ente y quienes ejercen el Derecho de Acceso a la Información Pública.

Una vez presentada la solicitud, el ente podrá prevenir al solicitante, admitir la solicitud o desecharla.

En caso de admisión, el plazo de atención a la solicitud es de 10 días hábiles, contados a partir de que se tenga por recibida la solicitud, el cual podrá ser ampliado hasta por 10 días más en función del volumen o la complejidad de la información, circunstancia que debe notificarse al solicitante.

Cuando se requiera información considerada como pública de oficio, ésta se deberá atender en un plazo no mayor a 5 días hábiles.

En caso de que el Ente Obligado sea competente para atender sólo una parte de la solicitud, éste deberá canalizarla al ente que tenga competencia para atender el resto de la solicitud. Asimismo, podrá orientar al solicitante para que presente su solicitud ante el ente que considere que tiene la información solicitada o, en su caso, informar de manera fundada y motivada la imposibilidad de dar acceso a ésta.

Cuando el solicitante deba pagar por la reproducción de la información, la documentación solicitada debe entregarse en un tiempo máximo de tres días hábiles posteriores a que compruebe el pago de ésta ante la OIP.

Se aplica la "caducidad del trámite" cuando después de 30 días hábiles de haberse emitido la respuesta el interesado, por cualquier circunstancia, no concluye el trámite y/o no recibe la información, ya sea porque no realiza el

pago correspondiente, no es localizado en el lugar que señaló para recibirla y/o no acude a la OIP a recibirla .

4.10 Información restringida

La Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (LTAIPDF) reconoce la información gubernamental como un bien de dominio público accesible a cualquier persona en los términos que la propia ley señala. De tal manera, toda la información que detentan, administran y poseen los distintos sujetos obligados del Distrito Federal es pública.

No obstante lo anterior, la publicidad de la información admite algunas excepciones tendientes a proteger el interés público y la vida privada de las personas; la primera, como excepción temporal de lo público; y la segunda, como restricción permanente.

De tal manera, la LTAIPDF, en su Capítulo IV, Título Primero (artículos del 36 al 44), establece que la información podrá ser clasificada como de acceso restringido en sus modalidades de reservada y confidencial, y no podrá ser divulgada en los términos que la propia Ley señala.

También establece, como regla general, que la información deberá ser clasificada por el sujeto obligado antes de dar respuesta a una solicitud de acceso a la información y no de manera anticipada. De igual forma, precisa que no podrá clasificarse información como de acceso restringido antes de que ésta sea generada.

En caso de que existan datos que contengan parcialmente información cuyo acceso se encuentre restringido en los términos de lo establecido por la propia Ley, deberá proporcionarse el resto de la información que no tenga tal carácter mediante una versión pública.

En este sentido, en los casos en que los sujetos obligados consideren que se actualiza alguno de los supuestos de reserva o confidencialidad de la información, no bastará con que el ente informe dicha circunstancia a los solicitantes, pues deberá atender el procedimiento de clasificación de la información previsto en el artículo 50 de la LTAIPDF, en el cual el comité de transparencia puede confirmar, revocar o modificar la clasificación que se le proponga.

El artículo referido establece el siguiente procedimiento:

- El responsable de la clasificación de la información es la unidad administrativa que la posea, por lo tanto, ésta deberá remitir al titular de

la oficina de información pública la solicitud, así como un oficio con los elementos necesarios para fundar y motivar la clasificación para que la OIP someta el asunto a consideración de su comité de transparencia, y sea éste el que resuelva.

Es de señalarse que en las solicitudes que existan duda respecto a la clasificación de la información, la oficina de información pública, antes de someterla a consideración del Comité, deberá solicitar la opinión técnica de aquellas unidades o áreas administrativas que estime convenientes, con el objeto de dotar de mayores elementos que justifiquen adecuadamente la clasificación de la información como reservada o confidencial.

- A partir de la propuesta de clasificación y los elementos aportados al comité de transparencia, éste podrá:
  - Confirmar, negando el acceso a la información.
  - Modificar la clasificación y conceder el acceso a parte de la información (versión pública).
  - Revocar la clasificación y conceder el acceso a la información.
- Durante la tramitación de este procedimiento el comité de transparencia podrá tener acceso a los documentos que se encuentren en poder del sujeto obligado.

4.10.1 Información reservada

La información reservada es aquella que se encuentra temporalmente fuera del acceso público debido a que su difusión puede poner en riesgo la vida, seguridad y salud de las personas; así como la seguridad, estabilidad, gobernabilidad del Estado.

El artículo 6º constitucional establece, en su fracción I, que la información pública puede ser reservada temporalmente por razones de interés público en los términos que fijen las leyes.

En este sentido, la LTAIPDF, en su artículo 4, fracción X, define a la información reservada como "la información pública que se encuentre temporalmente sujeta a alguna de las excepciones previstas en esta Ley".

El artículo 37 de la LTAIPDF establece las hipótesis de reserva temporal de la información, dentro de las cuales se encuentran, entre otras:

- Cuando su divulgación ponga en riesgo:
    - La seguridad pública nacional o del Distrito Federal.
    - La vida, la seguridad o la salud de cualquier persona.
    - El desarrollo de investigaciones reservadas.

En estos supuestos se busca salvaguardar la vida, la seguridad y la salud de toda persona, bienes jurídicamente tutelados cuya divulgación puede poner en riesgo a sus titulares y que al estar vinculados con la función pública pueden ser fácilmente vulnerados.

Por otra parte, la seguridad implica la protección de información relacionada con las medidas encaminadas a garantizar los mínimos de control frente a acontecimientos que alteren la estabilidad ordinaria del país o del Distrito Federal o bien, que pueda causar un perjuicio o daño irreparable a las instituciones públicas.

- Cuando su divulgación impida:
    - Las actividades de verificación sobre el cumplimiento de las leyes.
    - La prevención o persecución de los delitos.
    - La impartición de justicia.
    - La recaudación de las contribuciones.

En este supuesto se debe clasificar toda aquella información relacionada con acciones de corte policial, cuya divulgación pueda entorpecer la prevención e investigación de delitos; así como toda aquella información cuya publicidad pueda perjudicar la impartición de justicia en el Distrito Federal.

De igual forma se debe proteger aquella información que pueda generar la evasión de la aplicación de una ley o el pago de impuestos.

- Cuando la ley expresamente la considere como reservada. Esto se refiere a la reserva de aquella información que, de manera explícita, sea definida como tal por el legislador. Un ejemplo es la Ley que Regula el Uso de la Tecnología para la Seguridad Pública del Distrito Federal, que, en su artículo 23, define aquella información que es considerada como reservada.

- Se relacione con:
    - La propiedad intelectual.

- Patentes o marcas en poder de los sujetos obligados u otra considerada como tal por alguna otra disposición legal.

Se debe proteger aquella información relacionada con la propiedad intelectual patentes y marcas, en atención a los derechos que de ellas derivan y que surten efectos contra terceros, de conformidad con la Ley de la Propiedad Industrial y demás normatividad aplicable.

- Los expedientes, archivos y documentos que se obtengan producto de las actividades relativas a la prevención, que llevan a cabo las autoridades en materia de seguridad pública y procuración de justicia en el Distrito Federal. En esta hipótesis encuadra toda aquella información y documentos cuya publicidad pueda poner en riesgo las actividades que, de manera preventiva, llevan a cabo los sujetos obligados en materia de seguridad pública y de procuración de justicia.

- Las averiguaciones previas en trámite. Esto implica la obligación de salvaguardar toda aquella información que pueda entorpecer la investigación y el ejercicio de la acción penal.

- Cuando se trate de expedientes judiciales o procedimientos administrativos seguidos en forma de juicio, mientras la sentencia o resolución de fondo no haya causado ejecutoria. Se debe proteger la información contenida en los expedientes sustanciados ante los órganos judiciales y las distintas autoridades administrativas, en tanto no se agoten los procedimientos respectivos y hayan causado ejecutoria; esto es, que ya no puede ser impugnada.

- Los expedientes, archivos y documentos que se obtengan producto de las actividades relativas a la prevención, que llevan a cabo las autoridades en materia de seguridad pública y procuración de justicia en el Distrito Federal.

- Cuando se trate de procedimientos de responsabilidad de los servidores públicos, quejas y denuncias tramitadas ante los órganos de control, en tanto no se haya dictado la resolución administrativa definitiva.

- La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, en tanto pueda influenciar un proceso de toma de decisiones que afecte el interés público y hasta que no sea adoptada la decisión definitiva.

- La contenida en informes, consultas y toda clase de escritos relacionados con la definición de estrategias y medidas a tomar por los Entes Obligados en materia de controversias legales.

- La que pueda generar una ventaja personal indebida en perjuicio de un tercero o de los Entes Obligados.

- La transcripción de las reuniones e información obtenida por las Comisiones de la Asamblea Legislativa del Distrito Federal, cuando se reúnan en el ejercicio de sus funciones fiscalizadoras para recabar información que podría estar incluida en los supuestos de este artículo.

- La relacionada con la seguridad de las instalaciones estratégicas de los Entes Obligados. En este punto los Entes Obligados deben salvaguardar aquella información relacionada con infraestructura de las instalaciones con las que cuentan para el ejercicio de sus funciones, a fin de evitar acciones tendientes a intervenir o sabotear, que potencialicen una amenaza a las instituciones del Distrito Federal (oficinas de gobierno, centros de readaptación social, instalaciones de agua, luz o gas, plantas de tratamiento de agua, instalaciones de transporte público, etc.)

De esta manera, la información que se considere en alguna de las hipótesis previstas en el artículo 37 de la LTAIPDF deberá ser clasificada como reservada mediante resolución fundada y motivada, en la cual se expongan los elementos objetivos y verificables que identifiquen la probabilidad de dañar el interés público protegido (prueba de daño).

La información deberá ser reservada al responder la solicitud de acceso a la información, momento a partir del cual se contabiliza el plazo de reserva, por lo que la LTAIPDF prohíbe la emisión de acuerdos clasificatorios previos a la presentación de una solicitud de información.

Por otra parte, la LTAIPDF establece excepciones a la reserva de la información, por lo tanto, no podrá ser considerada como reservada por los Entes Obligados ni podrá dejarse de difundir aquella información relacionada con:

- La investigación de violaciones graves a derechos humanos.

- Delitos de lesa humanidad.

Asimismo, la Ley prohíbe de manera expresa la emisión de acuerdos generales que clasifiquen información como reservada.

Plazos de restricción

La LTAIPDF establece, en su artículo 40, que el periodo de reserva de la información puede ser hasta por 7 años contados a partir de la clasificación, periodo que podrá ser excepcionalmente renovado hasta por 5 años más,

siempre y cuando subsista alguna de las causales que dieron lugar a la reserva de la información y las autoridades competentes consideren que debe continuar reservada la información.

Para renovar el plazo de reserva, el sujeto obligado deberá informar dicha circunstancia al INFODF para que éste emita la recomendación respectiva en un plazo no mayor a 30 días naturales a partir de la solicitud. El INFODF deberá valorar si persisten las condiciones y si corresponde la reserva por cinco años más; dicha resolución será vinculante para los sujetos obligados, por lo que estos últimos están obligados a acatar la recomendación del Instituto.

Las causales de reserva desaparecen cuando:

- Dejen de existir los motivos que justificaban la restricción, aun y cuando no haya concluido el periodo de reserva, por lo que los sujetos obligados podrán difundirla.
- Sea necesaria para la defensa de los derechos del solicitante ante los tribunales.
- Por resolución firme del INFODF, en la que se invalide la determinación del sujeto obligado mediante resolución a un recurso de revisión.

4.10.2 Información confidencial

Se define en el artículo 4, fracción VII, como aquella información que contiene datos personales y se encuentra en posesión de los Entes Obligados, siendo susceptible de ser tutelada por el derecho fundamental a la privacidad, intimidad, honor y dignidad y aquella que la ley prevea como tal.

Este tipo de información se mantendrá con tal carácter de manera indefinida y sólo podrán tener acceso a ella los titulares de ésta y aquellos servidores públicos que requieran conocerla para el debido ejercicio de sus funciones.

En sentido amplio, esta modalidad protege dos derechos fundamentales que son el derecho a la vida privada y a la protección de datos personales.

La LTAIPDF contempla como información confidencial (artículo 38):

- Los datos personales que requieran del consentimiento de las personas para su difusión, distribución o comercialización y cuya divulgación no esté prevista en una ley. Se consideran datos personales, entre otros: la información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable, la relativa a su

origen racial o étnico, las características físicas, morales o emocionales a su vida afectiva y familiar, información genética, número de seguridad social, la huella digital, domicilio y teléfonos particulares, preferencias sexuales, estado de salud físico o mental, correos electrónicos personales, claves informáticas, cibernéticas, códigos personales, creencias o convicciones religiosas, filosóficas y morales u otras análogas que afecten su intimidad.

- La información protegida por la legislación en materia de derechos de autor o propiedad intelectual. Lo anterior en atención a las normas especiales que rigen los derechos de autor y la propiedad intelectual y que prevén periodos de protección específicos.

- La relativa al patrimonio de una persona moral de derecho privado, entregada con tal carácter a cualquier sujeto obligado. Dicha información debe ser protegida, toda vez que se refiere al conjunto de bienes, derechos y obligaciones pertenecientes a una persona moral, los cuales salen de la esfera de lo público.

- La relacionada con el derecho a la vida privada, el honor y la propia imagen[19]. En este supuesto se debe proteger del conocimiento público:

  Aquella información que no está dedicada a una actividad pública y que, por ende, es intrascendente y sin impacto en la sociedad de manera directa; incluye conductas y situaciones que, por su contexto y por desarrollarse en un ámbito estrictamente privado, no están destinados al conocimiento de terceros o a su divulgación o no se han difundido por el titular del derecho.

  El honor, el cual se relaciona con la valoración que las personas hacen de la personalidad ético-social de un sujeto y que se identifica con la reputación y la fama.

  La propia imagen, que se relaciona con la reproducción identificable de los rasgos físicos de una persona sobre cualquier soporte material.

- La información protegida por el secreto comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal. En estos supuestos se debe de extraer de lo público toda aquella información que genere una ventaja competitiva para el poseedor de la información comercial[20] e industrial[21] frente a un tercero, la relacionada

[19] Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal; artículos 9 a 21.

[20] Organización Mundial de la Propiedad Intelectual. Patentes o secretos comerciales? Consultable en Ohttp://www.wipo.int/sme/es/ip_business/trade_secrets/patent_trade.htm

[21] LÓPEZ-AYLLÓN, Sergio. Las pruebas de daño e interés público en materia de acceso a la información. Una perspectiva comparada. Consultable en http://www.juridicas.unam.mx/inst/becarios/eureka/3/art2.htm.

con operaciones realizadas por los usuarios con instituciones bancarias[22], con autoridades en ejercicio de sus funciones de recaudación, etc.

No podrá invocarse el secreto bancario o fiduciario cuando el titular de las cuentas sea un sujeto obligado, ni cuando se hubieren aportado recursos públicos a un fideicomiso de carácter privado, en lo que corresponda a la parte del financiamiento público que haya recibido.

Tampoco podrá invocarse el secreto fiduciario cuando el sujeto obligado se constituya como fideicomitente o fideicomisario de fideicomisos públicos.

Por lo que hace a los créditos fiscales, respecto de los cuales opere una disminución, reducción o condonación, no podrán ser motivo de confidencialidad y, por tanto, se debe dar a conocer el nombre, el monto y la razón que justifique el acto.

Resumen

La LTAIPDF incorpora las causales de excepción a la publicidad de la información, tendientes a proteger el interés público (como excepción temporal de lo público) y la vida privada de las personas (como restricción permanente sólo reductible para efectos de una mejor aplicación de las leyes).

De esta manera, sólo podrá clasificarse como información de acceso restringido en su modalidad de reservada o confidencial, aquélla que se encuentre dentro de las hipótesis previstas en los artículos 37 y 38 de la LTAIPDF.

La información reservada se encuentra temporalmente sujeta a algunas de las excepciones previstas en la Ley. De conformidad con la LTAIPDF, el plazo máximo de reserva es de 12 años, siempre y cuando subsistan las causas que dieron origen a la reserva.

En tanto que la Información confidencial protege el derecho a la vida privada y a la protección de datos personales. La difusión de esta información requiere del consentimiento de las personas para su difusión, distribución o comercialización y cuya divulgación no esté prevista en una Ley; esta información se mantendrá con tal carácter de manera permanente.

Cuando los sujetos públicos consideren que la información que les es solicitada tenga el carácter de reservada o confidencial, deberán atender el procedimiento de clasificación previsto en el artículo 50 de la LTAIPDF, sometiendo a consideración de su comité de transparencia dicha circunstancia para que este órgano de decisión determine la procedencia o no de la clasificación.

[22] DÁVALOS, Susana. Las facultades de fiscalización del IFE y el secreto bancario. Consultable en http://www.juridicas.unam.mx/inst/becarios/eureka/3/art2.htm

5. Excepciones a la publicidad y a las restricciones de la información

5.1 Prueba de Daño

La LTAIPDF define a la prueba de daño como la carga de los sujetos obligados de demostrar que la divulgación de la información lesiona el interés jurídicamente protegido por la ley, y que el daño que puede producirse con la publicidad de la información es mayor que el interés de conocerla (artículos 4, fracción XVI, y 42).

Sólo procede la acreditación de prueba de daño cuando se trate de información considerada como reservada, en términos del artículo 37 de la LTAIPDF.

De esta manera, los encargados de acreditar la prueba de daño son los sujetos obligados, que deberán:

- Indicar la fuente de la información.
- Indicar que la información solicitada encuadra en las hipótesis de reserva previstas en el artículo 37 de la LTAIPDF.
- Exponer las razones por las cuales considera que la divulgación de la información lesiona el interés que protege.
- Precisar que el daño que puede producirse con la publicidad de la información es mayor que el interés público de conocerla.
- Fundar y motivar su determinación.
- Precisar las partes de los documentos que se reservan.
- Indicar el plazo de reserva.
- Designar a la autoridad responsable de la conservación, guarda y custodia de la información.

Es importante señalar que la información de naturaleza confidencial no admite prueba de daño, toda vez que sólo tiene acceso a ella su titular.

5.2 Excepciones a la información confidencial

Tal como quedó señalado en apartados anteriores, la información confidencial no está sujeta a plazos de restricción temporales, tal como ocurre con la

información considerada como reservada, así que permanecerá con tal carácter de manera indefinida y sólo se garantizará el acceso a sus titulares.

Si bien es cierto que la protección de la información confidencial no está sujeta a plazos de vencimiento, también lo es que la LTAIPDF, de manera excepcional, prevé la publicidad de dicha información, previo consentimiento del titular para su difusión.

En aquellas solicitudes de acceso a la información pública que se encuentren relacionadas con información de carácter confidencial, los sujetos obligados deberán tomar las medidas necesarias para que este tipo de información se mantenga restringida; de tal manera que la procedencia o no de la clasificación de la información deberá ser determinada por el comité de transparencia, siguiendo el procedimiento previsto en el artículo 50 de la LTAIPDF, el cual fue descrito en el apartado 1 titulado "Información restringida" del presente documento.

La determinación del comité de transparencia deberá encontrarse debidamente fundada y motivada, señalando las hipótesis de confidencialidad previstas en el artículo 38 de la LTAIPDF que se consideren en cada caso, exponiendo las razones por las cuales no resulta procedente dar acceso a la información, a fin de dar certeza jurídica al solicitante y garantizar plenamente su Derecho de Acceso a la Información.

5.3 Prueba de interés público

Con el fin de ampliar los mecanismos de acceso a la información pública gubernamental y favorecer el principio de máxima publicidad, en la LTAIPDF se incorporó la Prueba de Interés Público (artículo 4, fracción XXVI, y 87), la cual se define como la obligación del Instituto de fundar y motivar, de manera objetiva, cuantitativa y cualitativa, el beneficio de ordenar la publicidad de la información de acceso restringido por motivos de interés público.

Lo anterior, procede en los recursos de revisión interpuestos por inconformidad con la clasificación de la información como reservada o confidencial (Art. 77, fracción III de la LTAIPDF). En este caso, el recurrente podrá aportar las pruebas que hagan presumible el interés público de la difusión de la información.

Asimismo, de manera excepcional y por razones de interés público, el INFODF podrá ordenar la difusión de la información de acceso restringido mediante la resolución del recurso de revisión, la cual deberá contener una valoración objetiva, cuantitativa y cualitativa de los intereses en conflicto, que permita, razonablemente, asegurar que los beneficios sociales de divulgar la información serán mayores al daño que se pudiera generar.

Durante la sustanciación del recurso de revisión, y en caso de que la información en análisis contenga información confidencial, se respetará la garantía de audiencia de los titulares de los datos personales.

5.4 Versión pública

En la fracción XX, del artículo 4 de la LTAIPDF, se define a la versión pública como el documento en el que se elimina la información clasificada como reservada o confidencial, para permitir su acceso, previa autorización del comité de transparencia.

La versión pública constituye un medio para hacer del conocimiento de las personas que los requieran, información que contiene, tanto información pública como información de acceso restringido; es decir, se trata de una vía para que, sin dejar de tutelar la protección de datos personales y el interés público, se reduzca al mínimo posible la restricción de acceso a la información y así se someta al escrutinio de las personas la información relativa a la función pública, sin afectación a otra esfera de derechos o de protección legal.

De tal manera, la emisión de la versión pública debe ser aprobada por el comité de transparencia de los sujetos obligados a fin de garantizar el Derecho de Acceso a la Información Pública de los solicitantes y verificar que no se dé a conocer información de acceso restringido.

Resumen

Con el propósito de garantizar plenamente el Derecho de Acceso a la Información Pública, la LTAIPDF incorpora las excepciones a la publicidad y a las restricciones de la información, dentro de las cuales se encuentran la prueba de daño, la difusión de manera excepcional de información confidencial y la prueba de interés público.

Tratándose de información reservada, los sujetos obligados deberán acreditar la prueba de daño, justificando que la divulgación de la información que les es solicitada lesiona el interés jurídicamente protegido por la ley y que el daño que puede producirse con su publicidad es mayor que el interés de conocerla.

Por otra parte, la Prueba de Interés Público implica la publicidad de información de acceso restringido por motivos de interés público, y sólo procede en los recursos de revisión interpuestos por inconformidad con la clasificación de la información como reservada o confidencial. Quienes están obligados a su acreditación son el INFODF y el recurrente.

A fin de garantizar el acceso a la información, la LTAIPDF prevé la figura de la

Versión Pública que es el medio por el cual se puede hacer del conocimiento de las personas información que contenga, tanto información pública como de acceso restringido, con lo que se reduce la restricción de acceso a la información.

6. Órgano garante

El Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (INFODF) se encarga de vigilar y promover el cumplimiento de la Ley de Transparencia y Acceso a la Información Pública y de la Ley de Protección a Datos Personales, ambos ordenamientos del Distrito Federal.

Es un órgano autónomo del Distrito Federal, reconocido como tal en la LTAIPDF, dotado de personalidad jurídica y patrimonio propios, así como de autonomía presupuestaria, de operación y de decisión en materia de transparencia y acceso a la información pública.

El funcionamiento e independencia de las decisiones del INFODF le permiten emitir sus decisiones con plena imparcialidad y en estricto apego a la normatividad aplicable al caso, sin tener que acatar o someterse a indicaciones, instrucciones, sugerencias o insinuaciones provenientes de superiores jerárquicos de los Poderes del Distrito Federal.[23]

Este órgano colegiado se integra por un comisionado presidente y cuatro comisionados ciudadanos, representantes de la sociedad civil, los cuales son designados por la Asamblea Legislativa del Distrito Federal y permanecen en su encargo por un periodo de seis años, siendo renovados de manera escalonada sin posibilidad de ser reelegidos.

El presidente del Instituto será nombrado por la Asamblea Legislativa del Distrito Federal para un periodo de tres años, pudiendo ser reelecto por un periodo más.

El Pleno del Instituto será la instancia directiva, y la presidencia, la ejecutiva, por lo tanto tendrá las atribuciones suficientes para hacer cumplir la LTAIPDF, salvo aquellas que le estén expresamente conferidas al Pleno del Instituto.

El Pleno del Instituto sesionará válidamente con la presencia de la mayoría

[23] SENTENCIA dictada en la Acción de Inconstitucionalidad 76/2008 y sus acumuladas 77/2008 y 78/2008, promovidas las dos primeras por el Procurador General de la República y la última por el Partido del Trabajo, en contra del Poder Legislativo del Estado de Querétaro y otras autoridades, y votos particular del Ministro Genaro David Góngora Pimentel y de minoría de este último y del Ministro José de Jesús Gudiño Pelayo. Consultable en http://www.diputados.gob.mx/LeyesBiblio/compila/inconst.htm

simple de sus miembros, tomando sus acuerdos por unanimidad o por mayoría de votos de los asistentes, surtiendo efectos para todos y obligándolos a su cumplimiento.

6.1 Atribuciones del INFODF

Entre las atribuciones del Instituto se encuentra la de resolver los recursos de revisión interpuestos contra los actos y resoluciones dictados por los distintos sujetos obligados, con relación a las solicitudes de acceso a la información que les sean presentadas.

De conformidad con la LTAIPDF, el INFODF debe velar porque en sus resoluciones imperen los principios de certeza, legalidad, independencia, imparcialidad y objetividad.

Otra de las funciones que la ley encomienda al Instituto, es la de organizar seminarios, cursos, talleres y demás actividades que promuevan el conocimiento de la LTAIPDF y las prerrogativas de las personas en cuanto al Derecho de Acceso a la Información Pública. Esta es una tarea de suma importancia para la consolidación de este derecho, ya que implica la promoción, entre las personas y los servidores públicos, de un cambio en la manera de entender las relaciones entre gobierno y gobernados, lo que implica el reconocimiento de la información como un bien público, accesible a todos, y la obligación de conceder su acceso únicamente con las restricciones legales que eventualmente existan.

Con el propósito de crear una cultura de la transparencia y acceso a la información pública entre los habitantes del Distrito Federal, el Instituto debe promover, en colaboración con instituciones educativas y culturales del sector público o privado, actividades, mesas de trabajo, exposiciones y concursos relativos a la transparencia y acceso a la información en el Distrito Federal.

De igual forma, el INFODF propondrá, a las autoridades educativas, la inclusión de contenidos sobre la importancia social del Derecho de Acceso a la Información Pública en los planes y programas de estudio de educación preescolar, primaria, secundaria, normal y para la formación de maestros de educación básica que se impartan en el Distrito Federal. De igual manera, la Ley dispone, en su artículo 35, que el Instituto de Educación Media Superior del Distrito Federal procurará incluir, en sus planes y programas de estudio y en sus actividades extracurriculares, los temas de acceso a la información pública, transparencia y rendición de cuentas.

El Instituto también debe incidir en la promoción del desarrollo de acciones

inéditas en los Entes Obligados, que constituyan una modificación creativa, novedosa y proactiva de los procesos de transparencia y acceso a la información. Una de las formas para lograr dichos objetivos se lleva a cabo en el Certamen Innovaciones en Materia de Transparencia, el cual permite desarrollar políticas novedosas a favor de la ciudadanía y fortalecer los mecanismos de transparencia.

En relación con la vigilancia y evaluación del cumplimiento de las disposiciones de la LTAIPDF por parte de los Entes Obligados, el INFODF tiene la facultad de diseñar y aplicar indicadores para determinar el desempeño que se observa en la materia; estos indicadores se nutren de la información que los mismos entes deben entregar al INFODF respecto del ejercicio del Derecho de Acceso a la Información Pública y de los Derechos ARCO. De la misma manera, la Ley dispone que el Instituto debe publicar anualmente los índices de cumplimiento de la LTAIPDF por parte de los Entes Obligados; así, el ejercicio de evaluación que hace el Instituto se socializa, dejando al escrutinio público los resultados de cada uno de los Entes Obligados en el cumplimiento de la Ley.

Otra de las atribuciones del INFODF, es la de promover que los Entes Obligados desarrollen portales temáticos sobre asuntos de interés público. Al respecto, el Instituto ha dado impulso a la generación de portales de Transparencia Focalizada o de Transparencia Ciudadana, en los que se incluyen temas específicos de interés de la ciudadanía en formatos comprensibles, sencillos y de fácil acceso, orientados a responder al interés y a las demandas de información de la gente.

Resumen

El INFODF es el órgano que dirige y vigila el cumplimiento de la LTAIPDF, la LPDPDF y las normas que de ellas deriven.

Es un órgano autónomo del Distrito Federal, dotado de personalidad jurídica y patrimonio propios, así como de autonomía presupuestaria, de operación y de decisión en materia de transparencia y acceso a la información pública; por lo tanto, cuenta con facultades suficientes para cumplir y hacer cumplir las Leyes sobre sí mismo y sobre los demás Entes Obligados.

Dentro de sus atribuciones se encuentran las siguientes:

- Resolver los recursos de revisión.
- Organizar seminarios, cursos, talleres y demás actividades que promuevan el conocimiento de la LTAIPDF y las prerrogativas de las personas en cuanto al Derecho de Acceso a la Información Pública.

- Promover la cultura de la transparencia y acceso a la información pública entre los habitantes del Distrito Federal.
- Promover el desarrollo de portales temáticos sobre asuntos de interés público.

7. De los medios de impugnación

La LTAIPDF establece procedimientos para la defensa del Derecho de Acceso a la Información, en los que sin duda prevalecen los principios de rapidez y sencillez. Dentro de estos procedimientos se encuentran:

- La denuncia.
- El recurso de revisión.
- El recurso de revocación.

7.1 De la denuncia

7.1.1 Por falta de publicación de información considerada como pública de oficio

De conformidad con el artículo 32 de la LTAIPDF, cualquier persona podrá denunciar ante el INFODF el incumplimiento a la publicación de la información definida como pública de oficio en el Capítulo II del Título Primero de la LTAIPDF.

Al recibirse la denuncia, el INFODF la revisará a efecto de determinar su procedencia. En un plazo no mayor a veinte días hábiles, contados a partir de su recepción, el Instituto emitirá una resolución en la que ordene al ente tomar las medidas que resulten necesarias para garantizar la publicidad de la información.

El proceso de atención de denuncias se encuentra previsto en el Procedimiento para la atención de las denuncias de un posible incumplimiento a las disposiciones establecidas en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

7.1.2 Por incumplimiento a las disposiciones contenidas en la LTAIPDF

De conformidad con el artículo 71, fracción XLIII, de la LTAIPDF, el INFODF tiene la atribución de conocer aquellas denuncias que sean presentadas por hechos que puedan constituir infracciones a la propia Ley y demás disposiciones de la materia.

Para la atención de dichas denuncias, se seguirá lo previsto en el Procedimiento para la atención de las denuncias de un posible incumplimiento a las disposiciones establecidas en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, expedido por el INFODF.

7.2 Recurso de Revisión: Un medio de defensa del Derecho de Acceso a la Información Pública

El recurso de revisión es un medio de defensa que tienen las personas para impugnar las respuestas que les son notificadas en atención a sus solicitudes de acceso a la información. El recurso de revisión es una garantía para que las personas hagan efectivo su Derecho de Acceso a la Información Pública en la Ciudad de México.

El fundamento legal del recurso de revisión se encuentra en el artículo 76 de la LTAIPDF.

Durante el procedimiento de atención del recurso de revisión, el INFODF deberá aplicar la suplencia de la deficiencia de la queja a favor del recurrente.

A fin de contar con mayores elementos al momento de emitir la resolución, el Instituto tendrá acceso a la información reservada o confidencial cuando resulte indispensable para resolver el recurso, la cual deberá ser mantenida con tal carácter y no estar disponible en el expediente, lo que también aplica para aquella información que hubiere sido ofrecida por alguna de las partes.

7.2.1 ¿Quién puede interponer un recurso de revisión?

Cualquier persona por sí misma o a través de su representante legal, que haya presentado una solicitud de acceso a información pública ante cualquier Ente Obligado.

7.2.2 ¿Cuándo procede el recurso de revisión?

El recurso de revisión procede cuando los Entes Obligados (artículo 77):

- Nieguen el acceso a la información.
- Declaren la inexistencia de información.
- Clasifiquen la información como reservada o confidencial.
- Entreguen información distinta a la solicitada.
- Entreguen información en un formato incomprensible.

- Entreguen información incompleta o que no corresponda a la solicitud.
- Nieguen el acceso a la consulta directa de la información.

También procede por inconformidad de los solicitantes con los costos, tiempos de entrega y contenido de la información, así como cuando el solicitante estime que la respuesta del Ente Obligado es antijurídica o carente de fundamentación y motivación y por falta de respuesta en el plazo legalmente establecido.

7.2.3 ¿Cuántos días se tienen para interponer un recurso de revisión?

El recurso de revisión debe presentarse dentro de los 15 días hábiles siguientes a que surta efectos la notificación de la respuesta que se impugna.

Para el caso de la falta de respuesta, el plazo contará a partir del momento en que haya transcurrido el término para dar respuesta a la solicitud (5 días tratándose de información pública de oficio, 10 días si se requiere información de naturaleza pública y 20 días en el supuesto de que se amplíe el plazo de respuesta).

7.2.4 ¿Qué instancia resuelve los recursos de revisión?

La autoridad encargada de resolver los recursos de revisión es el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

7.2.5 ¿Cuántos días tiene el INFODF para resolver?

El INFODF cuenta con 40 días hábiles para emitir una resolución, contados a partir del día siguiente de su admisión. En casos excepcionales, dicho plazo puede ampliarse hasta por 10 días más (artículo 80).

En el supuesto de que el ente no haya rendido el Informe de Ley requerido por el INFODF durante la sustanciación del recurso, el plazo para resolver será de 20 días hábiles siguientes al plazo de vencimiento para la presentación del informe (artículo 85).

Para el caso de que el recurso sea interpuesto por la falta de respuesta por parte del Ente Obligado, el plazo para resolver será de 10 días hábiles contados a partir de su admisión (artículo 86).

7.2.6 ¿Cuáles son los requisitos para interponer un recurso de revisión?

Los requisitos se encuentran previstos en el artículo 78 de la LTAIPDF; éstos son:

- Estar dirigido al Instituto.
- El nombre del recurrente y, en su caso, el de su representante legal o mandatario, acompañando el documento que acredite su personalidad.
- El nombre del tercero interesado, si lo hubiere.
- El domicilio o medio electrónico para oír y recibir notificaciones y, en su caso, a quien en su nombre autorice para oírlas y recibirlas; en caso de no haberlo señalado, aun las de carácter personal se harán por estrados.
- Precisar el acto o resolución impugnada y la autoridad responsable de éste.
- Señalar la fecha en que se le notificó el acto o resolución que impugna, excepto en el caso de omisión.
- Mencionar los hechos en que se funde la impugnación, los agravios que le cause el acto o resolución impugnada.
- Acompañar copia de la resolución o acto que se impugna y de la notificación correspondiente. Cuando se trate de solicitudes que no se resolvieron en tiempo, anexar copia de la iniciación del trámite.

Adicionalmente, se podrán anexar las pruebas y demás elementos que se considere hacer del conocimiento del Instituto.

En caso de que el recurrente no cumpla con los requisitos referidos, el INFODF deberá prevenirlo en un plazo no mayor de cinco días hábiles, para que en un plazo igual, contado a partir del día siguiente a que haya surtido efectos la notificación, subsane las irregularidades. En el mismo acto deberá apercibir al recurrente de que si no desahoga la prevención, se tendrá por no interpuesto el recurso de revisión (artículo 79).

7.2.7 ¿Cuáles son los medios para interponer recurso de revisión?

El recurso de revisión podrá ser presentado por escrito libre o a través de los formatos que al efecto proporcione el INFODF, o por medios electrónicos, cumpliendo los requisitos referidos en el punto anterior.

7.2.8 ¿Cuáles son las etapas del procedimiento de recurso de revisión?

La LTAIPDF prevé tres procedimientos para la atención de recursos de revisión, los cuales se encuentran definidos por los plazos de resolución que pueden ser 40, 20 y 10 días, lo que obliga a reducir las etapas del procedimiento:

Procedimiento de 40 días:

- Una vez presentado el recurso, se dictará el acuerdo que corresponda dentro de los tres días hábiles siguientes.

  En caso de admisión, en el mismo auto se ordenará al Ente Obligado que, dentro de los cinco días hábiles siguientes a que surta efectos la notificación, rinda un informe respecto del acto o resolución recurrida, en el que agregue las constancias que le sirvieron de base para la emisión de dicho acto, así como las demás pruebas que considere pertinentes. En caso de no atender dicho requerimiento en tiempo y forma, el plazo de resolución se reducirá a 20 días, sin posibilidad de ser ampliado.

  Si existe un tercero interesado, se le notificará para que en el mismo plazo acredite su carácter, alegue lo que a su derecho convenga y aporte las pruebas pertinentes.

- Recibida la contestación al requerimiento referido en el párrafo anterior, el Instituto dará vista al recurrente para que, en un término de cinco días hábiles siguientes a que surta efectos la notificación, se pronuncie respecto a dicho informe y presente las pruebas y alegue lo que a su derecho convenga.

  Las partes podrán ofrecer todo tipo de pruebas, con excepción de la confesional de los Entes Obligados y aquellas que sean contrarias a derecho.

- En caso de que alguna de las parte hubiere ofrecido medio de convicción que no se desahogue por su propia y especial naturaleza, se señalará fecha de audiencia pública para su desahogo dentro de los tres días siguientes a que se recibieron. Una vez desahogadas las pruebas, se declarará cerrada la instrucción y el expediente pasará a resolución.

- El INFODF en su caso, podrá avenir a las partes con la finalidad de evitar pasos dilatorios en la entrega de la información.

- Durante el procedimiento, el Instituto deberá asegurarse de que las partes puedan presentar, de manera oral, escrita o electrónica, los argumentos que funden y motiven sus pretensiones, así como formular sus alegatos.

- De manera excepcional, el INFODF podrá ampliar el plazo de resolución del recurso de revisión hasta por 10 días.

Procedimiento de 20 días (artículo 85):

Ante la omisión del ente recurrido en remitir, en tiempo y forma, el informe que le sea requerido por el INFODF durante la sustanciación del recurso de revisión, el plazo para resolver el recurso será de 20 días hábiles, contados a partir de que feneció el plazo de cinco días conferido al ente para rendir dicho informe.

Una vez que se determine el incumplimiento, el instituto declarará cerrado el periodo de instrucción y ordenará la elaboración del proyecto de resolución que corresponda.

La omisión referida hace presumir como ciertos los hechos que se hubieren señalado en él, siempre que éstos le sean directamente imputables.

Procedimiento de 10 días (artículo 86):

Éste procede cuando el recurso de revisión es interpuesto por falta de respuesta. En este supuesto, el Instituto dará vista al ente recurrido, al día siguiente de tener por recibido el recurso de revisión, para que alegue lo que a su derecho convenga en un plazo no mayor a tres días.

Una vez remitido el informe referido en el párrafo anterior, el Instituto declarará el cierre del periodo de instrucción y ordenará la elaboración del proyecto de resolución en un plazo no mayor a diez días.

La resolución que se emita deberá ser favorable al solicitante, salvo que el Ente Obligado pruebe que respondió, en tiempo y forma, la solicitud o que exponga de manera fundada y motivada que se trata de información reservada o confidencial.

7.2.9 ¿Cómo puede resolver el INFODF el procedimiento de recurso de revisión?

Durante el desahogo, tramitación y resolución del recurso de revisión, el INFODF podrá:

- Desechar el recurso de revisión por improcedente.
- Sobreseer el recurso.
- Confirmar el acto o resolución impugnada.
- Revocar o modificar la respuesta.
- Ordenar la emisión de una respuesta y ordenar la entrega de la información.

7.2.10 ¿Cuándo procede el desechamiento de un recurso de revisión por improcedente?

El artículo 83 establece las hipótesis en las que procede el desechamiento de los recursos de revisión por improcedentes, la cual se actualiza cuando el INFODF determina que el medio de impugnación no cumple con todos los requisitos legales, que son insubsanables.

Procede el desechamiento del recurso de revisión por improcedente cuando:

- Sea presentado de manera extemporánea (una vez transcurrido el plazo de 15 días para su interposición).
- El Instituto anteriormente haya resuelto en definitiva sobre la materia de éste.
- Se recurra una resolución que no haya sido emitida por el ente recurrido.
- Se esté tramitando algún procedimiento en forma de juicio ante la autoridad competente, promovido por el recurrente en contra del mismo acto o resolución.
- Se interponga contra un acto o resolución con el que haya identidad de partes, pretensiones y actos reclamados, respecto a otro recurso de revisión.

7.2.11 ¿Cuáles son las causas de sobreseimiento del recurso de revisión?

El sobreseimiento del recurso de revisión tiene como efecto poner fin al procedimiento de manera anticipada, sin entrar a fondo al estudio del asunto.

Las causales de sobreseimiento se encuentran previstas en el artículo 84 de la LTAIPDF, que a saber son:

- Por desistimiento expreso del recurrente.
- Porque el recurrente fallezca o, tratándose de personas morales, que ésta se disuelva.
- Porque una vez admitido el recurso de revisión, se actualice alguna causal de improcedencia en los términos previstos en la LTAIPDF o la normatividad supletoria.
- Porque el Ente Obligado cumpla con el requerimiento de la solicitud,

caso en el que deberá haber constancia de la notificación de la respuesta al solicitante; al respecto, el Instituto dará vista al recurrente para que manifieste lo que a su derecho convenga.

- Cuando quede sin materia el recurso.

7.2.12 ¿Qué elementos debe contener la resolución de un recurso de revisión?

La resolución que se emita deberá constar por escrito, señalar los plazos para su cumplimiento y señalar los procedimientos para asegurar su ejecución; asimismo, deberá contener los siguientes aspectos:

- Lugar, fecha en que se emitió, el nombre del recurrente, Ente Obligado y extracto breve de los hechos cuestionados.
- Los preceptos que la fundamenten y las consideraciones que la sustenten.
- Los alcances y efectos de la resolución, fijando con precisión, los órganos obligados a cumplirla.
- La indicación de la existencia de una probable responsabilidad y la solicitud de inicio de la investigación en materia de responsabilidad de servidores públicos.
- En los puntos resolutivos, que podrán ordenar la entrega de la información, confirmar, modificar o revocar la resolución del Ente Obligado.

Las resoluciones deberán ser notificadas a las partes dentro de un plazo de 10 días hábiles posteriores al día de su aprobación por el Pleno del INFODF.

Las resoluciones emitidas por el INFODF son definitivas, inatacables y obligatorias para los sujetos obligados. Esto es, que las resoluciones de los recursos de revisión no pueden ser impugnadas ante ninguna otra instancia, por lo que deben ser cumplidas a cabalidad por los sujetos obligados.

Por otra parte, sólo el recurrente podrá impugnar las resoluciones emitidas por el INFODF mediante juicio de amparo, esto en caso de encontrarse inconforme con la resolución definitiva que emita el Instituto.

7.3 Recurso de Revocación

Otro medio de impugnación con el que cuentan los recurrentes es el recurso de revocación, previsto en el artículo 89 de la LTAIPDF, el cual procede contra

los acuerdos y resoluciones no definitivas pronunciadas en la substanciación del recurso de revisión.

Dicho recurso será sustanciado en los términos que establezca el Reglamento Interior del INFODF, y será resuelto por el Pleno éste.

La tramitación del recurso se sujetará a las siguientes normas:

- Se iniciará mediante escrito material o medio electrónico ante la Dirección Jurídica y Desarrollo Normativo del INFODF, dentro de los tres días hábiles siguientes a que surta efectos la notificación del acuerdo o resolución impugnada.
- El recurso deberá cumplir con los siguientes requisitos:
    - Estar dirigido a la Dirección Jurídica y Desarrollo Normativo del INFODF.
    - Indicar el nombre completo del promovente y domicilio o correo electrónico para oír y recibir notificaciones.
    - Precisar la resolución o acuerdo impugnado.
    - Señalar la fecha en que se notificó la resolución o acuerdo impugnado.
    - Precisar los hechos en que funda el recurso, así como los agravios que le cause la resolución o acuerdo impugnado, acompañando las pruebas que, en su caso, considere pertinentes.

En la sustanciación de este recurso, sólo será admisible la prueba documental y su valoración se hará en los términos que establece el Código de Procedimientos Civiles para el Distrito Federal.

- Dentro de los tres días hábiles siguientes a la recepción del escrito, el INFODF acordará sobre la procedencia del recurso, así como de las pruebas ofrecidas, desechando de plano las que no fuesen idóneas para desvirtuar los hechos en que se basa la resolución.
- Una vez cerrada la instrucción, únicamente se admitirán pruebas supervenientes.
- Desahogadas las pruebas, el INFODF emitirá resolución dentro de los cinco días hábiles siguientes al desahogo y notificará dicha resolución al interesado en un plazo no mayor a tres días hábiles.

Contra la resolución que al efecto emita el Pleno, no procederá recurso alguno.

En caso de que el recurso de revocación no sea procedente en los términos previstos en la LTAIPDF y el Reglamento Interior del INFODF, éste será desechado.

La interposición de este recurso suspenderá los plazos previstos para resolver el recurso de revisión.

Resumen

En este apartado se abordaron los recursos administrativos con los que cuentan los particulares para hacer valer su Derecho de Acceso a la Información.

Uno de ellos es la presentación de denuncias ante el INFODF por presuntas infracciones a la LTAIPDF y demás normatividad aplicable a la materia y por la falta de publicación de información considerada como pública de oficio, las cuales serán tramitadas y sustanciadas por el INFODF conforme al proceso previsto en el Procedimiento para la atención de las denuncias de un posible incumplimiento a las disposiciones establecidas en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Otro medio de impugnación es el recurso de revisión, el cual se interpone ante el INFODF por inconformidad con la atención brindada por los Entes Obligados a las solicitudes de acceso a la información que les son presentadas o por la falta de respuesta a ellas.

La LTAIPDF prevé tres procedimientos para la atención de los recursos de revisión, que inciden en la disminución de los plazos de resolución.

Durante la sustanciación del recurso de revisión los recurrentes cuentan con un medio de impugnación en caso de estar inconformes con los acuerdos que se emitan o resoluciones que no pongan fin al procedimiento denominado recurso de revocación.

8. De las responsabilidades en materia de transparencia y acceso a la información pública

Todos los integrantes de los entes están obligados a dar cabal cumplimiento a lo dispuesto en la LTAIPDF, sin embargo, ante una eventual inobservancia de ésta, el legislador, en cumplimiento a lo mandatado en el artículo 6º Constitucional, incorporó un capítulo en el cual se establece el catálogo de conductas sancionables, dentro de las que se encuentran:

- La omisión o irregularidad en:
    - La publicación o actualización de la información considerada como pública de oficio.
    - La atención a las solicitudes en materia de acceso a la información; esto es, que se deje de observar el procedimiento de acceso a la información.
    - El suministro de la información pública solicitada o en la respuesta a los solicitantes; lo que implica que los Entes Obligados dejan de garantizar plenamente el Derecho de Acceso a la Información de los solicitantes.
    - La observancia de los principios rectores del acceso a la información.
    - La omisión de desclasificar la información como reservada cuando los motivos que dieron origen ya no subsistan.
- La negativa total o parcial en el cumplimiento de las recomendaciones que emita el Instituto.
- La omisión o presentación extemporánea de los informes que solicite el Instituto (por ejemplo, el no remitir en tiempo y forma el informe requerido durante la sustanciación del recurso de revisión).
- La falsificación, daño, sustracción, extravío, alteración, negación, ocultamiento o destrucción de datos, archivos, registros y demás información que posean los sujetos obligados.
- No cumplir con las resoluciones que emita el INFODF, al no proporcionar la información cuya entrega haya sido ordenada.
- Declarar, de manera arbitraria, la inexistencia de información cuando ésta exista total o parcialmente en los archivos del sujeto obligado.
- Negar intencionalmente información no clasificada como reservada o confidencial.
- Clasificar de manera dolosa la información.
- Entregar información clasificada como reservada o confidencial.
- Crear, modificar, destruir o transmitir información confidencial en contravención a los principios establecidos en la Ley.

- Incumplimiento a lo dispuesto en la LTAIPDF.
- Intimidar o inhibir a los solicitantes de información.

En este sentido, cuando el Instituto advierta que algún servidor público pudo haber incurrido en alguna de las conductas referidas en la LTAIPDF, deberá hacer del conocimiento de la autoridad competente (órganos de control) dicha circunstancia, para que realicen la investigación correspondiente y, de ser procedente, se inicie el procedimiento de responsabilidad en los términos de la Ley Federal de Responsabilidades de los Servidores Públicos.

Las infracciones son independientes de las del orden civil o penal que procedan, así como los procedimientos para el resarcimiento del daño ocasionado por un Ente Obligado.

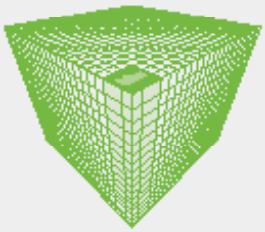
Resumen

La LTAIPDF incorpora un capítulo de responsabilidades en el que se describen los supuestos que constituyen infracciones a la Ley, el Instituto está facultado expresamente para denunciar cualquier conducta que encuadre en los supuestos enunciados en la ley, sin embargo, el eventual fincamiento de responsabilidades se deja en el ámbito del régimen disciplinario establecido en la Ley Federal de Responsabilidades de los Servidores Públicos, a través de los órganos de control correspondientes.

El INFODF carece de la capacidad de sancionar directamente las infracciones que se cometan en materia de transparencia y acceso a la información, sin embargo, lo más importante es que la vigilancia, denuncia y sanción de ellas sean realizadas de manera consistente y eficaz.

infodf

Transparencia y Datos Personales en el Distrito Federal



Capítulo II

Derecho de Protección de Datos Personales

1. Una aproximación a los datos personales en el Distrito Federal

1.1 Introducción

En el transcurso de esta lectura se obtendrá un conocimiento de la evolución de los Derechos Humanos y en específico del Derecho Humano a la Protección de Datos Personales; asimismo, se adquirirán los conocimientos básicos que permitirán distinguir entre este último derecho y el Derecho Humano a la Privacidad, así como los principios que regulan los datos personales en el Distrito Federal y en algunos países de la Unión Europea, Estados Unidos, Canadá y Argentina.

1.2 De los Datos Personales

Los datos personales son elementos informativos relativos a una persona física que lo identifica o lo hace identificable, es decir, son aquellos elementos que le dan una identidad y que le permiten ser identificado entre un colectivo; así mismo, describen elementos delicados, como el origen racial, estado de salud, ideologías (religiosas, políticas, sindicales, etc.).

El procesamiento de los datos facilita la interacción entre los seres humanos y distingue a los individuos de entre los demás integrantes de una sociedad, partiendo, en todo momento, del procesamiento de una u otra forma de esos datos[1]. Sin embargo, en la última década del siglo XX y la primera del siglo XXI, los avances tecnológicos han hecho que el procesamiento o tratamiento de esos datos personales se utilicen de diversas formas, sin que, necesariamente, respondan al fin con el que previamente hayan sido proporcionados.

Con el fin de proteger a los individuos de las consecuencias del tratamiento indebido de los datos personales, desde la década de los 60´s, la Unión Europea ha iniciado una serie de acciones normativas tendientes a la protección de datos personales. Pero antes de realizar el abordaje teórico de ese marco normativo, es necesario partir de un piso mínimo de conocimientos, que nos permita identificar, de manera aproximada, el surgimiento de los Derechos Humanos a la Intimidad, Privacidad y a la Protección de los Datos Personales.

[1] Dicho procesamiento siempre debe responder a un fin determinado, por ejemplo, cuando se otorga a un conocido nuestros datos de localización, tales como la dirección física o electrónica, o el teléfono, su fin es mantener una interacción con esa persona.

1.3 Derechos Humanos y el Derecho a la Protección de Datos Personales

Toda sociedad civilizada parte de un cúmulo de derechos previamente reconocidos, que le dan una organización y subsistencia; la mayoría de ellas actúan bajo estas premisas. Dentro de estos derechos reconocidos, se encuentran los Derechos Humanos; una idea que parte de la Ilustración y que implicó una reforma normativa sustancial, la cual impactó la manera en que los Estados se organizaban, partiendo del reconocimiento de diversos derechos inherentes al ser humano, lo que ha culminado en el cimiento establecido, después de casi 150 años[2], en la Declaración Universal de los Derechos Humanos.

1.3.1 Generación de los Derechos Humanos

A raíz de la Revolución Francesa, se detonó el reconocimiento de diversos Derechos Humanos con sus múltiples formas de clasificarlos; entre ellos, destacan los enfoques: historicista[3], de jerarquía[4] y por generaciones; esta última es la más conocida dentro del mundo y sobre la que se basará el estudio de este apartado.

El enfoque que las "cuatro generaciones" de los Derechos Humanos es el período basado en la evolución de la cobertura de estos.

[2] El germen detonador del reconocimiento de algunos Derechos Humanos fue la Revolución Francesa, en 1789-1799.

[3] El enfoque historicista parte de la protección progresiva de los derechos.

[4] El enfoque basado en la jerarquía distingue entre los Derechos Esenciales y los Derechos Complementarios.

<table>
<tr><td rowspan="2">Primera Generación</td><td colspan="2">Partió de la Revolución Francesa, cuya culminación –en forma independiente a la transformación del concepto de Estado– fue el reconocimiento de los Derechos Civiles y Políticos, tales como la vida, la libertad, la igualdad, derecho al nombre, etc., los cuales buscan la defensa de Libertad, Igualdad y Fraternidad.</td></tr>
<tr><td>Estos derechos son:</td><td>- la vida;
- la integridad física y moral;
- la libertad personal;
- la igualdad ante la ley;
- la libertad de pensamiento, de conciencia y de religión;
- la libertad de movimiento y libertad de tránsito;
- la justicia;
- la nacionalidad;
- participar en la dirección de asuntos políticos;
- poder elegir y ser elegido a cargos públicos;
- formar un partido o afiliarse a uno; y
- participar en elecciones democráticas.</td></tr>
<tr><td rowspan="2">Segunda Generación</td><td colspan="2">Se constituye con los Derechos Económicos, Sociales y Culturales; Derechos Sociales que buscan procurar mejores condiciones de vida. Su característica es que se extienden a la esfera de responsabilidad del Estado, por medio de dos partes: la satisfacción de necesidades y la prestación de servicios.</td></tr>
<tr><td>Estos derechos son:</td><td>- la seguridad social;
- el trabajo;
- igual salario por igual trabajo;
- una remuneración equitativa y satisfactoria que asegure una existencia conforme a la dignidad humana;
- fundar un sindicato y a sindicalizarse;
- al descanso y al tiempo libre;
- un nivel de vida adecuado para la salud y el bienestar (alimentación, vestido, vivienda y asistencia médica);
- seguros en caso de desempleo, enfermedad, invalidez, vejez y otros casos independientes de la propia voluntad;
- la protección de la maternidad y de la infancia;
- la educación;
- la participación en la vida cultural de la comunidad;
- derecho de autor; y
- la inviolabilidad del hogar y comunicados.</td></tr>
</table>

Tercera Generación	Se forman por los Derechos de los Pueblos o de Solidaridad, y surgen a raíz de una necesidad de interacción entre las naciones, así como de los grupos que los integran.	
	Estos derechos son:	- desarrollo integral del ser humano; - progreso y desarrollo económico y social de todos los pueblos; - descolonización, prevención de discriminaciones; - mantenimiento de la paz y la seguridad internacionales; - libre determinación de los pueblos (condición política, desarrollo económico, social y cultural); y - derecho de los pueblos a ejercer soberanía plena sobre sus recursos naturales.
Cuarta Generación	Lo constituyen aquellos derechos de los nuevos actores sociales, y que no se encuentran previamente reconocidos como sujetos sociales. Por ejemplo, el derecho a la autodeterminación informativa, los derechos difusos, el derecho de acceso a la información pública, el derecho a la protección de datos personales (según el punto de vista con el que se aborde este derecho humano, ya que, para algunos estudiosos, su reconocimiento surge a raíz de la quinta generación), etc.	

En otro orden de ideas, podemos observar que, desde la primera generación de los Derechos Humanos y desde un punto de vista filosófico, el Estado que ha surgido a raíz de la Revolución Francesa, empezó a reconocer ciertos elementos que conforman los datos personales, tales como, el nombre, la vida, la ideología, etc., y por ende, el establecimiento de diversos mecanismos estatales para su protección.

De esta manera, se da un reconocimiento autónomo al Derecho Humano a la Protección de Datos Personales, esto debido a los avances tecnológicos y progresos sociales, que han demandan no sólo la protección de éstos, sino también garantías "… para asegurar al gobierno de la persona en sus relaciones con terceros…"[5], lo que busca conocer al individuo en una dimensión social, y que alcanza un significado cuando se tutela a la persona en su condición social, es decir, es un derecho que se disfruta plenamente cuando su titular interactúa con su entorno físico o virtual. Es aquí lo destacado del derecho en comento, ya que no importa la naturaleza íntima del dato, sino la finalidad del tratamiento y las posibles interconexiones de éstos.

Es por lo anterior que se considera que el Derecho Humano a la Protección de Datos Personales surge a raíz de esta generación de los Derechos Humanos, ya que constituye una respuesta jurídica frente a la sociedad de la información.

[5] Herrán Ortiz Ana Isabel, "El derecho a la protección de datos personales en la sociedad de la información", p. 13. Universidad de Deusto, Instituto de Derechos Humanos, Bilbao, España 2003.

1.3.2 Relación de los Derechos a la Intimidad y el Derecho a la Protección de Datos Personales

Como hemos observado en el apartado anterior, el Derecho a la Protección de Datos Personales se encuentra en una dimensión social del ser humano, sin embargo, éste, a pesar de ser social, tiene una dimensión "privada" fuera de esas interconexiones o del tratamiento de sus datos personales o del escrutinio público. Esta dimensión privada es necesaria para su gestación plena como ser humano, por lo que es menester que goce de un área que comprenda diversos aspectos de su vida individual y familiar, que se encuentre libre de las intromisiones generadas por el Estado o la propia sociedad.

La intimidad, esa esfera que se encuentra fuera del escrutinio público, encuentra su base jurídica en la dignidad de las personas; al respecto, el Tribunal Constitucional Español, en la STC 231/1998, señaló:

"… La dignidad de la persona se halla íntimamente vinculada con el libre desarrollo de la personalidad (art. 10) y los derechos a la integridad física y moral (art. 15), a la libertad de ideas y creencias (art. 16), al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1). Es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás…"

Es decir, desde un punto de vista subjetivo, el derecho a la intimidad debe ser entendido como la facultad que tiene el ser humano de conservar una esfera para desenvolver su vida de modo reservado, y que haya vinculado a la tutela su esencia, de tal forma que le permita, bajo su soberanía, su libre desarrollo, y ante violación, solicitar el amparo del Estado[6].

Al respecto el teólogo San Agustín, en su obra "Confesiones", ha señalado que:

"…los que me conocieron antes, ya también de los que no me conocieron, sino que a mí mismo o a otros han oído hablar de mí, aunque ni los unos ni los otros pueden aplicar sus oídos a las voces interiores de mi corazón, donde se halla realmente la verdad de lo que soy…"[7]

Esto quiere decir que el Derecho a la Intimidad implica ser dejado solo, sin intromisión (innecesaria) del exterior, y así lo reconoce la Constitución Política de los Estados Unidos Mexicanos en el primer párrafo del artículo 16, que señala:

[6] Fariñas Montoni, Luis Ma. "El derecho a la intimidad", Madrid, Trivium, 1983. P.327

[7] Consultable en: http://www.iglesiareformada.com/Agustin_Confesiones_Libro_X_Parte1.html

"…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…"[8]

Sobre el particular, la Suprema Corte de Justicia de la Nación ha señalado, en la Tesis Aislada, que el Derecho a la Intimidad es un derecho personalísimo que comprende:

"…el derecho del individuo a no ser conocido por otros en ciertos aspectos de su vida y, por ende, el poder de decisión sobre la publicidad o información de datos relativos a su persona, familia, pensamientos o sentimientos…"[9]
Con los elementos antes abordados, podemos decir, sin duda alguna, que el Derecho a la Intimidad es el derecho que protege la esfera reservada en la que se desenvuelve el individuo. Sin embargo, la reserva inmersa en el concepto previo no es absoluta, ya que cuando se trata de funcionarios públicos o personas públicas, su esfera se ve reducida y deben permitir la interferencia de lo público, al existir un mayor interés de la sociedad de conocer ciertas facetas de su vida. Al respecto, nuestro máximo órgano jurisdiccional ha señalado:

Localización:
Novena Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXXI, Marzo de 2010
Página: 923
Tesis: 1a. XLI/2010
Tesis Aislada
Materia(s): Constitucional

DERECHOS A LA PRIVACIDAD, A LA INTIMIDAD Y AL HONOR. SU PROTECCIÓN ES MENOS EXTENSA EN PERSONAS PÚBLICAS QUE TRATÁNDOSE DE PERSONAS PRIVADAS O PARTICULARES.

[8] Es de señalar que el primer reconocimiento constitucional al derecho a la intimidad que se realizó en el país, deviene de la Constitución Política de los Estados Unidos Mexicanos promulgada en 1857, manteniendo, en esencia, los alcances del Derecho a la Intimidad en la redacción de la Constitución de 1917. La Carta Magna de 1857 señalaba, en su artículo 16, que "… Nadie puede ser molestado en su persona, familia, domicilio, papeles y posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En el caso de delito infraganti, toda persona puede aprehender al delincuente y á sus cómplices, poniéndolos sin demora á disposición de la autoridad inmediata…" (sic).

[9] Véase: EL DERECHO DEL INDIVIDUO A NO SER CONOCIDO POR OTROS EN CIERTOS ASPECTOS DE SU VIDA Y, POR ENDE, EL PODER DE DECISIÓN SOBRE LA PUBLICIDAD O INFORMACIÓN DE DATOS RELATIVOS A SU PERSONA, FAMILIA, PENSAMIENTOS O SENTIMIENTOS, Semanario Judicial de la Federación y su Gaceta XXX, Diciembre de 2009, pág. 7, Tesis: P. LXVII/2009

Las personas públicas o notoriamente conocidas son aquellas que, por circunstancias sociales, familiares, artísticas, deportivas, o bien, porque han difundido hechos y acontecimientos de su vida privada, o cualquier otra situación análoga, tienen proyección o notoriedad en una comunidad y, por ende, se someten voluntariamente al riesgo de que sus actividades o su vida privada sean objeto de mayor difusión, así como a la opinión y crítica de terceros, incluso aquella que pueda ser molesta, incómoda o hiriente. **En estas condiciones, las personas públicas deben resistir mayor nivel de injerencia en su intimidad que las personas privadas o particulares, al existir un interés legítimo por parte de la sociedad de recibir y de los medios de comunicación de difundir información sobre ese personaje público, en aras del libre debate público.** De ahí que la protección a la privacidad o intimidad, e incluso al honor o reputación, es menos extensa en personas públicas que tratándose de personas privadas o particulares, porque aquéllas han aceptado voluntariamente, por el hecho de situarse en la posición que ocupan, exponerse al escrutinio público y recibir, bajo estándares más estrictos, afectación a su reputación o intimidad.

Amparo directo 6/2009. 7 de octubre de 2009. Cinco votos. Ponente: Sergio A. Valls Hernández. Secretarios: Laura García Velasco y José Álvaro Vargas Ornelas.

Sin embargo, esta tarea de delimitar esa línea fina que existen entre lo público y lo privado no es tarea simple, ya que se debe ponderar los Derechos Humanos y la política pública en juego, que a saber son: el Derecho a la Información, el Derecho de Acceso a la Información y la política pública de la Transparencia.

Localización:
Novena Época
Instancia: Primera Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXXI, Marzo de 2010
Página: 928
Tesis: 1a. XLIII/2010
Tesis Aislada
Materia(s): Constitucional

LIBERTAD DE EXPRESIÓN, DERECHO A LA INFORMACIÓN Y A LA INTIMIDAD. PARÁMETROS PARA RESOLVER, MEDIANTE UN EJERCICIO DE PONDERACIÓN, CASOS EN QUE SE ENCUENTREN EN CONFLICTO TALES DERECHOS FUNDAMENTALES, SEA QUE SE TRATE DE PERSONAJES PÚBLICOS O DE PERSONAS PRIVADAS.

La libertad de expresión y el derecho a la información operan en forma diversa tratándose de personajes públicos, quienes, como las personas privadas, se encuentran protegidos constitucionalmente en su intimidad o vida privada, por lo que podrán hacer valer su derecho a la intimidad frente a las opiniones, críticas o informaciones lesivas. La solución de este tipo de conflictos ameritará un ejercicio de ponderación entre los derechos controvertidos, a efecto de determinar cuál de ellos prevalecerá en cada caso. Así, el interés público que tengan los hechos o datos publicados, será el concepto legitimador de las intromisiones en la intimidad, en donde el derecho a la intimidad debe ceder a favor del derecho a comunicar y recibir información, o a la libertad de expresión cuando puedan tener relevancia pública, al ser un ejercicio de dichos derechos la base de una opinión pública libre y abierta en una sociedad. Por consiguiente, en la solución al conflicto entre la libertad de expresión y el derecho a la información, frente al derecho a la intimidad o a la vida privada, deberá considerarse el caso en concreto, a fin de verificar cuál de estos derechos debe prevalecer distinguiéndose, en el caso de personas públicas a la mayor o menor proyección de la persona, dada su propia posición en la comunidad, así como la forma en que ella misma ha modulado el conocimiento público sobre su vida privada.

Amparo directo 6/2009. 7 de octubre de 2009. Cinco votos. Ponente: Sergio A. Valls Hernández. Secretarios: Laura García Velasco y José Álvaro Vargas Ornelas. No podemos soslayar que los derechos antes señalados tampoco son absolutos. Un ejemplo de esto es el artículo séptimo de la Constitución Política de los Estados Unidos Mexicanos, que señala que la libertad de pensamiento tiene como uno de sus límites el respeto a la vida privada; misma limitante se encuentra en la libertad de expresión, contemplada en el artículo sexto de la Carta Magna Mexicana.

Con base en lo anterior, podemos decir que el Derecho a la Intimidad no implica un derecho de exclusión de terceros del ámbito privado de cada persona, por el contrario, señala Ana Isabel Herrerán Ortiz, que este derecho humano "… representa el derecho a controlar y decidir sobre la información y la vida privada que sólo a cada uno concierne…"[10]; y agrega: "… el derecho a la intimidad asegura una calidad mínima de vida en las relaciones con los terceros, de suerte que únicamente se conozca aquello que cada persona debe compartir y revelar a los demás…"[11]; claro está, sin que esto implique que esa persona pierda el control de su información.

En sí, es una libertad fundamental que tienen todas las personas frente a las potenciales agresiones del exterior, y a un tratamiento ilegítimo de su información, la cual posee una dimensión positiva que excede el ámbito de ese derecho fundamental.

[10] Op. Cit. "El derecho a la protección de datos personales en la sociedad de la información", Pág. 12

[11] Ibídem

Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad, con quien comparte el objetivo de ofrecer una eficiente protección de la vida privada y familiar, busca garantizar, a la persona, el otorgamiento de un poder de control sobre sus datos personales, sobre su uso y destino, con el fin último de evitar su tráfico ilegal y dañino a su dignidad. El Derecho Humano a la Intimidad permite excluir determinados datos de una persona del conocimiento de terceros; en cambio, el Derecho Humano a la Protección de Datos Personales garantiza, al particular, un poder de disposición sobre esos datos, lo que podemos traducir en la imposición de deberes jurídicos a terceros.

Por ende, el objeto de este derecho fundamental no se reduce irrestrictamente a los datos íntimos de la personal, sino a cualquier información de tipo personal, sea o no íntimo, cuya exteriorización puede afectar a sus derechos y, por lo tanto, abarca aquellos datos personales públicos, que, por ese simple hecho, no escapan al poder de disposición del afectado, porque así lo garantiza su derecho a la protección de datos.
En pocas palabras, podemos señalar que el contenido del Derecho Humano a la Protección de Datos Personales faculta a la persona para decidir cuáles de sus datos proporciona a un tercero, sea el Estado o a un particular, o cuáles ese tercero puede recabar; asimismo, le permite saber quién posee información de él, y oponerse a su tratamiento.

1.3.3 Habeas Data como una nueva forma de protección al individuo

Los procedimientos de protección constitucional de los derechos humanos o fundamentales tienen una gran historia en el mundo del derecho. Un ejemplo es el juicio de amparo o habeas corpus, que data de la edad medieval en Inglaterra, e implicaba que una persona privada de su libertad fuera presentada ante un tribunal para que éste determinará si la detención era legal o no. Pero como bien sabemos, el campo de acción del Habeas Corpus es mucho más amplio y abarca a todos los derechos humanos reconocidos al individuo; sin embargo, en algunos países, cuando nos enfrentamos a una violación al Derecho Humano a la Información, al Acceso a la Información, a la Intimidad, a la Personalidad, y a la Protección de Datos Personales, la acción constitucional de amparo recibe el nombre de Habeas Data, cuyo origen es relativamente nuevo y ciertos de sus elementos pueden ser rastreados en Europa, en específico, en el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.
El fin último del citado Convenio, es:

"… garantizar […] 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»)…"[12]

Agrega la Convención 108, que los Estados parte deben establecer mecanismos internos que garanticen recursos contra las infracciones a los principios del Derecho a la Protección de Datos Personales conferidos en está[13].

Al respecto, Osvaldo Gozaíni ha señalado que esta herramienta procesal constitucional no sólo protege el derecho a la intimidad, sino también el derecho a la privacidad, a la dignidad humana, a la información, al honor, a la propia imagen, a la identidad o la autodeterminación informativa[14]. Tomando como referencia lo anterior, podemos observar que el Habeas Data parte de diversos derechos personales, por lo que es complicado resumir, en una palabra, el bien jurídico tutelado y los derechos que el Habeas Data cubre.

Sin duda alguna, a pesar de su amplio espectro, podemos señalar que el Habeas Data es un recurso constitucional que garantiza a las personas, la restitución de sus Derechos Humanos a la Intimidad, Protección de Datos Personales y/o de Información que han sido violentados o amenazados por el Estado o particular, es decir, es una garantía que finca la protección de cualquier tipo de dato personal, íntimo o no, público o privado, ya sea que su información tenga o no repercusión en los derechos al honor y a la intimidad de las personas. Y en esto radica su finalidad, en instituir –en aquellos países que lo tienen reconocido constitucionalmente- la garantía a favor del particular que se puede ver afectado por el tratamiento de sus datos, lo que se traduce en la posibilidad de que éste pueda ejercer determinados controles sobre dichos datos[15], materializado en una acción constitucional expedita.
Al respecto, la Corte Suprema de Justicia de la Nación de la República Argentina señaló que la "… ausencia de normas regulatorias de los aspectos instrumentales de la acción de hábeas data no es óbice para su ejercicio, incumbiendo a los órganos jurisdiccionales determinar provisoriamente […], las características con que tal derecho habrá de desarrollarse en los casos concretos…"[16], y agrega que el Hábeas Data también contempla el Derecho a la Verdad, al señalar que es una:

[12] Artículo 1 del Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

[13] En específico, el artículo 10. Sanciones y recursos, del Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la protección automatizada de datos de carácter personal, señala: "… 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 presente capítulo".

[14] Gozaíni, Osvaldo, "La defensa de la identidad y de los datos personales a través del habeas data", Ediar, Buenos Aires, 2001, pág. 7

[15] Peyrano, Guillermo F. "Régimen Legal de los Datos Personales y el Hábeas Data", LexisNexis, Depalma, Buenos Aires, Argentina, 2002, pág. 285.

[16] Suprema Corte de Justicia de la Nación de la República de Argentina, Urteaga, Facundo R. c. Estado Mayor Conjunto de las Fuerzas Armadas, (CSJN.15/10/1998, 1999-I-22).

"… garantía […] –dirigida a que el particular interesado tenga la posibilidad de controlar la veracidad de la información y el uso que de ella se haga–, forma parte de la vida privada y se trata, como el honor y la propia imagen, de uno de los bienes que integran la personalidad…"[17].

En ese mismo orden de ideas, la Corte Constitucional de Colombia, en la sentencia C 1011/08, señaló que el Hábeas Data es:

"Aquel que otorga la facultad al titular de datos personales de exigir de las administradoras de esos datos el acceso, inclusión, exclusión, corrección, adición, actualización y certificación de los datos, así como la limitación en las posibilidades de divulgación, publicación o cesión de los mismos, de conformidad con los principios que regulan el proceso de administración de datos personales".

Recapitulando, el Habeas Data se orienta a la protección de la intimidad, el cual debe ser entendido como el resguardo del derecho básico protegido en la Constitución del Estado, con el fin de garantizar el control activo al titular de los datos y que pueda tener el desarme informativo del Estado o del particular, para decidir acerca del destino y contenido de sus datos.

No omitimos señalar que, en México, no se ha desarrollado o reglamentado este tipo de procedimiento constitucional, y ante una posible violación a lo establecido en los artículos 6º, fracciones II y III, y 16 (segundo párrafo) de la Constitución Política de los Estados Unidos Mexicanos, el afectado deberá acudir, vía el Juicio de Amparo, a solicitar la protección del Estado Constitucional, sin que esto quiera decir que no contemos con una o más leyes dedicadas al tema de protección de datos personales, tales como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, o la Ley de Protección de Datos Personales del Distrito Federal, o algunas leyes que cuyo objeto de regulación principal es el Derecho Humano al Acceso a la Información Pública, pero contemplan un apartado al tema; un ejemplo claro de esto, es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

1.4 La evolución internacional del Derecho a la Protección de Datos Personales

Los avances tecnológicos constituyen un gran poder, puesto que eliminan las barreras del espacio y el tiempo y se constituyen en un elemento útil para el acopio y uso de todo tipo de información. Así mismo, han puesto en tensión constante al Derecho Humano a la Privacidad y, por ende, al Derecho a la

[17] Op.cit.

Protección de Datos Personales, por lo que se ha buscado, desde la segunda generación de los Derechos Humanos, la protección constante del primer derecho señalado.

De tal suerte que esos esfuerzos se han materializado diversos instrumentos internacionales, por ejemplo, la Declaración Universal de los Derechos Humanos o la Convención Europea de Derechos Humanos (adoptada por el Consejo Europeo en 1950), que en el artículo 8 señala:

"1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

"2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás" (sic).

Como podemos observar, dicho artículo considera al derecho a la intimidad en su aspecto estático, e impone una obligación de no hacer al Estado; sin embargo, como hemos observado en líneas anteriores, los avances tecnológicos ponen en riesgo otros aspectos del Derecho a la Intimidad, como pueden ser los datos personales.

1.4.1 Unión Europea

En 1967, el Consejo de Europa constituyó la Comisión Consultiva para estudiar las tecnologías de la información y su potencial vulneración a los derechos de la persona. Ello dio como resultado la Resolución 509 de 1968 sobre los derechos humanos y los nuevos logros científicos y técnicos, lo que sería conocido más tarde como protección de datos[18].
Dicha resolución fue un detonador de diversas leyes específicas, una de ellas, la Ley alemana de octubre de 1970, que tutela los datos personales en posesión de los entes públicos, o la Ley sueca de 1973, o la francesa que data de 1978.

Este esfuerzo del Consejo Europeo y de algunos países del viejo continente se ve materializado en el primer instrumento regional que regula el tema de protección de datos personales, que fue el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento

[18] García González, Aristeo. "La protección de datos personales: Derecho Fundamental del Siglo XXI. Un estudio comparado". Boletín Mexicano de Derecho Comparado, consultable en: http://www.juridicas.unam.mx/publica/rev/boletin/cont/120/art/art3.htm

automatizado de datos de carácter personal, del 28 de enero de 1981, el cual, fue desarrollado a partir del aumento -que se empezaba a gestar- de la circulación transfronteriza de los datos personales automatizados. Lo anterior, fue reforzado en el fin y objeto de dicho instrumento, al señalar:

"El fin del presente 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»)"[19]

La importancia del instrumento en comento no se circunscribe exclusivamente en regular ese flujo transfronterizo, sino en las obligaciones que de él derivan; una de ellas, la localizamos en el artículo 4, el cual señala que los Estados que signen este instrumento, deben adoptar en su régimen interno, las "… medidas necesarias para que sean efectivos los principios básicos para la protección de datos…".

Uno de los principios que destaca dentro del Convenio es el de "Calidad de los datos". El artículo 5 señala que para cumplir dicho principio es necesario que los datos personales:

"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".

Otro de los principios contemplados se localiza en el artículo 7, relativo al de seguridad:

"… Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra

[19] Artículo 1. Objeto y Fin. Convenio 108 del Consejo de Europa.

la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados".

Asimismo, impone la restricción para el tratamiento automatizado de los datos personales relativos al 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, es decir, los datos personales sensibles, al señalar que "… no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas…"[20].

El citado Convenio fue reforzado por medio de la Resolución 45/95 de las Naciones Unidas, adoptada el 14 de diciembre de 1990, que establece los "principios rectores para la reglamentación de los ficheros computadorizados de datos personales", sin embargo, la gran diferencia que existe entre ambos instrumentos internacionales, en forma independiente a los alcances legislativos, es el campo de acción, es decir, mientras que el primero de ellos abarca tanto al sector público como al privado, la Resolución de las Naciones Unidas se centra en los sistemas de datos personales en posesión de "instituciones gubernamentales públicas" (apartado B, no obstante esto, en el preámbulo de esta directriz se señala que los "… procedimientos para llevar a la práctica las normas relativas a los archivos de datos personales informatizados se dejan a la iniciativa de cada Estado…").

Los principios más relevantes recogidos en este instrumento[21] son:

1	**Principio de legalidad y lealtad**	La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.
2	**Principio de exactitud**	Las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que éstos se mantengan de la forma más completa posible, con el fin de evitar errores de omisión, así como de actualizarlos periódicamente o cuando se use la información contenida en un archivo, mientras están siendo procesados.

[20] Artículo 6, Op. Cit.

[21] La Resolución 45/95: Principios rectores aplicables a los ficheros computarizados de datos personales, de la ONU, puede ser consultable en: http://www.informatica-juridica.com/anexos/Principios_rectores_aplicables_ficheros_computarizados_datos_personales_Resolucion_45_95_14_diciembre_Asamblea_General_Naciones_Unidas.asp

3	**Principio de especificación de la finalidad**	La finalidad a la que vaya a servir un archivo y su utilización debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que, posteriormente, sea posible garantizar que: • Todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados; • Ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados; • El periodo durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados.
4	**Principio de acceso de la persona interesada**	Cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costos o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios. Debe preverse un recurso, en caso necesario, ante la autoridad supervisora especificada más abajo en el principio 8. El costo de cualquier rectificación será soportado por la persona responsable del archivo. Es conveniente que las disposiciones relacionadas con este principio se apliquen a todas las personas, sea cual sea su nacionalidad o lugar de residencia.
5	**Principio de no discriminación**	Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el principio 6, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.
6	**Principio de seguridad**	Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.

Un par de años más adelante de que fuera publicada la Resolución 45/95 de las Naciones Unidas, la Unión Europea dio otro paso fundamental en el tema de protección de datos personales; esto sucedió con la Directiva 95/46/CE, "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", que fue adoptada el 24 de octubre de 1995; la cual tiene como objeto establecer un piso mínimo en la Unión Europea para la protección de los datos personales y su libre flujo transfronterizo, y establecer la "guía" para que los Estados miembros armonicen sus disposiciones internas con relación a esa Directiva.

Con referencia al principio de calidad, la Directiva señala, en el artículo 6, que éste se cumplirá cuando 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 científico".

Agrega in fine el citado artículo, que el responsable del tratamiento será el responsable de garantizar que estos elementos sea cumplidos, so pena de que el tratamiento sea considerado como ilícito. No se puede perder de vista que el responsable debe no solamente observar lo señalado en el artículo en comento, sino que también deberá observar lo dispuesto en la Ley aplicable en el Estado.

En forma independiente, también el tratamiento de los datos personales debe

cumplir con el principio de legitimidad, el cual se encuentra regulado en el artículo 7, que señala:

"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 presente Directiva."

En otras palabras, para que se dé cumplimiento al principio de legitimidad es necesario que exista el consentimiento previo, o previsión legal, entendida ésta en un amplio sentido (cumplimiento de una norma o de un contrato), o sea necesario para la salvaguarda de otros derechos o libertades humanas.

Uno de los principios rectores del tema de protección de datos personales, es el de confidencialidad, que implica, en términos del artículo 16, que:

"Las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, incluido este último, sólo 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".

Lo anterior, se traduce en una obligación de no hacer del encargado o responsable del tratamiento, la cual consiste en no tener conocimiento de más datos personales de los que están legítimamente autorizados.

Dicho principio se ve hermanado con el principio de seguridad, el cual se encuentra contemplado en el artículo 17, y señala, entre otros elementos, que:

"… 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 …".

Recientemente, el Grupo de Trabajo Artículo 29[22] busca incorporar a dicha Directiva el principio de responsabilidad, el cual implica:

"… que los responsables del tratamiento de datos garanticen la adopción de medidas eficaces que aporten una auténtica protección de datos…"[23].

Es de resaltar que, este principio no es nuevo en el ámbito del Derecho a la Protección de Datos Personales, ya que la Organización de Cooperación y Desarrollo Económicos, a través de las directrices sobre privacidad adoptadas en 1980, incorporó este principio, y señaló que "… todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios expuestos"[24].

La redacción propuesta por dicho Grupo de Trabajo, es:

"Artículo X – Aplicación de los principios de protección de datos

"**1.** El responsable del tratamiento de datos aplicará medidas adecuadas y eficaces para garantizar el cumplimiento de los principios y obligaciones dispuestos en la Directiva.

"**2.** A instancias de la autoridad de control, el responsable del tratamiento de datos demostrará el cumplimiento del apartado 1."[25]

[22] El Grupo de trabajo del artículo 29 está compuesto por un representante de la autoridad de protección de datos de cada Estado miembro de la UE, el Supervisor Europeo de Protección de Datos y la Comisión Europea.
Sus funciones, las localizamos en el artículo 30 de la Directiva, que señala:
"a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;
"b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad y en los países terceros;
"c) asesorar a la Comisión sobre cualquier proyecto de modificación de la presente Directiva, cualquier proyecto de medidas adicionales o específicas que deban adaptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades;
"d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria"

[23] Dictamen 3/2010 sobre el principio de responsabilidad. Adoptado el 13 de julio de 2010.

[24] Op. Cit., Numeral 16.

[25] Op. Cit., Numeral 34.

Este principio, como podemos observar, busca imponer la obligación a los responsables de:

- Observar e implementar todos los principios generales que derivan de la Directiva.

- Adoptar los niveles de seguridad aplicables a los sistemas de datos personales, con el fin de garantizar la fidelidad y confidencialidad de los datos ahí almacenados.

En otro orden de ideas, otro instrumento de la Unión Europea que marco un hito en el Derecho a la Protección de Datos Personales fue la Directiva 97/66/CE del Parlamento Europeo y del Consejo, del 15 de diciembre de 1997, "relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones"[26], que, como su nombre lo indica, tiene por objeto (artículo 1.1):

"… establece[r] la armonización de las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la libre circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad".

El punto 2 del artículo 1, de la citada Directiva, establece que es un instrumento que complementa la Directiva 95/46/CE, previamente analizada.
Esta Directiva, fue diseñada como un complemento de la Directiva 95/46/CE, por lo que no incorpora per se nuevos principios al tema, sin embargo, es importante resaltar el punto relativo a la confidencialidad de las comunicaciones, que establece la obligación de mantener en secreto las "… comunicaciones realizadas a través de las redes públicas de telecomunicación y de los servicios de telecomunicación accesibles al público…"[27], quedando claro que están permitidas las grabaciones legalmente autorizadas por la autoridad competente para tal efecto.

Ahora bien, el artículo 6.1 de la Directiva 97/66/CE incorporó el principio de temporalidad, al señalar que:

"**1.** […] los datos sobre tráfico relacionados con los usuarios y abonados tratados para establecer comunicaciones y almacenados por el proveedor de

[26] La cual estuvo vigente hasta el 12 de julio de 2002, que fue derogada por la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

[27] Artículo 5.1. Directiva 97/66/CE.

una red o servicio público de telecomunicación deberán destruirse o hacerse anónimos en cuanto termine la comunicación.
"**2.** A los efectos de la facturación de los usuarios y de los pagos de las interconexiones, podrán ser tratados los datos […] únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago…"

Ahora, esta Directiva fue derogada por la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y protección de la intimidad en el sector de las comunicaciones[28]; la cual, en su preámbulo, señala que los avances tecnológicos vividos a partir de la publicación de la Directiva 97/66/CE, hacen necesaria su actualización, a fin de que responda a las necesidades imperantes.

Asimismo, busca proteger no solamente los derechos fundamentales de un ser humano, como el Derecho a la Intimidad, sino también los intereses legítimos de las personas morales; esto en virtud de que los datos tratados en las redes de comunicación electrónicas contienen información relativa a la vida privada de una persona física identificada o identificable, asimismo afecta, de una u otro forma, los intereses legítimos de una persona moral[29]. Por lo anterior, señala la Directiva que el tratamiento de los datos debe mantenerse mientras tanto dure el servicio que se presta, incluyendo el período de facturación y los demás pagos conexos del servicio, por lo que cualquier otro tipo de procesamiento deberá contar con el consentimiento expreso e informado del interesado.
Un apartado importante sobre los sistemas de geolocalización, es desarrollado en esta Directiva, al señalar, en el considerando 35, que:

"En las redes móviles digitales se tratan los datos sobre localización que proporcionan la posición geográfica del equipo terminal del usuario móvil para hacer posible la transmisión de las comunicaciones. Tales datos constituyen datos sobre tráfico a los que es aplicable el artículo 6 de la presente Directiva. Sin embargo, además, las redes móviles digitales pueden tener la capacidad de tratar datos sobre localización más precisos de lo necesario para la transmisión de comunicaciones y que se utilizan para la prestación de servicios de valor añadido tales como los servicios que facilitan información sobre tráfico y orientaciones individualizadas a los conductores. El tratamiento de tales

[28] El artículo 19 de la Directiva 2002/58/CE, señala al respecto:
"…
Se deroga la Directiva 97/66/CE con efecto a partir de la fecha contemplada en el apartado 1 del artículo 17.
"Las referencias a la Directiva derogada se entenderán hechas a la presente Directiva".
El apartado 1 del artículo 17, señala:
"…
Los Estados miembros pondrán en vigor antes del 31 de octubre de 2003 las disposiciones necesarias para dar cumplimiento a lo establecido en la presente Directiva…"
[29] Considerando 26, Directiva 2002/58/CE

datos para la prestación de servicios de valor añadido sólo debe permitirse cuando los abonados hayan dado su consentimiento. Incluso en los casos en que los abonados hayan dado su consentimiento, éstos deben contar con un procedimiento sencillo y gratuito de impedir temporalmente el tratamiento de los datos sobre localización".

El Artículo 6 de la Directiva señala:

"**1.** Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sea necesario a los efectos de la transmisión de una comunicación.

"**2.** Podrán ser tratados los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones. Se autorizará este tratamiento únicamente hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago.

"**3.** El proveedor de un servicio de comunicaciones electrónicas disponible para el público podrá tratar los datos a que se hace referencia en el apartado 1 para la promoción comercial de servicios de comunicaciones electrónicas o para la prestación de servicios con valor añadido en la medida y durante el tiempo necesarios para tales servicios o promoción comercial, siempre y cuando el abonado o usuario al que se refieran los datos haya dado su consentimiento. Los usuarios o abonados dispondrán de la posibilidad de retirar su consentimiento para el tratamiento de los datos de tráfico en cualquier momento.

"**4.** El proveedor del servicio deberá informar al abonado o al usuario de los tipos de datos de tráfico que son tratados y de la duración de este tratamiento a los efectos mencionados en el apartado 2 y, antes de obtener el consentimiento, a los efectos contemplados en el apartado 3.

"**5.** Sólo podrán encargarse del tratamiento de datos de tráfico, de conformidad con los apartados 1, 2, 3 y 4, las personas que actúen bajo la autoridad del proveedor de las redes públicas de comunicaciones o de servicios de comunicaciones electrónicas disponibles al público que se ocupen de la facturación o de la gestión del tráfico, de las solicitudes de información de los clientes, de la detección de fraudes, de la promoción comercial de los servicios de comunicaciones electrónicas o de la prestación de un servicio con valor añadido, y dicho tratamiento deberá limitarse a lo necesario para realizar tales actividades.

"**6.** Los apartados 1, 2, 3 y 5 se aplicarán sin perjuicio de la posibilidad de que los organismos competentes sean informados de los datos de tráfico con arreglo a la legislación aplicable, con vistas a resolver litigios, en particular los relativos a la interconexión o a la facturación"

Ahora bien, al igual que la Directiva 97/66/CE, este instrumento contempla ciertos límites al derecho a la protección de los datos personales o a los intereses legítimos de las personas morales, éstos los encontramos en el artículo 5, que en la parte conducente señala:

"…. En particular, prohibirán [el Estado] la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartido 1 del artículo 15…"

El Artículo 15, apartado 1, señala que:

"**1.** Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones […], cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la Seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución del delito o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE […] Todas las medidas contenidas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario…"

El Artículo 13 de la Directiva señalada establece los límites y excepciones al tema de protección de datos personales, al establecer:

"… ***Artículo 13*** Excepciones y limitaciones
"**1.** Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de:

"a) la seguridad del Estado;

"b) la defensa;

"c) la seguridad pública;

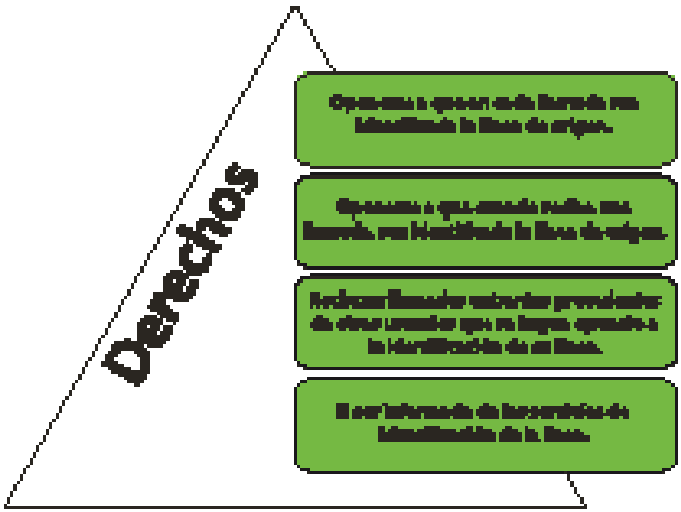
"d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;

"e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;

"f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);

"g) la protección del interesado o de los derechos y libertades de otras personas.

Un punto a resaltar, que es retomado de la Directiva que derogó, es el relativo a la prestación y restricciones de la identificación de la línea[30] de origen, establecido en el artículo 8, y constituye a favor del particular diversos derechos, que a saber son:



Otro punto a destacar, se encuentra localizado en el artículo 13 de la Directiva, que versa sobre comunicaciones no solicitadas. Dicho artículo se centra en el consentimiento del usuario, ya que será él, quien, previa autorización, podrá

[30] No se debe perder de vista que, el número telefónico es un dato personal, susceptible de ser protegido por el paraguas del Derecho a la Protección de Datos Personales.

recibir llamadas automáticas (sin intervención humana), o correos electrónicos publicitarios, cuando, previamente, éste haya adquirido un producto con esa persona, y ésta última sólo podrá enviar correos mercadológicos sobre productos similares. Agrega el citado artículo, que, en caso contrario, se deben establecer mecanismos internos para que el usuario pueda oponerse a esto. Este artículo prohíbe:

"… mensaje electrónico con fines de venta directa en los que disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, o que no tengan una dirección válida a la que el destinatario pueda evitar una petición de que se ponga fin a tales comunicaciones…"
Como podemos observar, el desarrollo normativo e interpretativo de los Derechos Humanos a la Intimidad y a la Protección de Datos Personales en la Unión Europea ha sido amplio desde la década de los 60´s., y es un claro ejemplo de que los Derechos Humanos no son estáticos, y su avance normativo se encuentra supeditado, en gran medida, a los avances tecnológicos que se susciten en la historia de la humanidad.

Antes de concluir este apartado, es conveniente resaltar la importancia de este Derecho Humano para la Unión Europea, ya que, al igual que otras libertades, fue incorporado en el Tratado por el que se establece una Constitución para Europa, en la Parte II, Título II: Libertades, Artículo II-68: Protección de datos de carácter personal, que a la letra señala:

"***Artículo II-68*** Protección de datos de carácter personal

"**1.** Toda persona tiene derecho a la protección de los datos de carácter personal que le 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 obtener su rectificación.

"**3.** El respeto de estas normas estará sujeto al control de una autoridad independiente".

1.4.2 Aspectos generales de las Leyes de: España, Inglaterra,Estados Unidos, Canadá y Argentina

Es importante señalar que, en este apartado, sólo se analizarán algunos aspectos relevantes de las leyes de protección de datos personales o de privacidad, ya que, no se pretende hacer un estudio profundo de lo abordado en ellas.

España

El Derecho Humano a la Protección de Datos Personales en España se encuentra localizado en el artículo 18.4 de su Carta Magna, que establece:
"… La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos…".

La regulación y desarrollo del artículo constitucional antes señalado se encuentra en la Ley Orgánica 15/1999, del 13 de diciembre de 1999, que lleva a cabo el aterrizaje en el ordenamiento jurídico español de la Directiva Comunitaria 95/46/CE. Sin embargo, fue el Tribunal Constitucional español, en la sentencia 254/1993, que señaló que el Derecho a la Protección de Datos Personales es una garantía constitucional que da respuesta a una nueva forma de amenaza –generada por los avances tecnológicos- concreta a la dignidad y a los derechos al honor y a la intimidad. Lo anterior al señalar:

"… En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la libertad de la persona proveniente de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama 'la informática".

Esta resolución del Tribunal Constitucional español, fue perfeccionada en la sentencia 11/1998, al señalar:

"… no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, como ha quedado dicho, sino que además, consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la privacidad según la expresión utilizada en la Exposición de Motivos de la Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos. Trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios…".

Asimismo, el Tribunal señaló, en la sentencia 292/2000, que:

"Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye

a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran.

"… La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad (por todas STC 144/1999, de 22 de julio, FJ 8). En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado".

Ahora bien, estas resoluciones y las Directivas señaladas en el apartado anterior, se ven materializadas en la Ley Orgánica **15/1999, del 13 de diciembre, de Protección de Datos de Carácter Personal** (LOPDP), cuyo objetivo es:

"***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".

La forma de garantizar este Derecho Humano se encuentra inmersa en siete títulos, estructurados de la siguiente forma:

- TÍTULO I. DISPOSICIONES GENERALES (artículos 1 al 3)
- TÍTULO II. PRINCIPIOS DE LA PROTECCIÓN DE DATOS (artículos 4 al 12)
- TÍTULO III. DERECHOS DE LAS PERSONAS (artículos 13 al 19)
- TÍTULO IV. DISPOSICIONES SECTORIALES (artículos 20 al 32)
- TÍTULO V. MOVIMIENTO INTERNACIONAL DE DATOS (artículos 33 y 34)
- TÍTULO VI. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (artículos 35 al 42)
- TÍTULO VII. INFRACCIONES Y SANCIONES (artículos 43 al 49)

Como hemos visto en los apartados anteriores, el eje rector de la protección de datos personales[31] se centra en los principios de la materia; en el caso español éstos son:

El principio de calidad implica que los datos personales sólo podrán ser tratados "… 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…"[32]; es decir, los datos personales: no podrán utilizarse

[31] Para efectos de la LOPDP, un dato personal es "…cualquier información concerniente a personas físicas identificadas o identificables…". Al respecto, la Agencia de Datos de la Comunidad de Madrid ha señalado que estos datos pueden manifestarse "… de diferente manera (numérica, alfabética, gráfica, fotográfica y acústica), y que deben referirse siempre a una persona física identificada o identificable, puede ser muy diversa: nombre y apellidos, correo electrónico, estado civil, número de cuenta bancaria…" [consultable en: http://www.madrid.org/cs/Satellite?cid=1247227036068&language=es&pagename=PortalAPDCM%2FPage%2FPAPD_contenidoFinal]

[32] Artículo 4 de la LOPDP.

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,

para fines incompatibles para los que fueron recolectados y deben ser exactos y responder a la realidad del titular.

El principio de información implica el deber de comunicar de forma expresa, precisa e inequívoca, al titular, sobre el tratamiento de sus datos personales; para tal efecto, la LOPDP establece que, para dar cumplimiento al principio en comento, deberá ser informado:
"…

"**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.

Ahora bien, el consentimiento es el principio que rige el tema, en virtud de que implica la manifestación libre e inequívoca, por la cual el titular de esta información permite el tratamiento de sus datos. Al respecto, el artículo 6 de la LOPDP señala que no se requerirá ese consentimiento cuando:

- Los "… datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias
- 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…"
- El "… tratamiento de los datos tenga por finalidad proteger un interés vital del interesado…"
- 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…"

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.

•

Ahora bien, el principio de seguridad, como se observó en las Directivas analizadas previamente, obliga al responsable y/o encargado a:

"… 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"[33].

El deber de secreto fue analizado en el apartado anterior, bajo la óptica de la confidencialidad, e implica, en los términos del artículo 10 de la LOPDP, que:

"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal estén 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".

Un punto a resaltar dentro de la ley en estudio, es la protección de los datos personales especialmente protegidos, que son aquellos que se encuentran íntimamente relacionados a la raza, salud, la vida sexual, ideología, afiliación, creencias religiosas, filosóficas, políticas o morales, protegidas desde la óptica de diversos instrumentos internacionales, tales como: la Declaración Universal de los Derechos Humanos, que los considera como libertades[34]; su fin último, de la especial protección de esos datos, es evitar actos de discriminación en contra de su persona; está protección estriba en:

- Requerir el consentimiento expreso y por escrito del titular[35] para el tratamiento de sus datos personales.
- Prohibir la creación de sistemas de datos personales, creados exclusivamente para la recolección y tratamiento de estos datos.

La LOPDP establece que los derechos conferidos en este instrumento jurídico

[33] Artículo 9.1 LOPDP.

[34] Véase los artículos 18, 19, 20, 21 de la Declaración Universal de los Derechos Humanos.

[35] El artículo 7.2, párrafo 2, señala que se exceptúa de ese consentimiento aquellos sistemas (o 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". Agrega el artículo 7.6, que se exceptúa también el tratamiento de este tipo de datos personales, cuando "… 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 se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto…", es decir, cuando se encuentre en peligro un bien mayor, que a saber es el de la salud y la vida.

serán velados por la Agencia Española de Protección de Datos Personales, que es "… un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones…"[36]. En materia de las Comunidades Autónomas de España, la vigilancia de estos derechos se encuentra a cargo de organismos locales, que tienen las mismas características señaladas, sin embargo, su campo de acción se limita a los "… ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial…"[37].

Inglaterra

La Ley de Protección de Datos (LPD) de Inglaterra, publicada en 1998, entrando en plena vigencia en 2003, derogó la ley del mismo nombre que se encontraba vigente desde 1984. Esta Ley, en términos del órgano garante (Information Commissioner´s Office [ICO]), responde a los estándares de la Directiva 95/46/CE. Estableciendo las normas para el tratamiento de los datos personales, en posesión del sector público y privado.

Los principios rectores de esta ley inglesa se encuentran en el Anexo I, parte 1, y a saber son:

- Tratamiento justo y legal.
- Los datos personales deben ser obtenidos sólo para uno o varios objetivos específicos y legales, y no podrán ser tratados de manera incompatible con esos objetos.
- Ser exactos y no excesivos para el tratamiento que se persigue.
- Deben estar actualizados.
- Deben estar sujetos a una temporalidad, la cual dependerá del objetivo del tratamiento.
- Procesados de conformidad a los derechos del interesado, y que le son conferidos en la LPD.
- Debe adoptar las medidas técnicas y de organización para evitar el acceso no autorizado o ilegal a los sistemas de datos personales objeto de tratamiento[38].
- Las transferencias internacionales sólo se permitirán cuando el país de

[36] Artículo 35.1. de la LOPDP.

[37] Artículo 41.1 de la LOPDP.

[38] Las medidas de seguridad que se adopten, señala el apartado 2, del Anexo I, dependerán: Del daño que podría causarse por el tratamiento ilícito, o ilegítimo, o la pérdida, o la alteración de los datos personales; asimismo, se deberá tomar en consideración la naturaleza de la información objeto de tratamiento.

destino asegure los niveles de seguridad establecidos por la LPD.
En términos de la Parte II de la LPD, el titular de los datos personales tiene el derecho de acceso, lo cual le permite obtener información sobre datos que se están tratando en los diversos sistemas en posesión del sujeto obligado. Otro de los derechos conferidos al titular, es el de evitar que sus datos personales sean tratados para fines mercadológicos; así mismo, se le reconoce la posibilidad de solicitar la corrección, bloqueo, eliminación y destrucción de sus datos, cuando estos son inexactos o contienen opiniones basadas en esos datos inexactos o erróneos.

Es de llamar la atención el derecho que tiene el particular para oponerse a que un sujeto obligado tome una decisión automatizada (sin la intervención de un ser humano) sobre su persona. Otro derecho que también es conferido, es el relativo a prevenir el procesamiento cuando éste genere un daño considerable e injustificado o angustia al titular.

ICO es el órgano garante inglés del tema de protección de datos personales y la libertad de información; y cuenta con las siguientes atribuciones, en los términos del Apartado VI de la LPD:

- Promover el buen manejo de información.
- Difundir información sobre protección de datos.
- Crear o aprobar códigos de práctica para los controladores de datos.
- Presentar notificaciones sobre información: solicitando que un controlador de datos facilite información específica a la Oficina del Comisionado de Información en un plazo de tiempo determinado.
- Realizar evaluaciones de cumplimiento.
- Presentar notificaciones de ejecución cuando se haya producido una violación que requiera que un controlador de datos tome medidas específicas o deje de tomar medidas específicas para cumplir con la LPD.
- Enjuiciar a quienes hayan violentado las disposiciones de la LPD.

Estados Unidos

A diferencia de España o Inglaterra, Estados Unidos de América no contempla bajo una misma ley de privacidad o de protección de datos personales al sector público y al sector privado, por lo que, en este apartado, analizaremos la Ley de Privacidad de 1974 (Sector Público) y Fair Information Practice y Safe Harbor (sector privado), que son algunas de las normas que regulan el tema de protección de datos en ese país.

Sector público

La Ley de Privacidad de 1974 (PA74) (Privacy Act of 1974, USC 552ª) establece una serie de prácticas que regulan la recolección, mantenimiento, uso y difusión de los datos personales que se encuentran en posesión de las entidades gubernamentales federales, estableciendo que éstas no podrán recolectar ningún tipo de dato si el sistema de datos no se encuentra inscrito en el Sistema de Registro, el cual es definido en el 552a (a)(5), que señala el grupo de cualquier registro bajo el control de cualquier agencia federal, la cual es recuperada por el nombre de la persona o por algún número de identificación, o cualquier otro dato de identificación asignado a una persona[39]. El registro de dicho sistema deberá ser hecho del conocimiento del particular, señalándole:

- El nombre y ubicación del sistema.
- La categoría de datos que se recaban.
- La categoría de los registros.
- Los accesos diarios a los sistemas.
- Las políticas y prácticas de la agencia respecto al almacenamiento, recuperación, controles de acceso, retención y eliminación de los registros.
- El nombre y dirección de la agencia gubernamental.
- Los procedimientos por los cuales el titular de los datos personales puede hacer una solicitud de acceso y los medios de notificación.

Un ejemplo de la forma en que es presentado al público en general el sistema en comento es[40]:
La PA74, al igual que las demás leyes que regulan el Derecho Humano a la Protección de Datos Personales, establece la prohibición de revelar la información relativa a una persona, cuando no se cuente con el consentimiento expreso para ello, salvo que se encuentre previsto en algunas de las causales de excepciones establecidas en la ley, las cuales están contenidas en 552a (b), partes 1 a 12, que a saber son:

- A los servidores públicos que dan mantenimiento al sistema de datos.

[39] La obligación de inscripción tiene algunas excepciones, las que se encuentran establecidas en el punto 28, parte 16, subparte E.

[40] Consultable en: http://www.justice.gov/opcl/privacyact.html#DOJ

- Uso cotidiano de la agencia gubernamental.
- Sea requerido por la Agencia del Censo para fines de planificación o llevar a cabo el censo o encuestas o actividades conexas al censo.
- A un tercero, cuando se cuente con el consentimiento para tal efecto.
- Al Archivo Nacional y Administración de Documentos, cuando el registro tenga valor histórico.
- Cuando se encuentre en riesgo la salud o vida del interesado.
- Al Poder Legislativo.
- Cuando exista un mandato judicial.

Algunas de las obligaciones que establece la PA74, a cargo de los sujetos obligados son:

- Recabar los datos, cuando éstos sean necesarios para la ejecución de sus atribuciones.
- La recolección de los datos, en la medida de lo posible, debe ser directamente del interesado.
- Mantener los registros de manera exacta y que respondan a la realidad del titular de esos datos.
- No recolectar, en la medida de lo posible, aquellos datos personales considerados como sensibles.
- Notificar al interesado, cuando sus datos personales sean tratados por otros[41], y éstos adquieran una relevancia de interés público.
- Establecer códigos de conducta para los involucrados en el diseño, desarrollo, operación o mantenimiento de cualquier sistema de registros, o en el mantenimiento de cualquier registro, e instruir a cada persona con respecto a las normas, requisitos y sanciones establecidos en la ley.
- Las promulgaciones de reglas, por las cuales se establezcan:
    - Los mecanismos por los cuales se llevarán a cabo las notificaciones a los interesados, cuando éste ejercite el Derecho de Acceso a Datos

[41] No se puede perder de vista que los datos personales que obran en un sistema de datos personales, pueden ser transferidos por un mandato judicial o entre agencias, sin que medie consentimiento expreso del afectado.

DEPARTMENT OF JUSTICE (DOJ)
* Last publication of complete notice

SYSTEM	TITLE	DATE PUBLISHED	FEDERAL REGISTER
DOJ-001	Accounting Systems for, the Department of Justice	06-03-04* 1-3-2006 1-25-2007 3-22-2010	69 FR 31406* 71 FR 142 72 FR 3410 75 FR 13575
DOJ-002	DOJ Computer Systems Activity & Access Records	12-30-99* 1-31-2001 1-25-2007	64 FR 73585* 66 FR 8425 72 FR 3410
DOJ-003	Correspondence Management Systems for the Department of Justice; Corrections	06-04-01* 6-29-2001 10-25-2002 1-25-2007	66 FR 29992* 66 FR 34743 67 FR 65598 72 FR 3410
DOJ-004	Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Requests and Administrative Appeals; Corrections	06-04-01* 6-29-2001 1-25-2007	66 FR 29994* 66 FR 34743 72 FR 3410
DOJ-005	Nationwide Joint Automated Booking System (JABS)	09-07-06* 1-25-2007	71 FR 52821* 72 FR 3410
DOJ-006	Personnel Investigation and Security Clearance Records for the Department of Justice	09-24-02* 11-10-2004 1-25-2007	67 FR 59864* 69 FR 65224 72 FR 3410
DOJ-007	Reasonable Accommodations for the Department of Justice	05-16-02* 1-25-2007	67 FR 34955* 72 FR 3410
DOJ-008	Department of Justice Grievance Records	10-29-03* 8-4-2004 1-25-2007	68 FR 61696* 69 FR 47179 72 FR 3410
DOJ-009	Emergency Contact Systems for the Department of Justice	01-12-04* 1-25-2007	69 FR 1762* 72 FR 3410
DOJ-010	Leave Sharing Systems	04-26-04* 8-4-2004 1-25-2007	69 FR 22557* 69 FR 47179 72 FR 3410
DOJ-011	Access Control System (ACS)	12-03-04* 1-25-2007	69 FR 70279* 72 FR 3410
DOJ-012	Department of Justice Regional Data Exchange System (RDEX)	07-11-05* 12-2-2005 1-25-2007 1-31-2007	70 FR 39790* 70 FR 72315 72 FR 3410 72 FR 4532
DOJ-013	Justice Federal Docket Management System [Justice FDMS]	3-15-2007	72 FR 12196
DOJ-014	Department of Justice Employee Directory Systems	11-4-2009	74 FR 57194

Personales.

- Los tiempos en los que se dará respuesta.
- Los procedimientos internos para el desahogo de éste derecho.

Ahora bien, esta ley impone la obligación específica a cada una de las agencias de crear un Comité de Integridad de Datos, el cual debe estar integrado por los servidores públicos que designe el titular de cada agencia. Dicho Comité tiene bajo su cargo la implementación y vigilancia de la PA74, asimismo:

- Deberá revisar, aprobar y mantener todos los acuerdos escritos para la recepción o divulgación de los registros de la agencia.

- Deberá revisar todos los programas en los que la agencia ha participado durante el año, ya sea como fuente de información personal de una agencia u organismo destinatario; además de determinar el cumplimiento con las leyes, reglamentos, directrices y acuerdos de agencia, y evaluar los costos y beneficios de dichos programas.

- Elaborará un informe anual que se presentará al jefe de la agencia y la Oficina de Gerencia y Presupuesto, y se pondrá a disposición del público, previa petición.

- Será la oficina en donde se recibirán las peticiones y proporcionará la información sobre la exactitud, integridad y confiabilidad de los registros utilizados en programas de comparación;

- Será la encargada de la interpretación (administrativa) y orientación de la PA74;

- Revisará el mantenimiento de registros y de las políticas y prácticas para la eliminación de los sistemas.

Sector privado

Estados Unidos de América no cuenta con una legislación específica que regule el tratamiento de datos personales en posesión de los particulares; esto a diferencia de México, que cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Sin embargo, a raíz de su historia legislativa, ha publicado diversas normas sectoriales que, de una u otra forma, regulan el tema. Un ejemplo de éstas son: Children's Online Privacy Protection

Act[42]; Financial Services Modernization Act[43] y Health Insurance Portability and Accountability Act[44], por mencionar algunas. También existen algunas normas o códigos que buscan armonizar las disposiciones norteamericanas con las Directivas (vigentes) emitidas en la Unión Europea; por ejemplo: Safe Harbor, así como Fair Information Practice Principles (FIP´s).

En este subapartado analizaremos someramente estos dos últimos instrumentos: el FIP´s es resultado de diversos esfuerzos para analizar la formas electrónicas en que son recolectados, almacenados y utilizados los datos personales, y el establecimiento de algunas garantías mínimas que se deben adoptar para la protección de éstos, de tal suerte que la Comisión Federal de Comercio de Estados Unidos estableció, por medio de éste instrumento, cinco principios básicos que deben observar las personas que recaban datos de manera electrónica.

Estos principios son:

- Aviso. Este principio o regla implica que el cliente o consumidor debe ser informado de las prácticas o formas en que se utilizarán sus datos; esto, claro está, antes de que los proporcione. El aviso debe contener:

    - La identificación de la empresa que recaba los datos personales.
    - La identificación de la forma en que serán utilizados los datos.
    - La identificación de los destinatarios de los datos personales, es decir, si se contempla la transferencia o no de los datos personales.
    - La naturaleza de los datos personales que son recabados y el fin por el que se obtienen.
    - Si los datos recabados son obligatorios o no, y las consecuencias de otorgarlos.
    - Los niveles de seguridad que serán empleados para asegurar la confidencialidad, integridad y calidad de éstos.

[42] Esta acta o ley, también conocida como COPA, regula la recolección online de datos personales de los menores de 13 años, detallando los elementos que deben contemplar las políticas de privacidad que le son aplicables sitios de internet que se encuentran dirigidos a los menores de edad.

[43] Esta norma también es conocida como Ley Gramm-Leach-Bliley (GLB), que busca aumentar la competencia en la industria de servicios financieros, proporcionando un marco prudencial para la afiliación de los bancos, sociedades de valores, y otros proveedores de servicios financieros, así como el manejo de la privacidad en este sector productivo.

[44] Esta ley, establece algunos mecanismos para garantizar la cobertura de los seguros médicos de los trabajadores y sus familiares, cuando estos pierden su trabajo. Dentro de los diversos apartados que conforma esta norma, también conocida como HIPAA, se encuentra un apartado importante sobre el manejo que deben dar las aseguradoras a los datos personales sus asegurados.

- Elección / Consentimiento. La elección y consentimiento implica dar la posibilidad al titular de los datos personales de decidir la forma en que será utilizada su información, en específico, darle la opción –antes de culminar la recolección de los datos- de la forma en que ulteriormente serán utilizados sus datos personales.

- Acceso / Participación. Implica la posibilidad de que el titular de la información no sólo tenga el acceso a sus datos personales, sino que también pueda verificar si esos datos responden a su realidad.

- Integridad / Seguridad.

    - La integridad de los datos significa la posibilidad que tiene, el que recaba los datos personales, de verificar, en otras bases de datos (confiables), la exactitud de la información que es proporcionada por el titular de éstos.

    - La seguridad de los datos implica las medidas de gestión y las técnicas, adoptadas por la persona que los recaba para proteger los datos personales contra la pérdida, acceso no autorizado, destrucción, uso o divulgación.

    - Las medidas de gestión incluyen disposiciones internas empleadas tendientes a limitar el acceso a los datos y asegurar que las personas con acceso a ellos no los utilicen para fines no autorizados.

    - Las medidas técnicas de seguridad para evitar accesos no autorizados incluyen la encriptación en la transmisión y almacenamiento de datos, los límites en el acceso a través del uso de contraseñas, y el almacenamiento de datos en servidores seguros o los equipos que no son accesibles vía remota.

- Aplicación / Compensación.

    - La aplicación de FIP´s será por medio de la autorregulación, lo que implica que la persona que recolecte los datos personales o asociación (o agrupación) a la que pertenece, adopte ciertas medidas para asegurar el cumplimiento de los anteriores principios; asimismo, se debe contemplar mecanismos de auditorías para verificar el cumplimiento de estos principios y procesos de certificación.

    - La compensación por la reparación de los daños y perjuicios causados por la violación de estos principios, deben estar establecidos en estos mecanismos de autorregulación, y deben ser informados a los titulares de estos[45].

[45] Para mayor información sobre FIP´s, se recomienda visitar la siguiente página: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

Como podemos observar, FIP´s establece principios básicos para asegurar la privacidad de los datos personales que son tratados por las empresas, pero no se puede perder de vista que este instrumento no tiene la fuerza de una legislación o reglamento, y queda en mano de éstos la aplicabilidad de estos principios.

La Directiva 95/46/CE analizada con anterioridad establece, entre otras restricciones, la imposibilidad de que los países miembros (y por ende sus empresas) realicen transferencias de datos personales a países que no cumplen con los estándares fijados por ella, lo que, en cierta medida, limitó el intercambio comercial entre Estados Unidos y la Unión Europea, ya que el país en estudio utiliza un enfoque sectorial, que se basa en una mezcla de legislación, regulación y autorregulación. Mientras que la Unión Europea, como hemos observado, se basa en una legislación integral que requiere, entre otras cosas, la creación de agencias independientes del gobierno de protección de datos, el registro de bases de datos con esos organismos y, en algunos casos, consentimiento previo para procesar los datos personales.

Bajo esa lógica, el Departamento de Comercio de Estados Unidos, en colaboración con la Unión Europea, desarrollaron un punto de equilibrio denominado Safe Harbor (SH) (o puerto seguro), el cual fue aprobado por este último en el 2000, con lo que se buscó impedir una interrupción en el intercambio comercial.

El SH consiste en un proceso de auto-certificación, mediante el cual la persona física o moral se adhiere a las políticas de autorregulación sobre privacidad del SH; o diseña estas políticas de autorregulación que cumplan con los principios contemplados. La certificación se realiza ante el Departamento de Comercio, en donde públicamente acepta su adherencia al SH·

Cual fuere el mecanismo adoptado por la persona física o moral, debe cumplir con los siguientes principios[46]:

- **Aviso:** Las organizaciones deben notificar a las personas acerca de los fines para los que recogen los datos personales y utilizan esa información. Asimismo, se debe proporcionar información acerca de cómo el titular de los datos puede contactar a la organización con cualquier pregunta o queja sobre el tratamiento; el nombre de la entidad que recibirá a través de una transferencia los datos personales, y la forma en que se limitará el uso de estos datos.

- **Elección:** La organización debe dar al individuo la posibilidad de escoger qué información puede ser revelada a un tercero o ser usada para un fin

[46] Los principios pueden ser consultados en su fuente original: http://export.gov/safeharbor/eu/eg_main_018476.asp

distinto por el cual fue otorgada. En el caso de que se recabe información sensible, se deberá dar la opción de manera explícita, al titular de los datos, de oponerse a que sus datos sean transferidos a un tercero, o sean utilizados para un fin distinto por el cual fueron recabados.

- **Transferencia a terceros:** Para divulgar la información a un tercero, las organizaciones deben aplicar los principios de notificación y elección. Cuando una organización desea transferir información a un tercero, puede hacerlo si se asegura de que éste se adhiere a los principios establecidos en SH, o está sujeto a la Directiva. Como alternativa, la organización puede firmar acuerdos por escrito con el tercero, donde éste se compromete a proporcionar, al menos, el mismo nivel de protección aplicado por la organización.

- **Acceso:** El titular de los datos personales debe tener la posibilidad de acceder a su información que se encuentre en posesión de las organizaciones, así como la posibilidad de corregirla o eliminarla cuando ésta no sea exacta, salvo que la carga o el gasto de proporcionar acceso sean desproporcionados con relación a los riesgos para la privacidad del individuo, o cuando los derechos de otras personas se pusieran en riesgo.

- **Seguridad:** Las organizaciones deben tomar las precauciones necesarias para proteger la información personal, la pérdida, mal uso y acceso no autorizado de la divulgación, alteración y destrucción.

- **Integridad de los datos:** La información personal debe ser pertinente a los fines para los que se va a utilizar. Una organización debe tomar medidas razonables para asegurar que los datos sean confiables para su uso previsto, así mismo, deben ser precisos, completos y actuales.

- **Aplicación:** Con el fin de garantizar el cumplimiento de los principios de SH, debe haber: a) mecanismos independientes disponibles y asequibles, para que las quejas de cada titular de los datos y los conflictos que se deriven del tratamiento puedan ser investigados y resueltos y, en su caso, la indemnización concedida en la ley; b) procedimientos para verificar que los compromisos de las empresas que se adhieran a los principios de SH se han llevado a cabo, y c) la obligación de solucionar los problemas que surjan por un incumplimiento de los principios. Las sanciones deben ser lo suficientemente rigurosos para asegurar el cumplimiento por la organización. Organizaciones que no proporcionen cartas de auto-certificación anual, no aparecerán en la lista de los participantes y los beneficios de SH no serán asegurados.

Las organizaciones que cumplan con estos principios y obligaciones, podrán realizar todo tipo de transferencia de datos a la Unión Europea y viceversa.

Canadá

Al igual que México, Canadá cuenta con dos leyes que regulan el tratamiento de los datos personales: la primera de ellas está dirigida al sector gubernamental, denominada como "Privacy Act" (PA83) o Ley de Privacidad, la cual entró en plena vigencia el 1 de julio de 1983, y establece las reglas para el tratamiento de los datos personales que se encuentran en posesión de las agencias gubernamentales; la siguiente norma es la Personal Information and Elecrtonic Documents Act (PIPEDA) o Ley Federal de Información Personal y documentos electrónicos, que rige la recopilación, uso y divulgación de información personal en conexión con actividades comerciales y la información personal sobre los empleados, empresas y negocios. Por lo general, no se aplica a las organizaciones no comerciales o los gobiernos provinciales, los cuales han adoptado algunas legislaciones en la materia.

Siguiendo la lógica del apartado anterior, analizaremos, en una primera instancia, la PA83, y posteriormente la PIPEDA.

Sector Público

La PA83, como se mencionó en párrafos anteriores, tiene como propósito regular los datos personales que se encuentran en posesión del gobierno canadiense y establecer las reglas básicas bajo las cuales se utilizará el derecho de acceso a los datos personales.

Al igual que en el caso de la PA74 de Estados Unidos, las agencias gubernamentales, para recabar los datos personales, deben observar algunas reglas básicas:

- Una agencia gubernamental no puede recabar datos personales si no cuenta con las atribuciones legales para ello.

- La agencia gubernamental que recabe algún dato personal, para fines administrativos públicos, deberá, en la medida de lo posible, recabarlo directamente del titular de esa información.

- La agencia gubernamental deberá informar, al titular de los datos personales, el nombre de la entidad y la finalidad por la que se recaba esa información

- La información deberá ser mantenida en los archivos gubernamentales por el periodo necesario para cumplir el fin por el que se recabó el dato personal.

Ahora bien, los datos personales que se encuentren en su posesión, no podrán ser transmitidos a terceros si la agencia gubernamental no cuenta con el consentimiento para tal efecto, salvo que se trate de alguna de las excepciones contempladas en PA83[47], que a saber son:

- Por mandato de una orden de la Corte o del Fiscal.
- Por mandato de una ley.
- Por un mandamiento dado por alguna comisión de investigación, previamente instalada en los términos de la ley aplicable.
- Cuando sea transmitida entre agencias federales o provinciales.
- A miembros del parlamento.
- Cuando tenga fines estadísticos.

El derecho de acceso a datos personales regulado en PA83 establece la posibilidad de que el titular de los datos personales pueda acceder a cualquier dato personal almacenado en una base de datos en posesión de la agencia gubernamental. En todo caso, el interesado podrá solicitar la corrección de un dato cuando éste considere que es erróneo o existe una omisión, o saber a quién han sido transferidos sus datos personales. En el caso de que no se pueda realizar esa corrección, la agencia gubernamental deberá hacer los asientos o anotaciones marginales que haga constar esa modificación[48].

Las agencias gubernamentales canadienses, a diferencia de las de nuestro vecino del norte, cuentan con un máximo de 13 días para emitir una respuesta, en la que se comunicará al particular si su solicitud fue aceptada o no; y, en el caso de ser positiva, deberá señalar las partes a las que se dará acceso, quedando obligado a entregar esa información en un plazo no mayor a 30 días, contabilizados a partir del día 13. En el supuesto de que la respuesta fuera negativa, deberá indicar si la información requerida existe o no en sus archivos, o si no se puede entregar por estar sujeta a alguna de las causales de excepción prevista en la ley.

Existen, al igual que en el caso del Distrito Federal, diversos mecanismos para la protección de los datos personales; uno de ellos es por medio de la denuncia,

[47] En el caso de que se dé una transferencia, por algunas de las causales señaladas, la agencia gubernamental que realice la transferencia, deberá mantener una copia de la solicitud y de los datos personales que son transferidos; su resguardo, será hasta que prescriban las acciones legales.

[48] Párrafo 12, 2 (b), Privacy Act 1983

que es presentada ante el órgano garante del tema en Canadá (Office of the Privacy Commissioner of Canada), la cual procede ante una negativa de acceso a datos personales, o si el interesado siente que su derecho no ha sido atendido adecuadamente[49], etc.; el otro mecanismo, que es llevado a cabo por ese órgano garante, consiste en la revisión de oficio de los sistemas de datos personales que se encuentran en posesión de las entidades gubernamentales, lo que, en el Distrito Federal, se conoce como las auditorías; también podrá revisar aleatoriamente el cumplimiento de la PA83 por parte de la agencia gubernamental.

Sector privado

La PIPEDA, como se menciono anteriormente, regula la forma en que el sector comercial privado da tratamiento a los datos personales que se encuentren en su posesión. Es de señalar que esta ley, al igual que SH, es una respuesta a los estándares fijados por la Unión Europea en sus directivas. Sin embargo, su implementación fue gradual: en una primera fase (2001) aplicó exclusivamente a las empresas reguladas federalmente (tales como las aerolíneas, bancos, etc.); en el 2002 inició su aplicación para el sector salud; y en el 2004, al resto de las organizaciones que recaban datos personales.

Esta ley establece que los datos personales es toda aquella información sobre una persona identificable, pero no entra dentro de este concepto el nombre comercial, dirección comercial o el total de empleados que tiene esa empresa (Apartado 1, 2). Es de señalarse que esta ley permite el acceso a cualquier registro, que implica, bajo el mismo apartado, toda la correspondencia, memorando, el libro, plan, mapa, dibujo, diagrama, la obra pictórica o gráfica, fotografía, película, microforma, grabación de sonido, video, grabaciones y cualquier otro documento material, independientemente de la forma o características físicas y copia de cualquiera de esas cosas, lo que abre el abanico a una infinidad de posibilidades de almacenamiento de esta información.

La PIPEDA reconoce a los titulares de los datos personales el derecho a:

- Saber qué organización recopila, usa o revela sus datos personales.
- Ser informado sobre el fin del tratamiento, uso y destino de los datos personales recolectados.
- Ser informado sobre los niveles de seguridad empleados para proteger los datos personales.

[49] En el caso de que el particular, después de que se haya emitido la resolución por parte del órgano garante, podrá acudir ante la Corte canadiense.

- Tener mecanismos para asegurar que sus datos sean exactos, completos y actualizados.

- Tener acceso a sus datos personales y a su corrección.

- Tener mecanismos de defensa.

Al igual que la SH, PIPEDA establece ciertas obligaciones a cargo del sujeto obligado, que a saber son:

- Obtener el consentimiento del titular de los datos personales para el procesamiento de éstos.

- Suministro de un servicio o producto, a pesar de que el titular de los datos personales se niegue a proporcionar su consentimiento para el tratamiento de sus datos personales.

- Recolectar los datos personales de manera justa y adecuada, así como mantenerla de manera confidencial.

- Tener políticas para el uso de la información personal, que sean claras y de fácil acceso.

Ahora bien, los mecanismos de defensa son similares a los establecidos en la PA83, estableciendo, en forma independiente, un procedimiento específico de auditoría a los registros mantenidos por las organizaciones.

Argentina

Al igual que en los casos anteriores, Argentina es un país que ha reforzado su normatividad vigente en materia de protección de datos personales, a fin de mantener el vínculo comercial con la Unión Europea, la cual, en la Resolución C (2003) 1731 de la Comisión de las Comunidades Europeas, estableció:

"Considerando lo siguiente:

"**(1)** De conformidad con la Directiva 95/46/CE, los Estados miembros sólo permitirán la transferencia de datos personales a un país tercero si éste proporciona un nivel de protección adecuado y se cumplen en él, con anterioridad a la transferencia, las disposiciones legales que los Estados miembros aprueben en aplicación de otros preceptos de dicha Directiva.

…

" **(4)** Ante los diferentes enfoques sobre la protección de datos adoptados en los terceros países, tanto la evaluación de la adecuación como la ejecución de las decisiones en virtud del apartado 6 del artículo 25 de la Directiva 95/46/CE deben hacerse sin que originen, en igualdad de condiciones, una discriminación arbitraria o injustificada contra terceros países o entre ellos, ni constituyan una restricción comercial encubierta contraria a los compromisos internacionales de la Comunidad.

" **(5)** En el caso de Argentina, las normas de Derecho relativas a la protección de datos personales están reguladas mediante leyes generales y sectoriales, todas ellas de efecto jurídico obligatorio.

" **(6)** Las normas generales están contempladas en la Constitución, la Ley 25 326 sobre protección de datos personales y el Decreto Reglamentario nº 1558/2001…

…

" **(8)** La Ley 25 326 sobre protección de datos personales, de 4 de octubre de 2000 […] desarrolla y amplía lo dispuesto en la Constitución. Contiene normas sobre los principios generales de protección de datos, los derechos de los titulares de datos, las obligaciones de responsables y usuarios de datos, el órgano de control, las sanciones y el procedimiento del recurso judicial habeas data.

"**(14)** La legislación argentina comprende todos los principios fundamentales necesarios para que las personas físicas reciban una protección adecuada, pese a que también estén previstas excepciones y limitaciones para proteger intereses públicos importantes…

"HA ADOPTADO LA PRESENTE DECISIÓN:

…

"**1.** Sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las normas nacionales adoptadas de conformidad con preceptos diferentes a los contemplados en el artículo 25 de la Directiva 95/46/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia un receptor argentino, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos en que:

"**a)** la autoridad competente argentina compruebe que el receptor ha vulnerado las normas de protección aplicables; o

"**b)** existan grandes probabilidades de que se estén vulnerando las normas de protección, existan razones para creer que la autoridad competente

argentina no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia pueda crear un riesgo inminente de grave perjuicio a los afectados, y las autoridades competentes del Estado miembro hayan hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad responsable del tratamiento en Argentina y proporcionarle la oportunidad de alegar.

"La suspensión cesará en cuanto quede garantizado el cumplimiento de las normas de protección y las autoridades correspondientes de la Comunidad hayan sido notificadas de ello.
…"

Argentina, al igual que España, contempla en una sola ley la regulación del Derecho Humano a la Protección de Datos Personales para el sector público y privado. El objetivo de dicha norma es:

"… la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre…"[50]

Es importante señalar, que el legislador argentino reconoció a dicha norma como reglamentaria del artículo 43 de la Constitución de ese país, que es el que confiere la protección constitucional de los datos personales.

Es de señalar que el caso de la ley argentina de protección de datos personales, condiciona la licitud del tratamiento[51] a:

- Que el sistema de datos personales se encuentre previamente inscrito.
- Que cumpla con todos los principios establecidos en la Ley, tal como el de calidad de los datos personales.

El principio de calidad de los datos personales se encuentra conformado por otros tantos, tales como: lealtad en la recolección de éstos, el de finalidad, exactitud y actualización de los datos, almacenamiento accesible; esto en virtud de que este principio rector de la ley argentina establece una serie de obligaciones repartidas en toda ley, tendientes a asegurar que los datos tratados respondan a la exigencia de otros principios, como el de exactitud, veracidad, pertinencia y actualidad.

[50] Artículo 1, de la Ley 25.326
[51] Op. Cit. Artículo 3.

El principio relativo a la lealtad en la recolección de los datos personales implica que los datos personales no sean obtenidos de manera desleal o fraudulenta, o contrarios a la finalidad que persigue el tratamiento. El segundo principio señalado, se encuentra hermanado al anterior, y establece que los datos personales no pueden ser utilizados para otro fin distinto al dado a conocer al titular de estos datos; no se puede perder de vista que la finalidad de la recolección de los datos personales y la utilización de éstos establecen un vínculo que no se debe romper, ya que la finalidad legitima su utilización.

La exactitud y actualización de los datos personales establecen la obligación de cerciorarse que la información responda a la realidad del titular, con el fin de que el tratamiento no conlleve a errores o medias verdades y, en su caso, permitir a éste la actualización de la información objeto de tratamiento, a fin de que responda a su realidad.

Del almacenamiento accesible, este cuarto principio implica que los datos personales sean almacenados de tal forma que se permita el ejercicio de los derechos contemplados en la Ley, tales como el de acceso a los datos personales.

Por último, está el principio de destrucción de los datos personales, opera una vez concluido el motivo por el que se recabaron dichos datos, en otras palabras, este principio tiene como fin impedir la permanencia en uno o más sistemas de aquellos datos personales obsoletos, cuya calificación lo determinará la finalidad del tratamiento.

Antes de concluir el estudio de la Ley, es de señalar que, en forma independiente a los principios señalados en los párrafos anteriores, también se contempla el principio de confidencialidad, previamente analizado, así como los Derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) y la acción de Habeas Data. En forma independiente a esto, la Ley establece que las asociaciones o entidades privadas podrán elaborar códigos de conducta, los cuales deberán buscar establecer las normas para el procesamiento de los datos personales, con el fin último de asegurar y mejorar las condiciones de operación de los sistemas que se encuentren en poder de sus agremiados. Estos códigos, se encuentran regulados en el artículo 30 de la Ley 25.326, e impone una condicionante para su validez, consistente en la obligación de registrar esos instrumentos ante la Dirección Nacional de Protección de Datos Personales, órgano garante de la materia.

1.5 La evolución del Derecho a la Protección de Datos Personales en México

La evolución normativa del Derecho Humano a la Protección de Datos Personales en nuestro país se encuentra hermanada, por lo menos en el sector público, con la evolución o involución del Derecho Humano de Acceso a la Información Pública y la política pública de transparencia, cuyos orígenes datan del 2002, con la promulgación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

1.5.1 Antecedentes: Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

En esta Ley se estableció el tema de los datos personales y la privacidad como un límite al derecho de acceso a la información; así mismo, se estableció un capítulo específico en materia de protección de datos personales en posesión de los sujetos obligados a esa ley, el cual fue ampliamente desarrollado por el Instituto Federal de Acceso a la Información y Protección de Datos, mediante lineamientos de observancia general.

Esta longeva ley de transparencia establece diversos principios básicos en la materia en estudio, que a saber son: calidad de la información, de información, fidelidad, seguridad, consentimiento y confidencialidad, tal como se puede observar en los artículos 20 y 21 de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental:

"***Artículo 20...***

"**I.** Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

"**II.** Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

"**III.** Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;

"**IV.** Procurar que los datos personales sean exactos y actualizados;

"V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren

inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

" **VI.** Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

"***Artículo 21.*** Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.
..."
Sin embargo, a pesar del reconocimiento de estos principios recogidos en la Ley señalada, sólo contempla la posibilidad de ejercitar los derechos de acceso y rectificación de datos personales en posesión de los sujetos obligados.

Ahora bien, con referencia al consentimiento, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, establece que, éste no será requerido cuando sean:

"II. [...] necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

"III. [...] transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

"IV. [...] exista una orden judicial;

"V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido;

1.5.2 Antecedentes en el Distrito Federal

En centro del país, la evolución del tema de protección de datos personales, al igual que en la federación, se encuentra en la Ley de Transparencia y Acceso a la Información Pública promulgada por la Asamblea Legislativa en el 2003, en la cual, siguiendo la pauta dada por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, se incorporó el tema en un capítulo donde se reconoció el derecho de todas las personas a acceder a los registros y/o datos que obraren en los archivos de los entes públicos (ahora entes obligados), a la rectificación y supresión de éstos; asimismo, siguiendo la

lógica fijada por la Directiva 95/46/CE y ley federal señalada, se establecieron algunos principios rectores, tales como el de licitud y publicidad.

Además, se instituyó en la Ley del 2003 la obligación de los entes de recabar el consentimiento de los interesados para su revelación a terceros, y el de mantenerlos actualizados[52].

Durante las múltiples reformas que sufrió esa ley, el capítulo en comento permaneció inerte, exceptuando la adición del artículo 32 bis, el 28 de octubre del año 2005, cuando el legislador incorporó algunas excepciones al consentimiento previo, que son las mismas que actualmente contempla le Ley de Protección de Datos Personales para el Distrito Federal.

No fue sino hasta el año 2008 que el tema de protección de datos personales en el Distrito Federal obtuvo una vida propia, cuando dejó de ser un apéndice de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal; esto se debió a que el tema se reguló independientemente en la Ley de Protección de Datos Personales para el Distrito Federal.

Los detonantes de la promulgación de la ley antes citada fueron dos factores: el primero de ellos, la intensa actividad realizada por el Instituto de Acceso a la Información y Protección de Datos Personales; y el segundo, la reforma del artículo sexto constitucional.

1.5.3 Reforma constitucional

A pesar de que nuestra Constitución, desde 1857, reconoció el derecho a la privacidad o intimidad, fue hasta el 2006 que se reconoció expresamente el derecho a la protección de datos personales como un Derecho Humano.

La Constitución Política de los Estados Unidos Mexicanos de 1857 reconoció en el artículo 16 que:

"... Nadie puede ser molestado en su persona, familia, domicilio, papeles y posesiones, sino en virtud de mandamiento escrito de la autoridad competente..."

Esa redacción fue mantenida en el constituyente del 17, y pasaron más de 85 años para que el Constituyente Permanente incorporara en nuestra Carta Magna el Derecho Humano a la Protección de Datos Personales y reconocerlo como un derecho independiente. Este reconocimiento lo hizo dentro de

[52] Santisteban, Maza Rodrigo, "Una aproximación al derecho de protección de datos personales en la Ciudad de México", Temas Selectos del Derecho a la Información, Derecho a la Intimidad, Transparencia y Datos Personales; Editado: Instituto Tabasqueño de Transparencia y Acceso a la Información Pública, Universidad Juárez Autónoma de México, 2010, p.262.

la reforma del acceso a la información, publicada en el Diario Oficial de la Federación del 20 de julio de 2007.

Artículo 6° de la Constitución Política de los Estados Unidos Mexicanos

En las fracciones II y III del artículo sexto constitucional, el constituyente estableció una prerrogativa a favor de las personas, consistente en que el Estado debe proteger los datos personales que se encuentran en su posesión, y permitir el acceso a esa información de manera gratuita, en los términos fijados por las leyes expedidas en la materia.

Esta reforma constitucional detonó que a nivel estatal se iniciara la discusión y aprobación de algunas leyes de protección de datos personales en posesión del Estado, o, que fueran perfeccionadas las leyes de acceso a la información tendientes a garantizar la protección de los datos personales en posesión del sector público. Un ejemplo de esto son: la Ley de Protección de Datos Personales para el Distrito Federal; la reforma de la Ley de Protección de Datos Personales del Estado de Oaxaca, del 7 de agosto de 2008; y la reforma de la Ley de Información Pública, Estadística y Protección de Datos Personales de Morelos del 24 de diciembre de 2008.

Artículo 16° de la Constitución Política de los Estados Unidos Mexicanos

En el Diario Oficial de la Federación del 30 de abril de 2009, se escribió una página más en la historia reciente del Derecho Humano en estudio, al conferir, en el artículo 73, fracción XXIX-O, la facultad expresa al Congreso de la Unión para legislar sobre la protección de datos personales en posesión de los particulares, lo que ayudo a superar la discusión doctrinal y política, respecto a que el Congreso de la Unión no contaba con esa facultad, y, por ende no podía promulgar una ley que reglamentara ese derecho. Esta reforma constitucional se vio reforzada con la siguiente página de la historia mexicana del derecho a la protección de datos personales, que se dio, cuando en el Diario Oficial de la Federación del 1 junio de ese mismo año, se adicionó un segundo párrafo al artículo 16 constitucional, en el cual se reconoce expresamente el Derecho a la Protección de Datos Personales, al señalar que:

"...

"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."

Estas dos reformas constitucionales culminaron con la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), que fue publicada en el Diario Oficial de la Federación del 5 de julio de 2010.

Las competencias de la Federación y los Estados

Como hemos observado en el punto relativo a las reformas constitucionales, el tema de protección de datos personales se encuentra regulado desde la óptica de los artículos 6° y 16° constitucionales, los cuales van limitando los campos competenciales de la federación y los estados.

El segundo párrafo del artículo 6° de la Constitución Política de los Estados Unidos Mexicanos establece que la federación, los estados y el Distrito Federal se deberán regir por los principios y bases ahí establecidos; así mismo, establece en el artículo segundo transitorio, la obligación a cargo de éstos, de expedir leyes o adecuar las vigentes a esos principios y bases, dentro de las cuales se encuentra el tema de protección de datos personales en posesión del sector público.

Ahora bien, como pudimos observar, el artículo 73, fracción XXIX-O, establece que es competencia exclusiva del Congreso de la Unión regular el tema de protección de datos personales en posesión de los particulares. Excluyendo, de esta forma, la posibilidad de que un Congreso Local puedan expedir leyes que reglamenten los datos personales en posesión de los particulares; pero no excluye la posibilidad de que el Congreso de la Unión expida una Ley que reglamente la protección de datos personales en posesión del sector público, ya que, como vimos, el Constituyente Permanente le confiere esa atribución en el artículo segundo transitorio de la reforma del 20 de julio de 2007.

Aspectos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

La LFPDPPP, tiene por objeto:
"... la protección de los datos personales[53] 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..."[54]

Del artículo en comento podemos señalar que su fin es regular el tratamiento de los datos personales en posesión de los particulares, sin embargo, quedan

[53] En términos del artículo 3, fracción V, de la LFPDPPP, los datos personales son definidos como: "[c]ualquier información concerniente a una persona física identificada o identificable".
[54] Artículo 1 de la LFPDPPP.

excluidos de esta ley las sociedades de información crediticias y las personas que lleven a cabo el tratamiento de datos personales sin un fin de lucro o divulgación[55].

Los principios recogidos en esta Ley, que buscan responder a los estándares fijados por la Directiva 95/46/CE, los localizamos en el artículo 6°, y son: el de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Las reglas del consentimiento las localizamos en los artículos 8°, 9° y 10°, en los cuales se señala que existen dos tipos de consentimiento: el tácito y expreso; el primero de ellos aplica cuando el particular, teniendo a la vista el "Aviso de Privacidad"[56], no se opone al tratamiento de los datos personales que son recabados; y el expreso se requiere cuando el sujeto obligado recabe datos de índole patrimonial o sensibles[57]. El consentimiento, establece el señalado artículo, puede ser revocado en cualquier momento, con la condicionante de que no se le atribuyan efectos retroactivos.

Es importante resaltar que esta Ley señala que cuando se recaben los datos sensibles, el consentimiento debe estar por escrito y manifestado por medio de la firma autógrafa o electrónica; asimismo, prohíbe la creación de bases o sistemas de datos personales que contengan ese tipo de datos, salvo que se justifique su creación.

Esta Ley, al buscar cumplir con los estándares fijados tanto por la multicitada

[55] Artículo 2 de la LFPDPPP.

[56] El Aviso de Privacidad es definido en el artículo 3 de la LFPDPPP como: "... [d]ocumento 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 presente Ley...". Los elementos que conforman al Aviso de Privacidad los localizamos en el artículo 16 de esa misma ley, los cuales son:

"I. La identidad y domicilio del responsable que los recaba;

"II. Las finalidades del tratamiento de datos;

"III. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;

"IV. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;

"V. En su caso, las transferencias de datos que se efectúen, y

"VI. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

..."

Ese mismo artículo señala que cuando se recaben datos personales sensibles, se debe señalar expresamente que se dará tratamiento a ese tipo de datos.

[57] Los datos sensibles, en términos de la fracción VI del artículo 3 de la LFPDPPP, son: "[a]quellos 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 futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual".

Directiva, y las leyes analizadas previamente, establece la obligación, a cargo de los sujetos obligados, de fijar y mantener las medidas de seguridad administrativas, técnicas y físicas, que permitan proteger la integridad de los sistemas de datos que se encuentren en su posesión, y evitar las pérdidas, alteraciones o destrucción.

La LFPDPPP, a diferencia de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, reconoce la posibilidad de que los titulares de los datos personales puedan ejercitar los 4 derechos constitucionales reconocidos en el artículo 16, son: los derechos de Acceso, Rectificación, Cancelación y Oposición[58]. El procedimiento y plazos para dar respuesta a estos derechos, se encuentran regulados en los artículos 22 al 35 de la LFPDPPP.

Asimismo, esta Ley contempla un capítulo específico que reglamenta las transferencias nacionales e internacionales de los datos personales, estableciendo que no se requerirá el consentimiento del titular de los datos personales:

"**I.** Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

"**II.** Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

"**III.** Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

"**IV.** Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;

"**V.** Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

"**VI.** Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y

"**VII.** Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular"[59].

[58] Es importante resaltar que, estos derechos no serán desarrollados en éste apartado, en virtud de que serán analizados profundamente en la Sesión II "Algunos aspectos generales y los procedimientos contemplados en la Ley de Protección de Datos Personales para el Distrito Federal", apartado 2.5. "El procedimiento de los Derechos ARCO y los principios inmersos".
[59] Artículo 37 de la LFPDPPP.

Como podemos observar, no se requerirá el consentimiento previo cuando se encuentren en juego otros derechos superiores, tales como la seguridad o salud del titular, o cuando se trate de un bien mayor.

El Constituyente Permanente estableció que en nuestro país, siguiendo la lógica de algunas de las leyes analizadas con anterioridad, era necesario establecer un órgano garante que vigile el cumplimiento de la norma en estudio, dicho órgano es el Instituto Federal de Acceso a la Información y Protección de Datos[60], que tiene como objeto:

"***Artículo 38.-*** [...] 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 presente Ley y que deriven de la misma; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento".

La facultad de vigilancia, en términos de la LFPDPPP, el Instituto la podrá hacer por medio de las verificaciones, las cuales son iniciadas de dos formas: la primera de ellas es de oficio, la cual procederá -en los términos del artículo 59 de la LFPDPPP-, "... cuando se dé el incumplimiento a resoluciones dictadas con motivo de procedimientos de protección de derechos [conferidos en la ley] o se presuma, fundada y motivadamente, la existencia de violaciones..." a la Ley en estudio; y la segunda, a petición de parte.

1.6 Aspectos relevantes de la Ley de Protección de Datos Personales para el Distrito Federal

Como se señala en el Prólogo de la Ley de Protección de Datos Personales para el Distrito Federal Comentada, los órganos del "... Estado están obligado a difundir la información relacionada con el ejercicio del poder público, también tiene el deber de proteger la información de carácter personal que sobre sus gobernados detentan..."[61] con el fin último de garantizar el Derecho Humano a la Intimidad, y he aquí el objeto de la Ley señalada, que establece los principios, derechos, obligaciones y procedimientos que han de regular la recolección y procesamiento de los datos personales, que se encuentran bajo la tutela de los entes públicos.

I.6.1. Disposiciones de carácter general

La presente ley, al ser reglamentaria de un Derecho Humano, debe ser

[60] Es importante señalar que no se trata de un nuevo órgano del Estado, sino que su creación deviene del 2002, con publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental; con lo cual el Constituyente Permanente busco aprovechar la experiencia que tenía el Instituto en la vigilancia y promoción del Derecho de Acceso a la Información Pública.

[61] Ley de Protección de Datos Personales Comentada, p. 19.

interpretada de tal forma que, permita favorecer en todo momento al titular de los derechos conferidos en los artículos constitucionales previamente analizados y en la Ley de Protección de Datos Personales para el Distrito Federal; esta interpretación debe estar acorde a lo señalado en el segundo párrafo del artículo 1o. de la Constitución Política de los Estados Unidos Mexicanos, que señala:

"...

"Las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia.

..."

Al respecto, el artículo 3 de la Ley de Protección de Datos Personales para el Distrito Federal, impone la obligación al Instituto de Acceso a la Información Pública y Protección de Datos Personales y a los entes obligados, de interpretar las disposiciones ahí contempladas:

"... se realizará conforme a la Constitución Política de los Estados Unidos Mexicanos, la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales respectivos" Es decir, la Ley debe ser analizada desde el punto de visto de, por lo menos, nuestra Carta Magna y diversos instrumentos internacionales, que previamente haya ratificado nuestro país. Lo que implica, como menciona el Dr. Miguel Carbonell, en la obra previamente citada, la posibilidad, dentro del proceso de interpretación, de no sólo circunscribirnos a los instrumentos internacionales señalados, sino que nos abre el abanico para analizar otros tantos instrumentos internacionales y la interpretación que de ellos haya emanado, tales como la Convención de la Organización Internacional del Trabajo, la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, o la Convención Interamericana para la Eliminación de todas las formas de Discriminación de las Personas con Discapacidad.

Es de aclarar que la interpretación que haya emanado del instrumento internacional que sirva de base para clarificar un precepto contemplado en la ley, no debe ser analizada en sentido que restrinja el o los derechos analizados, sino que debe buscar, en todo momento, favorecer al titular de los datos personales, so pena de incurrir en una violación directa a la Constitución Política de los Estados Unidos Mexicanos.

La supletoriedad de una ley respecto de otra, procede para integrar una omisión "involuntaria" por parte del legislador en la ley, o para interpretar sus disposiciones en forma que se integren con otras normas o principios generales contenidos en otras leyes; he aquí la importancia de contar en una ley que regula un derecho fundamental, tener claramente las leyes en que los usuarios podrán basarse para interpretar los alcances de un precepto o subsanar un "error" legislativo. En el caso de la Ley de Protección de Datos Personales para el Distrito Federal, esta cláusula de supletoriedad, la encontramos en el artículo 4°, que señala que la Ley de Procedimientos Administrativos y el Código de Procedimientos Civiles, ambos instrumentos del Distrito Federal, serán las normas que se deberán de observar en caso de deficiencia. Es importante resaltar que estas normas generales aplican para la sujeción del actuar de la autoridad, y las acciones procesales dentro de su actuar.

El Dr. Carbonell, en su comentario plasmado en la obra coeditada antes señalada, menciona que la supletoriedad en el derecho a la protección de datos personales es aún más importante, debido a la:

"… razón de su objeto, que es muy novedoso dentro del ordenamiento jurídico mexicano y eso puede suscitar en ocasiones que haya asuntos en los que el legislador, comprensiblemente, no pueda reparar o no se haya detenido con la profundidad que ameritan. Por eso es que resulta indispensable una adecuada cláusula de supletoriedad como la que introduce el artículo 4 que ahora comentamos".
Agrega el autor que algunas tesis jurisprudenciales emitidas por el Poder Judicial de la Federación, estiman que esta figura jurídica se puede aplicar cuando la ley que se ha de suplir lo prevé expresamente una determinada institución jurídica, pero de forma incompleta o deficiente. Dado el caso de que la figura jurídica no estuviera contemplada en la ley a suplir, entonces la supletoriedad no procedería[62].

Un ejemplo de los criterios planteados por el autor, lo encontramos en las siguientes tesis aisladas:

Registro No. 164889
Localización:
Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
XXXI, Marzo de 2010
Página: 1054
Tesis: 2a. XVIII/2010
Tesis Aislada
Materia(s): Común

[62] Op. Cit. p. 49.

SUPLETORIEDAD DE LAS LEYES. REQUISITOS PARA QUE OPERE.

La aplicación supletoria de una ley respecto de otra procede para integrar una omisión en la ley o para interpretar sus disposiciones en forma que se integren con otras normas o principios generales contenidos en otras leyes. Así, para que opere la supletoriedad es necesario que: a) el ordenamiento legal a suplir establezca expresamente esa posibilidad, indicando la ley o normas que pueden aplicarse supletoriamente, o que un ordenamiento establezca que aplica, total o parcialmente, de manera supletoria a otros ordenamientos; b) la ley a suplir no contemple la institución o las cuestiones jurídicas que pretenden aplicarse supletoriamente o, aun estableciéndolas, no las desarrolle o las regule de manera deficiente; c) esa omisión o vacío legislativo haga necesaria la aplicación supletoria de normas para solucionar la controversia o el problema jurídico planteado, sin que sea válido atender a cuestiones jurídicas que el legislador no tuvo intención de establecer en la ley a suplir; y, d) las normas aplicables supletoriamente no contraríen el ordenamiento legal a suplir, sino que sean congruentes con sus principios y con las bases que rigen específicamente la institución de que se trate.

Contradicción de tesis 389/2009. Entre las sustentadas por los Tribunales Colegiados Segundo en Materia Administrativa del Segundo Circuito y Segundo en la misma materia del Séptimo Circuito. 20 de enero de 2010. Mayoría de cuatro votos. Disidente: Sergio Salvador Aguirre Anguiano. Ponente: José Fernando Franco González Salas. Secretaria: Ileana Moreno Ramírez.
Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
III, Abril de 1996
Página: 480
Tesis: IV.2o.8 K
Tesis Aislada
Materia(s): Común

SUPLETORIEDAD DE UNA LEY A OTRA. REQUISITOS PARA SU PROCEDENCIA. Los requisitos necesarios para que exista supletoriedad de una ley respecto de otra, son a saber: 1.- Que el ordenamiento que se pretenda suplir lo admita expresamente y señale la ley aplicable; 2.- Que la ley a suplirse contenga la institución jurídica de que se trata; 3.- Que no obstante la existencia de ésta, las normas reguladoras en dicho ordenamiento sean insuficientes para su aplicación al caso concreto que se presente, por falta total o parcial de la reglamentación necesaria, y 4.- Que las disposiciones con las que se vaya a colmar la deficiencia no contraríen las bases esenciales del sistema legal de

sustentación de la institución suplida. Ante la falta de uno de estos requisitos, no puede operar la supletoriedad de una ley en otra.

Amparo en revisión 44/96. Elsa Blomeier Eppen. 27 de marzo de 1996. Unanimidad de votos. Ponente: Leandro Fernández Castillo. Secretario: Daniel Cabello González.

Es necesario resaltar en este punto, la siguiente Tesis Aislada:

Localización:
Octava Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación
XV-II, Febrero de 1995
Página: 563
Tesis: VI.1o.185 C
Tesis Aislada
Materia(s): Civil

SUPLETORIEDAD DEL CODIGO FEDERAL DE PROCEDIMIENTOS CIVILES. SALVO DISPOSICION DE LA LEY, TIENE APLICACIÓN EN PROCEDIMIENTOS ADMINISTRATIVOS FEDERALES. El Código Federal de Procedimientos Civiles debe estimarse supletoriamente aplicable (salvo disposición expresa de la ley respectiva) a todos los procedimientos administrativos que se tramiten ante autoridades federales, teniendo como fundamento este aserto, el hecho de que si en derecho sustantivo es el Código Civil el que contiene los principios generales que rigen en las diversas ramas del Derecho, en materia procesal, dentro de cada jurisdicción, es el código respectivo el que señala las normas que deben regir los procedimientos que se sigan ante las autoridades administrativas, salvo disposición expresa en contrario.

PRIMER TRIBUNAL COLEGIADO DEL SEXTO CIRCUITO.

Amparo en revisión 82/89. Margarita Bernardina Hernández de los Santos. 27 de junio de 1989. Unanimidad de votos. Ponente: Carlos Gerardo Ramos Córdova. Secretario: Diógenes Cruz Figueroa.

1.6.2 Conceptos básicos

El artículo 1° de la Ley de Protección de Datos Personales para el Distrito Federal reconoce que el tema se encuentra conformado por diversos principios que le dan sustento; sin embargo, como se mencionaba anteriormente, al ser un tema novedoso en el sistema jurídico mexicano, es necesario establecer una

serie de conceptos básicos que nos permitan tener un panorama mayor de lo regulado en dicha ley.

Conceptos: Derechos ARCO

Los denominados derechos ARCO son el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales, los cuales se encuentran contemplados desde el artículo 16 constitucional y son recogidos por la Ley de Protección de Datos Personales para el Distrito Federal. Estos derechos "… sirven a la capital función que desempeña este derecho fundamental (Derecho a la Protección de Datos Personales): garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer…"[63].

El derecho de Acceso a los datos personales faculta al titular de los datos para dirigirse al ente púlbico, con el fin de "… solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevén hacer, en términos de lo dispuesto por esta Ley" (sic)[64].

El Derecho de Rectificación de datos personales, al igual que el anterior, faculta al titular la posibilidad de modificar aquellos datos que "…resulten inexactos o incompletos, inadecuados o excesivos…"[65]; es importante resaltar que el ejercicio de ese derecho se encuentra supeditado a que no resulte imposible su rectificación o exija esfuerzo desproporcionado.

El derecho de Cancelación de datos personales puede ser definido como aquel derecho que permite, al titular de éstos, solicitar al ente público el bloqueo y posterior eliminación de aquella información que no se encuentre ajustada a los principios y procedimientos establecidos en la Ley de Protección de Datos Personales para el Distrito Federal.

Por último, el Derecho de Oposición permite, al titular de los datos personales, negarse a que su información sea objeto de tratamiento dentro de un sistema, cuando ésta hubiere sido recabada sin el consentimiento de éste. El artículo 30 de la multicitada ley señala que su procedencia estará condicionada a que: existan motivos fundados y que la ley no disponga algo en contrario.

Es importante resaltar que el ejercicio de cualquiera de estos derechos no se encuentra condicionado al ejercicio previo de algún otro. Asimismo, es de

[63] Sentencia 292/2000 del Tribunal Constitucional Español, del 30 de noviembre de 2000.

[64] Artículo 27, de la Ley de Protección de Datos Personales para el Distrito Federal.

[65] Op.cit. Artículo 28.

señalar que los derechos ARCO, son derechos personalísimos cuya demanda sólo puede ser accionada por el titular de los datos personales o por su representante, bajo los términos señalados en la Ley de Protección de Datos Personales para el Distrito Federal.

Principios generales

Los principios generales que regulan la materia de protección de datos personales en el Distrito Federal los encontramos en el artículo 5 de la Ley de Protección de Datos Personales del Distrito Federal y en el Capítulo III de los Lineamientos para la Protección de Datos Personales para el Distrito Federal, publicados en la Gaceta Oficial del Distrito Federal (Lineamientos) el 26 de octubre de 2009.

Estos principios son: licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad. En los artículos 8 y 9 de la Ley en comento, se localizan los principios de transparencia y el de información.

Licitud

Con referencia al principio de licitud, el artículo 5 de la Ley de Protección de Datos Personales para el Distrito Federal señala que se cumplirá con éste cuando los:
"… sistemas de datos personales [obedezcan] exclusivamente a las atribuciones legales o reglamentarias de cada ente público y deberán obtenerse a través de medios previstos en dichas disposiciones…"

Lo que implica que los datos personales tratados en un sistema de datos personales, sean los necesarios para el cumplimiento de lo dispuesto en una norma previamente establecida. La licitud del tratamiento, como señala la Dra. Isabel Davara F. de Marcos, en la obra "Ley de Protección de Datos Personales, Comentada", "… también se concreta en que no puedan crearse sistemas de datos con finalidades que resulten contrarias a la Ley o a la moral pública…"[66]; en este sentido, el numeral 19 de los Lineamientos señala que no se cumplirá con este principio cuando el fin sea distinto o incompatible con los motivos que le dieron origen al sistema de datos personales.

Es de resaltar que no se considerará ilícito el tratamiento de un dato personal cuando el fin que se persiga se encuentre relacionado con información histórica, estadística o científica.

[66] Op. Cit. p. 53.

Consentimiento

Uno de los componentes que aseguran la legitimidad de un tratamiento, reside en el principio del consentimiento, el cual implica que el titular autorice el tratamiento de sus datos, a menos que concurra alguna de las excepciones previstas en la Ley. Al respecto, el artículo 5 de la norma en comento señala que el consentimiento:

"Se refiere a la manifestación de voluntad libre, inequívoca, específica e informada, mediante la cual el interesado consiente el tratamiento de sus datos personales".

No se debe omitir que el consentimiento es el paso posterior al principio de información[67], que contempla la obligación de los entes públicos de informar: "**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

[67] Los Lineamientos, respecto al principio de información, señalan que para que los entes públicos den cumplimiento "… deberán utilizar el siguiente modelo de leyenda para informar al interesado de las advertencias a que se refiere el artículo 9 de la Ley: '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'"

"**VI.** Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

…"[68]

Ahora, como hemos mencionado en múltiples ocasiones dentro de esta sección, existen excepciones al consentimiento, las cuales se encuentran contempladas en el artículo 16 de la Ley de Protección de Datos Personales para el Distrito Federal, que a saber son:

"***Artículo 16.-*** El tratamiento de los datos personales, requerirá el consentimiento inequívoco, expreso y por escrito del interesado, salvo en los casos y excepciones siguientes:

"**I.** Cuando se recaben para el ejercicio de las atribuciones legales conferidas a los entes públicos;

"**II.** Cuando exista una orden judicial;

"**III.** Cuando se refieran a las partes de un convenio de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento;

"**IV.** Cuando el interesado no esté en posibilidad de otorgar su consentimiento por motivos de salud y el tratamiento de sus datos resulte necesario para la prevención o para el diagnóstico médico, la prestación o gestión de asistencia sanitaria o tratamientos médicos, siempre que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente;

"**V.** Cuando la transmisión se encuentre expresamente prevista en una ley;

"**VI.** Cuando la transmisión se produzca entre organismos gubernamentales y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos;

"**VII**. Cuando se den a conocer a terceros para la prestación de un servicio que responda al tratamiento de datos personales, mediante la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente que la comunicación de los datos será legítima en cuanto se limite a la finalidad que la justifique;

"**VIII.** Cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia, o para la realización de estudios epidemiológicos; y

"**IX.** Cuando los datos figuren en registros públicos en general y su tratamiento sea necesario siempre que no se vulneren los derechos y libertades fundamentales del interesado.

[68] Op. Cit. Artículo 9.

"…"

Conforme a lo expuesto hasta este momento, podemos señalar que existen cuatro componentes que, sin los cuales, podríamos decir que estamos ante un tratamiento ilícito. Estos componentes se encuentran recogidos en el lineamiento 18.II de los lineamientos, que a saber son:

"**a)** Libre: Cuando es obtenido sin la intervención de vicio alguno de la voluntad;

"**b)** Inequívoco: Cuando existe expresamente una acción que implique su otorgamiento;

"**c)** Específico: Cuando se otorga referido a una determinada finalidad; e

"**d)** Informado: Cuando se otorga con conocimiento de las finalidades para las que el mismo se produce".

Calidad

Los datos personales que son recabados por el ente público, "… deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Los datos recabados deberán ser los que respondan con veracidad a la situación actual del interesado…"[69] , con la falta de alguno de estos elementos, el principio de calidad no se cumpliría.

¿Qué significa que el dato sea cierto? Se podría decir, como señala la Dra. Davara, para que los datos sean ciertos "… [d]eben estar actualizados en todo momento de manera que respondan a la situación actual de su titular. También puede entenderse la palabra ciertos en el sentido de ser veraces. En cualquier caso, el titular está obligado a proporcionar datos que sean veraces y el responsable a tratar los datos actualizados."

Siguiendo la exposición de la Doctora, se considerará que son adecuados, cuando los datos personales recabados sean pertinentes para el fin que se persigue con su tratamiento.

Se conjugará la pertinencia del tratamiento, cuando éste sea "… realizado por el personal autorizado para el cumplimiento de las atribuciones de los entes públicos que los hayan recabado…", lo anterior, en los términos del inciso c), de la fracción III, del numeral 19 de los Lineamientos.

El otro componente del principio de calidad es el relacionado con la minimización de los datos recabados, es decir, el ente público, en los términos

[69] Op. Cit. Artículo 5.

del inciso d), de la fracción III del numeral 19 de los Lineamientos, sólo podrá recabar aquellos datos "… estrictamente necesaria para cumplir con los fines…" para los que fue creado el sistema de datos personales.

Confidencialidad

La confidencialidad, otro componente del Derecho Humano a la Protección de Datos Personales, implica que sólo el interesado, el responsable o el usuario puedan acceder a los datos.

El deber de secrecía debe, en los términos del artículo 5 de la Ley de Protección de Datos Personales para el Distrito Federal, estar plasmado en un instrumento jurídico:

"… que correspondan a la contratación de servicios del responsable del sistema de datos personales, así como de los usuarios, deberán prever la obligación de garantizar la seguridad y confidencialidad de los sistemas de datos personales, así como la prohibición de utilizarlos con propósitos distintos para los cuales se llevó a cabo la contratación, así como las penas convencionales por su incumplimiento. Lo anterior, sin perjuicio de las responsabilidades previstas en otras disposiciones aplicables".
El alcance del principio de confidencialidad, lo encontramos en el numeral 4 de los Lineamientos, que a la letra señala:

"… Con relación al principio de confidencialidad, se entenderá que los datos personales son:

"**a)** Irrenunciables: El interesado está imposibilitado de privarse voluntariamente de las garantías que le otorga la legislación en materia de protección de datos personales;

"**b)** Intransferibles: El interesado es el único titular de los datos y éstos no pueden ser cedidos a otra persona; e

"**c)** Indelegables: Sólo el interesado tiene la facultad de decidir a quién transmite sus datos personales."

Al respecto, la Agencia de Protección de Datos Personales de la Comunidad de Madrid, en la resolución "[e]l deber de confidencialidad, obliga no sólo al responsable […] sino a todo aquel que intervenga en cualquiera de las fases del tratamiento"[70], al:

[70] http://www.madrid.org/cs/Satellite?c=PAPD_Generico_FA&cid=1142598687159&language=es&pageid=125230839484 6&pagename=PortalAPDCM%2FPAPD_Generico_FA%2FPAPD_fichaResolucion&vest=1252308394846

"… deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el 'deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo'…"

No es absoluto el principio de confidencialidad, y éste cederá ante una resolución jurisdiccional o cuando existan razones de seguridad pública, nacional o salud pública, que obliguen al ente público a revelar esta información sin el consentimiento previo del interesado.

Seguridad[71]

El principio de seguridad, en los términos del artículo 5 de la Ley de Protección de Datos Personales para el Distrito Federal, consiste:

"en garantizar que únicamente el responsable del sistema de datos personales o en su caso los usuarios autorizados puedan llevar a cabo el tratamiento de los datos personales, mediante los procedimientos que para tal efecto se establezcan…".
Este principio, como se ha mencionado en múltiples ocasiones, establece la obligación, del ente público, de adoptar las medidas de índole técnica y organizativas necesarias que garanticen la integridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado; estas medidas son plasmadas, en los términos del artículo 14 de la Ley de Protección de Datos Personales para el Distrito Federal, en el Documento de Seguridad, el cual será analizado más adelante.

Principio de Disponibilidad

Como se ha mencionado, este principio establece la obligación, del ente público, de almacenar los datos personales de modo que permita el tratamiento y el ejercicio de los Derechos ARCO.

Al respecto, la citada Doctora Davara, en la obra "Ley de Protección de Datos Personales para el Distrito Federal Comentada", ha señalado, en la página 59, que:

"… los datos tendrá[n] que estructurarse de manera que en todo momento sea posible atender el ejercicio de los derechos de los interesados.
"Así, al posibilitar el ejercicio de los derechos por los interesados, se puede

[71] Antes de continuar, conviene hacer una pausa, y señalar al lector que en este apartado no será desarrollado a profundidad el tema de los niveles de seguridad, ya que serán parte de la Sección II de este módulo.

garantizar efectivamente el cumplimiento de otros principios de la protección de datos, proteger al interesado, al mismo tiempo que quien los trata cumple con las obligaciones establecidas por la Ley y los Lineamientos".

Temporalidad

El último principio al que hace referencia el artículo quinto de la Ley de Protección de Datos Personales del Distrito Federal, se circunscribe a la obligación que tienen los entes de dar de baja aquellos datos personales que hayan dejado de ser necesarios o pertinentes para el fin por los que fueron recabados en una primera instancia. Esta temporalidad estará sujeta a lo establecido en las vigencias documentales, previamente establecidas en los términos de la Ley de Archivos del Distrito Federal.

Transparencia

Este principio se localiza en el artículo 8 de la norma en estudio, y se traduce en la obligación que tienen los entes públicos de publicitar, por medio del Registro Electrónico de Sistemas de Datos Personales, los sistemas que se encuentren en su posesión.

Sistemas de Datos Personales (SDP)

El SDP es definido, en la fracción XVIII del numeral 3 de los Lineamientos, como el:

"… Conjunto organizado de datos personales que estén en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, que permita el acceso a datos con arreglo a criterios determinados, cualquiera que fuere la modalidad de su creación, almacenamiento, organización o acceso…"

Los SDP se encuentran regulados en el contexto de la Ley de Protección de Datos Personales para el Distrito Federal en el Capítulo II, que define su creación y mantenimiento. Como señala la Dra. Issa Luna Pla, en la obra multicitada, en el estudio de los sistemas de datos personales no se puede perder de vista dos puntos fundamentales:

"Primero. La creación de los sistemas o bases de datos personales no deriva de un acto de voluntad de los titulares de las entidades y órganos sujetos a la Ley de Protección de Datos Personales. En cambio, se trata de una facultad de la norma que deviene precisamente de otro mandato legislativo, donde se expresa imperativamente que la entidad en cuestión tiene facultades para

recolectar cierta información de las personas o usuarios para el desempeño de sus funciones sustantivas…

"Segundo. El artículo 6 de la Ley en comento también manda que 'en el respectivo ámbito de sus competencias' las entidades y organismos puedan determinar la modificación o supresión de los datos. El texto normativo en este caso se limita a advertir la posibilidad de que dichos entes públicos intervengan en los actos de modificación total o parcial y hasta de la supresión de los datos personales. Así, esta Ley no otorga nuevas facultades a los entes para administrar los sistemas de datos personales, sino que remite a aquellas que establecen otras leyes para, en este caso, reconocer dicha facultad ya existente por magisterio y adecuarla a los lineamientos que la Ley en comento preverá en el artículo 7 que a continuación se suscribe. Igualmente, habilita la posibilidad de que por acuerdo del titular del ente u organismo público, sea legítima la creación, modificación o supresión de los datos personales.

"Es de esta forma que el artículo 6 de la Ley de Protección de Datos Personales para el Distrito Federal debe entenderse en el contexto de los principios de la tutela y protección de datos personales establecidos en el artículo 5 de la presente Ley. En particular interesan en esta disposición los principios de la licitud, consentimiento, finalidad, la seguridad y la temporalidad…
…"
Ahora bien, existen dos tipos de sistemas, los físicos y los automatizados: respecto de los primeros, los datos personales se encuentran contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos, y están estructurados conforme a criterios específicos relativos a personas físicas, de manera que se pueda acceder sin esfuerzos desproporcionados a los datos personales; los segundos, implican la posibilidad de acceder a la información relativa a una persona, utilizando herramientas tecnológicas.

Los primeros pasos que un ente público debe de observar para la creación de un SDP o para su modificación, se encuentran establecidos en las fracciones I y II del artículo 7 de la Ley. La inobservancia de estos dos elementos, haría que el tratamiento de los datos personales sea ilícito; estas reglas son:

- Publicar en la Gaceta Oficial del Distrito Federal la creación o modificación del SDP.

- Esta publicación deberá señalar: 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 el caso de que sea necesaria la supresión del sistema, el artículo en comento señala que el ente público, en las medidas que se tomen para tal efecto, deberá señalar: "… el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción…"[72].

Ahora bien, como hemos observado en algunas leyes previamente analizadas, los entes públicos se encuentran imposibilitados para crear SDP que tenga como único fin la recolección de datos sensibles, lo que se traduce en la prerrogativa que tiene el titular de estos de oponerse a proporcionarlos.[73]

Otra de las excepciones contempladas al principio del consentimiento se encuentran relacionadas con los SDP con fines de seguridad pública, bajo los cuales, en los términos del segundo párrafo del artículo 11 de la Ley de Protección de Datos Personales para el Distrito Federal, no se requerirá el consentimiento del afectado, y su tratamiento estará limitado a las siguientes condicionantes:

- A aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención o persecución de delitos.

- Sólo podrán ser tratados bajo los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas por los interesados ante los órganos jurisdiccionales.

- Una vez concluido estos fines, se cancelarán.

Es de señalar que, a pesar de que estos SDP con fines de seguridad pública tengan un tratamiento preferente, con relación a los demás SDP, no quiere decir que éstos se encuentran exentos de cumplir con todos los principios establecidos en la Ley, e incluso, cumplir con los niveles de seguridad contemplados en esa norma.

[72] Op. Cit. Artículo 7, fracción III.
[73] Op. Cit. Artículo 10.

1.6.3 De los objetivos de la Ley de Protección de Datos Personales para el Distrito Federal

Como se mencionó al inició de este apartado, el objetivo fundamental de la Ley de Protección de Datos Personales para el Distrito Federal se encuentra previsto en el artículo 1, al reconocer que esta norma instituye los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, con el fin último de asegurar un bien mayor, que son los Derechos Humanos a la Privacidad, Intimidad y Dignidad, contemplados en el artículo 16 Constitucional, y en los instrumentos internacionales analizados al principio de la sección.

Es decir, los objetivos de la ley no se circunscriben exclusivamente a señalar los alcances de la norma, sino que tienen como fin último la protección de los derechos fundamentales de las personas físicas y, especialmente, de su honor e intimidad personal y familiar.

Esto es así, recordemos, en virtud de que el Derecho Humano a la Protección de Datos Personales se circunscribe en la dimensión social del ser humano, y su fin último es salvaguardar la dimensión privada, la cual se encuentra fuera de las interconexiones generadas por el escrutinio social.

1.6.4 De los actores

Como todo Derecho Humano, se imponen obligaciones a los Estados para que éstos garanticen su cumplimiento. El caso del Derecho Humano a la Protección de Datos Personales no es la excepción, y la Ley de Protección de Datos Personales para el Distrito Federal identifica, claramente, quiénes son los actores de la Ley, como lo señala el Mtro. Rodrigo Santisteban Maza[74] :

Auditor	A pesar de que esta figura no es reconocida directamente por la ley, es contemplada de manera indirecta en el apartado de las medidas de seguridad, y es aquella persona interna o ajena al ente público, que audita las medidas de seguridad aplicables a sistemas de datos personales.
Cedente	El ente público que transmite datos personales.
Cesionario	Es la persona física, moral o de derecho público que recibe, para su tratamiento, un sistema de datos personales, la cual se encuentra sujeta a todas las disposiciones contempladas en la Ley capitalina.
Destinatario	Cesionario del sistema de datos personales.

[74] Op. Cit. 54, p. 276.

Encargado	Es el servidor público que, en el ejercicio de sus funciones, incide frecuentemente en el tratamiento de los datos personales que conforman el sistema.
Ente Público	La Ley capitalina sólo aplica: la Asamblea Legislativa del Distrito Federal; el Tribunal Superior de Justicia del Distrito Federal; El Tribunal de lo Contencioso Administrativo del Distrito Federal; El Tribunal Electoral del Distrito Federal; el Instituto Electoral del Distrito Federal; la Comisión de Derechos Humanos del Distrito Federal; la Junta de Conciliación y Arbitraje del Distrito Federal; la Jefatura de Gobierno del Distrito Federal; las Dependencias, Órganos Desconcentrados, Órganos Político Administrativos y Entidades de la Administración Pública del Distrito Federal; los Órganos Autónomos por Ley; los partidos políticos, asociaciones y agrupaciones políticas; así como aquellos que la legislación local reconozca como de interés público y ejerzan gasto público; y los entes equivalentes a personas jurídicas de derecho público o privado, ya sea que en ejercicio de sus actividades actúen en auxilio de los órganos antes citados o ejerzan gasto público.
Instancias responsables del tratamiento	La unidad administrativa del ente público que tiene entre sus archivos un sistema de datos personales.
Instituto de Acceso a la Información Pública y Protección de Datos Personales	Es la autoridad responsable del control y vigilancia de la Ley de Protección de Datos Personales para el Distrito Federal.
Interesado	Es la persona física titular de los datos personales.
Oficina de Información Pública	Es la unidad administrativa del ente público ante la cual se presentan las "… solicitudes de acceso, rectificación, cancelación y oposición de datos personales…", en términos del artículo 2° de la Ley,.
Órganos de control y fiscalización internos de los entes públicos	Es la unidad administrativa encargada de la aplicación de la Ley Federal de Responsabilidades de los Servidores Públicos, o de llevar a cabo las auditorías internas.
Responsable de seguridad	La Ley capitalina sólo hace una mención específica a esta figura, sin embargo, al realizar una interpretación armónica de esta disposición normativa, podemos concluir que es una persona distinta al responsable del sistema, y está encargado de las funciones de coordinar y controlar las medidas de seguridad aplicables.
Responsable del sistema de datos personales	Es el servidor público que tiene a su cargo el sistema de datos personales y decide sobre su contenido, así como el que, en colaboración con la Oficina de Información Pública, dará acceso a los datos personales, cancelará, o bloqueará los datos contenidos en el sistema. El servidor público es designado por el titular del ente público.
Titular del ente público	Es aquella persona que se encuentra al frente del ente público, y será el responsable de decidir sobre la finalidad, contenido y uso del tratamiento del sistema de datos personales, quien podrá delegar dicha atribución en la unidad administrativa en la que se concrete la competencia material, a cuyo ejercicio sirva instrumentalmente el sistema de datos y esté adscrito el responsable de éste.
Usuario	Es la persona autorizada por el titular del ente público, para prestarle servicios para el tratamiento de datos personales.

1.6.5 De las obligaciones de los Entes Obligados

La Ley de Protección de Datos Personales para el Distrito Federal, en forma independiente a algunas de las obligaciones de los entes públicos, previamente analizadas, establece, en el artículo 21 de la Ley, una serie de deberes a cargo de éstos.

El primero de ellos, es la designación del responsable del tratamiento, quien, en la práctica, velará por el cumplimiento de las disposiciones contempladas en la Ley en comento, sin que esto implique una delegación de la responsabilidad que le corresponda al ente público como responsable último, y sin perjuicio de la que sí sea exigible a quienes intervengan en el tratamiento de datos de carácter personal por el incumplimiento de sus obligaciones.

Siguiendo la lógica planteada por la Dra. Davara, en las páginas 152 y 153 de la obra "Ley de Protección de Datos Personales para el Distrito Federal Comentada", las obligaciones del ente público se pueden clasificar desde la óptica del objetivo que persiguen:

Materia	Obligaciones
Calidad y finalidad del tratamiento	VI. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;
Información al interesado al obtener sus datos	IV. Informar al interesado al momento de recabar sus datos personales, sobre la existencia y finalidad de los sistemas de datos personales, así como el carácter obligatorio u optativo de proporcionarlos y las consecuencias de ello;
Medidas de seguridad	II. Adoptar las medidas de seguridad necesarias para la protección de datos personales y comunicarlas al Instituto para su registro, en los términos previstos en esta Ley; X. Elaborar un plan de capacitación en materia de seguridad de datos personales; XIV. Coordinar y supervisar la adopción de las medidas de seguridad a que se encuentren sometidos los sistemas de datos personales de acuerdo con la normativa vigente;

Ejercicio de los derechos	V. Adoptar los procedimientos adecuados para dar trámite a las solicitudes de informes, acceso, rectificación, cancelación y oposición de datos personales y, en su caso, para la cesión de los mismos; debiendo capacitar a los servidores públicos encargados de su atención y seguimiento; VII. Permitir en todo momento al interesado el ejercicio del derecho de acceso a sus datos personales, a solicitar la rectificación o cancelación, así como a oponerse al tratamiento de los mismos en los términos de esta Ley; VIII. Actualizar los datos personales cuando haya lugar, debiendo corregir o completar de oficio aquellos que fueren inexactos o incompletos, a efecto de que coincidan con los datos presentes del interesado, siempre y cuando se cuente con el documento que avale la actualización de dichos datos. Lo anterior, sin perjuicio del derecho del interesado para solicitar la rectificación o cancelación de los datos personales que le conciernen; XV. Dar cuenta de manera fundada y motivada a la autoridad competente de la aplicación de las excepciones al régimen general previsto para el acceso, rectificación, cancelación u oposición de datos personales;
Tratamiento de los datos	I. Cumplir con las políticas y lineamientos, así como las normas aplicables para el manejo, tratamiento, seguridad y protección de datos personales; IX. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales; XII. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales; XIII. Llevar a cabo o, en su caso, coordinar la ejecución material de las diferentes operaciones y procedimientos en que consista el tratamiento de datos y sistemas de datos de carácter personal a su cargo;
Obligaciones con respecto al Instituto	III. Elaborar y presentar al Instituto un informe correspondiente sobre las obligaciones previstas en la presente Ley, a más tardar el último día hábil del mes de enero de cada año. La omisión de dicho informe será motivo de responsabilidad;

Este artículo culmina con el señalamiento de que estas obligaciones a cargo del ente público se deben considerar de manera enunciativas y no limitativas; esto en virtud de que, como hemos señalado, existen otras obligaciones contempladas en la Ley, que no son recogidas en el artículo en comento; tales como, la obligación de publicar en la Gaceta Oficial del Distrito Federal, la creación, modificación, supresión de los SDP que se encuentran en su posesión, o la obligación de dictar disposiciones de índole administrativa que contemple la supresión del SDP y el destino final de los datos ahí tratados; o el deber de confidencialidad.

2. Algunos aspectos generales y los procedimientos contemplados en la Ley de Protección de Datos Personales para el Distrito Federal

En esta sección abordaremos, desde un punto de vista teórico, algunos aspectos relevantes de la Ley de Protección de Datos Personales para el Distrito Federal, vinculados con otros instrumentos normativos.

2.1 Consentimiento y sus excepciones

Uno de los ejes rectores de la materia del derecho a la protección de datos personales es, sin duda, el consentimiento que da el titular para el tratamiento de sus datos personales[75].

[75] Es de recordar que en términos de la Ley de Protección de Datos Personales para el Distrito Federal, existen dos tipos de consentimiento, el expreso y el tácito, éste último se configura cuando existe una de las excepciones que analizaremos en el transcurso de éste apartado, y que para que este tipo de consentimiento pueda ser considerado inequívoco, es necesario que sea puesto a la vista del interesado la "leyenda", y se otorgue al titular de los datos personales, el derecho a revocar u oponerse al tratamiento de su información; el consentimiento expreso, se actualiza cuando el titular de los datos personales se expresa a través de de una declaración clara por su parte. Ahora bien, la Agencia Española de Protección de Datos Personales en el Expediente Nº: E/01225/2009 iniciado contra la Federación de Comunicación y Transportes CCOO, a punta al reconocimiento de otro tipo de consentimiento, que es el "presunto", al señalar que "…existiría un consentimiento implícito al respecto del tratamiento de datos referidos a la celebración practicada, no sólo ligada a la condición de afiliados de los denunciantes y por tanto en base a que los mismos se encuentran sometidos a la normativa interna del sindicato, sino en base a la participación de éstos en el propio congreso. Esto es así dado que en materia de protección de datos se articulan tipos de consentimiento más allá del calificado como expreso, como son los consentimientos tácitos y presuntos, desprendiéndose éste último del primigenio comportamiento de los denunciantes, que participaron en el acto sin oposición…". Es de resaltar que, el InfoDF no ha reconocido expresamente la existencia del consentimiento presunto, sin embargo, se infiere, como ha señalado la Agencia Española de Protección de Datos Personales, de un no hacer por parte del titular de los datos personales. Por ejemplo, este tipo de consentimiento se pudiera configurar en los casos, de los sistemas de videovigilancia (de seguridad privada), en donde, el interesado presuntamente consiente el tratamiento de su imagen para un fin determinado.

De conformidad con el artículo 5º de la Ley de Protección de Datos Personales para el Distrito Federal, para que se configure el consentimiento es necesario que se reúnan los siguientes requisitos:

Libre: implica que no existe ningún medio de coacción para su obtención; para que se dé es necesario que el ente público, al momento de recabar el dato personal, ofrezca la posibilidad, al titular de éstos, de oponerse a su tratamiento.

Inequívoco: significa que no debe existir duda alguna del otorgamiento del consentimiento; de ahí la importancia o relevancia de la leyenda que se encuentra contemplada en el artículo 9 de la Ley y el numeral 13 de los Lineamientos para la Protección de Datos Personales en el Distrito Federal (Lineamientos). Ese artículo señala en la parte que nos interesa:

> "Artículo 9. Cuando los entes públicos recaben datos personales deberán informar previamente a los interesados de forma expresa, precisa e inequívoca lo siguiente:
>
> "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;
>
> …"

Como podemos observar, la claridad con el que se redacte la finalidad del tratamiento del dato personal podría llegar a condicionar la validez del consentimiento, porque podría caber la duda sobre el tratamiento del que sería objeto.

Específico: este componente del consentimiento, al igual que el anterior, se encuentra adminiculado con la finalidad del tratamiento, es decir, para su recolección es necesario que el interesado reciba la "… información necesaria sobre la finalidad o finalidades con la que se van a tratar sus datos […] para poder consentir o no dicho tratamiento…"[76].

Informado: para la configuración de este componente del consentimiento, es necesario que, al momento de ser recabado el o los datos personales, se informe la finalidad del tratamiento.

[76] Comentario: Davara, Isabel. "Ley de Protección de Datos Personales para el Distrito Federal Comentada", Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, Gobierno del Distrito Federal, Secretaría de Gobierno, Asamblea Legislativa del Distrito Federal, Tribunal Superior de Justicia del Distrito Federal, México 2010, p. 55

Como apuntamos con anterioridad, para la existencia del consentimiento es necesario que el ente público cumpla con el principio de información, el cual se traduce en la obligación que tiene el ente público de informar, previamente a la recolección del dato personal, los siguientes elementos:

Artículo 9 de la Ley de Protección de Datos Personales para el Distrito Federal	
1	Señalamiento del Sistema de Datos Personales.
2	Señalamiento del tratamiento.
3	De la finalidad de ese tratamiento.
4	Destinatarios de ese dato (en el caso de existencia de una transferencia).
5	El carácter obligatorio o facultativo.
6	De la publicidad de que podrían ser objeto esos datos personales.
7	La posibilidad de ejercitar los Derechos ARCO.
8	Nombre del responsable del SDP.
9	En su caso, nombre del destinatario.

Estos elementos fueron ejemplificados en el numeral 13 de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, en la siguiente leyenda:

> "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"

Es de resaltar que muchos de los datos personales que obran en los sistemas de datos personales pueden tener una antigüedad mayor a la entrada en vigencia de la Ley en comento, por lo que, como medida compensatoria, el numeral 14 de los Lineamientos previamente citados señala que el deber de información no será requerido y, por ende, el consentimiento, cuando "… resulte material o jurídicamente imposible o requiera de esfuerzos desproporcionados, en razón del número de interesados y/o la antigüedad de los datos".

Otras excepciones al principio de información y del consentimiento las localizamos en los artículos 9, 11, 16 y 18 de la Ley de Protección de Datos Personales para el Distrito Federal. El primer artículo señalado, en su cuarto párrafo, marca que no se requerirá el consentimiento del titular de los datos personales cuando así lo haya estipulado una ley; lo anterior se traduce en lo dispuesto en la fracción I del artículo 16 de esa norma, que establece que no será requerido el consentimiento "expreso" del titular de los datos personales cuando sean recabados en el ejercicio de sus atribuciones legalmente conferidas al ente.

Otra excepción directa al principio del consentimiento se localiza en el artículo 11 de la norma en comento, que establece que no será requerido el consentimiento cuando la recolección de los datos personales se realice con fines policiales:

> "… limitándose a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la prevención o persecución de delitos…"

La Agencia Española de Protección de Datos Personales ha señalado, al respecto, que no será requerido el consentimiento expreso o tácito del titular de los datos personales cuando se trate de los mecanismos empleados por los cuerpos de seguridad para el reconocimiento facial, ya que es "… una práctica policial válida para investigar la identidad de una persona, señalando que dicho método puede constituir un punto de partida para iniciar las investigaciones policiales…"[77], y, al ser requerido el consentimiento, puede poner en riesgo el

[77] En la R/00753/2007, agrega la Agencia que: "… la legalidad de la identificación del delincuente mediante la exhibición de fotografías al testigo pues en definitiva tal diligencia prejudicial no tiene otro significado que el de apertura de una línea de

fin que se persigue, que a saber es el mantenimiento del orden público.

El artículo 16 de la Ley de Protección de Datos Personales para el Distrito Federal, establece una serie de excepciones expresas al consentimiento, que aplican tanto en la fase de recolección del dato, como en el tratamiento, en específico la transferencia. Las cuales, son:

> "**I.** Cuando se recaben para el ejercicio de las atribuciones legales conferidas a los entes públicos".

Esta excepción implica que el ente público debe contar con las facultades previamente conferidas –en un marco normativo- a la recolección del dato, las cuales deben estar referenciadas en la "leyenda" a la que hicimos referencia previamente, cuando hablamos del principio de información.

investigación policial en la que la utilización de fotografías, como punto de partida para iniciar las investigaciones policiales, constituye una técnica elemental de imprescindible empleo en todos los casos en que se desconoce la identidad del autor del hecho punible…" lo que, es traducido al caso concreto, que el requerir el consentimiento en estos casos, pone en riesgo un bien mayor, que a saber es el de la seguridad y el orden público.

Excepciones al consentimiento

Artículo 16 de la LPDDF

1. Sin consentimiento cuando exista disposición legal
2. Medie una orden judicial
3. En relación a las partes de un convenio
4. Sea información necesaria en posibilidades de conquista
5. La transmisión se encuentre prevista en una Ley
6. La transmisión se realice entre áreas públicas
7. Sea a terceros a efecto de la prestación de un servicio que responda con el fin del tratamiento
8. Se trate de datos personales relativos a la salud, necesarios por razones de salud pública, de emergencia o estudios epidemiológicos
9. Cuando los datos figuren en registros públicos y se transmitan sin vulnerar los derechos del titular

> "**II.** Cuando exista una orden judicial".

En pocas palabras, esta excepción implica un acto procesal previo a la recolección del dato personal, que es el mandato (fundado y motivado) de una autoridad jurisdiccional, por el que se ordena el procesamiento del dato sin el consentimiento del titular de éste, con el fin de garantizar la integridad de la investigación que lleve a cabo la autoridad competente.

> "**III.** Cuando se refieran a las partes de un convenio de una relación de negocios, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento".

El alcance de la fracción estriba en el tratamiento posterior al nacimiento del convenio, que es su seguimiento y cumplimiento de las obligaciones previamente adquiridas por las partes en ese instrumento jurídico.

> "**IV.** Cuando el interesado no esté en posibilidad de otorgar su consentimiento por motivos de salud y el tratamiento de sus datos resulte necesario para la prevención o para el diagnóstico médico, la prestación o gestión de asistencia sanitaria o tratamientos médicos, siempre que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente".

La fracción IV del artículo 16 de La ley contempla múltiples supuestos por los cuales no se requerirá el consentimiento, supeditados a la preservación de un bien mayor, que es la integridad de la vida y la existencia de una persona que se encuentre obligada a cumplir con el secreto profesional. Estos supuestos son: (1) prevención o diagnóstico médico y (2) prestación o gestión de asistencia sanitaria o tratamiento médico.

Es de resaltar que esta fracción se encuentra íntimamente relacionada con la fracción VIII[78] del artículo en comento, sin embargo, su diferencia radica en el bien tutelado, es decir, mientras que en la fracción IV el bien tutelado es la vida o salud de un individuo, la fracción VIII implica la salud de un colectivo identificable.

> "**V.**Cuando la transmisión se encuentre expresamente prevista en una ley".

[78] La fracción VIII del artículo 16 señala:
"… Cuando se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia, o para la realización de estudios epidemiológicos…
…"

La anterior fracción es aplicable a cualquier fase del tratamiento de los datos personales, e implica que la transferencia que realice el ente público a un tercero, se encuentre previamente contemplada en el marco normativo aplicable al ente público.

Asimismo, se exceptuará del consentimiento del titular la transmisión que se realice al amparo de una relación jurídica, previamente pactada entre el ente público y un tercero, y para el cumplimiento del objeto de esa relación, es necesario que sea indispensable la cesión de datos personales, es decir, que sea imprescindible para el cumplimiento de su finalidad; esto en los términos de la fracción VII del citado artículo. Un ejemplo de esto son las transferencias que realizan los entes públicos a diversas instituciones bancarias para el depósito del sueldo del servidor público.

> "**VI.** Cuando la transmisión se produzca entre organismos gubernamentales y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos".

La fracción VI condiciona la transmisión hacia otro ente, a la existencia de un tratamiento histórico, estadístico o científico, los cuales estarán a lo dispuesto en la norma aplicable a cada uno de ellos.

> "**IX.** Cuando los datos figuren en registros públicos en general y su tratamiento sea necesario siempre que no se vulneren los derechos y libertades fundamentales del interesado".

Esta fracción establece dos elementos acumulativos para la configuración del principio de licitud del tratamiento que se encuentre exento del consentimiento bajo esta hipótesis: el primero de ellos radica en que los datos personales se localicen en una fuente pública, es decir, que puedan ser consultados por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el pago de alguna contraprestación por ese servicio[79]; y el segundo de estos elementos consiste en que su tratamiento no vulnere los derechos del titular de esos datos accesibles libremente, lo que implica que el ente público y/o el InfoDF pondere(n) los derechos e intereses en conflicto, que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate.

Ahora bien, el artículo 18 de la Ley de Protección de Datos Personales para el Distrito Federal contempla otra de las excepciones al consentimiento, la cual,

[79] Agencia Española de Protección de Datos Personales, http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/telecomunicaciones/common/pdfs/2005-0136_Directorios-telef-oo-nicos-y-fuentes-accesibles-al-p-uu-blico-.pdf

es de señalar, se encuentra adminiculada con la fracción IV del artículo 16 de la citada Ley. Ese artículo, en la parte conducente señala:

> "… El tratamiento y cesión a esta información obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera tal que se mantenga la confidencialidad de los mismos, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación científica, de salud pública o con fines judiciales, en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales…"

Como podemos observar, no será necesaria la disociación del expediente clínico, cuando se presenten algunas de las tres hipótesis y una condicionante. Las tres hipótesis, son:

Antes de continuar, es importante destacar que el particular, en todo momento, en los términos del artículo 16 de la Ley de Protección de Datos Personales para el Distrito Federal, puede revocar el consentimiento dado previamente, siempre y cuando:

- Exista una causa justificada para ello.

- No se le atribuyan efectos retroactivos.

Los alcances de este derecho de revocación, fueron establecidos en el numeral 28 de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, al señalar que:

- En caso de ser procedente el ejercicio de este derecho, el responsable del tratamiento deberá:

  - Cesar el tratamiento de los datos.
  - Bloquear esos datos.
- En el supuesto de que hubieren sido cedidos previamente, el responsable deberá:

  - Determinar la procedencia del ejercicio de este derecho.

  - En caso de ser afirmativa la procedencia, deberá comunicarlo al cesionario, para que proceda al bloqueo de esos datos.

Para poder revocar el consentimiento, es necesario que el titular de los datos personales acuda ante la Oficina de Información Pública.

2.2 De los Sistemas de Datos Personales

Uno de los puntos medulares del Derecho Humano, contemplado en el segundo párrafo del artículo 16 constitucional, consiste en el ordenamiento sistemático de los expedientes que cuentan con datos personales, lo que se traduce, para el efecto de la Ley de Protección de Datos Personales para el Distrito Federal, en los Sistemas de Datos Personales (SDP), ya que sin la organización e identificación de esos expedientes no se puede garantizar la protección de ellos, que sería el fin último del citado artículo constitucional; esto adminiculado con la fracción II del artículo sexto de nuestra Carta Magna.

Los sistemas de datos personales, recordando lo analizado previamente, implican, en términos del artículo 2º de Ley en análisis, el "… conjunto organizado de archivos, registros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso…". Es de resaltar que esta definición, aportada por la ley, se debe completar con las definiciones abordadas en las fracciones XIX y XX del numeral 3 de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, las cuales señalan:

"**XIX.** Soporte físico: Son los medios de almacenamiento inteligibles a simple vista, es decir, que no requieren de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos; es decir, documentos, oficios, formularios impresos llenados "a mano" o "a máquina", fotografías, placas radiológicas, carpetas, expedientes, demás análogos;
"**XX.** Soporte electrónico: Son los medios de almacenamiento inteligibles sólo mediante el uso de algún aparato con circuitos electrónicos que procese su contenido para examinar, modificar o almacenar los datos; es decir, cintas magnéticas de audio, vídeo y datos, fichas de microfilm, discos ópticos (CDs y DVDs), discos magneto-ópticos, discos magnéticos (flexibles y duros) y demás medios de almacenamiento masivo no volátil;
…"

De lo anterior, podemos señalar que los sistemas de datos personales, son un conjunto de datos interrelacionados entre sí, que buscan su procesamiento para alcanzar un fin previamente determinado, los cuales no se podrán considerar estáticos, sino que tendrán una interacción con otra información que sea generada, administrada o manejada por el ente público.

2.2.1 Registro Electrónico de Sistemas de Datos Personales

Para que esos sistemas de datos personales cumplan con el principio de licitud, es necesario que su creación, modificación o supresión haya sido previamente publicada en la Gaceta Oficial del Distrito Federal. Dicha publicación, debe contar con:

1. **Identificación del SDP.** Se deberá señalar el nombre del sistema y el fundamento que le da origen.

2. **Origen de los datos.** Se debe indicar, en los términos del lineamiento 7, su procedencia, es decir, si es el titular, representante, etc.; y el procedimiento de recolección.

3. **Estructura básica del SDP.** De conformidad con ese mismo lineamiento, se debe señalar "… la descripción detallada de los datos identificativos que contiene y, en su caso, de los datos especialmente protegidos, así como las restantes categorías de datos de carácter personal, incluidas en el mismo y el modo de tratamiento utilizado en su organización…".

4. **En su caso, las cesiones previstas.** Es decir, el señalamiento de si se contempla realizar la transferencia del SDP; en el caso afirmativo, se deberá indicar el destinatario.

5. **Domicilio y dirección en donde se pueden presentar las solicitudes ARCO.** En este caso, se deberá señalar el domicilio de la Oficina de Información Pública del ente público.

6. **Indicación del Nivel de Seguridad.** Se deberá señalar si a ese SDP es aplicable el nivel básico, medio o superior, los cuales serán determinados en los términos del artículo 14 de la Ley.

Es de mencionar que los acuerdos de creación y de modificación de los sistemas de datos personales expedidos por el titular del ente público deberán ser publicados en la Gaceta Oficial del Distrito Federal, con, por lo menos, 15 días hábiles antes del inicio de la recolección o que surtan efecto las modificaciones que hubieren sufrido. Dichas modificaciones, en los términos del numeral 8 de los multicitados Lineamientos, deben ser notificadas al Instituto de Acceso a la Información Pública y Protección de Datos Personales, en un término no mayor a 10 días hábiles, contados a partir de la fecha en que haya sido publicada en la Gaceta.

En el caso de la supresión de un sistema de datos personales, el acuerdo que se publique en la Gaceta Oficial del Distrito Federal deberá indicar, entre otros elementos:

- El destino que se dará a los datos personales en él contemplado.
- Las previsiones que se adopten para su destrucción.

El citado acuerdo deberá ser publicado con una antelación de 30 días hábiles a que surta efecto la supresión, y será notificado al Instituto con 10 días hábiles posteriores a su publicación.

Cómo hemos observado en los párrafos anteriores, los entes públicos, una vez que hayan hecho la publicación en la Gaceta, tiene la obligación de hacerlo del conocimiento del InfoDF; esto se realiza por medio del Registro Electrónico de Sistemas de Datos Personales, el cual, es consultable en: **http://www.infodf.org.mx:8080/rsdp/.** Los rubros que deben ser llenados por el ente público, por conducto del responsable del sistema, se localizan en el numeral 11 de los multicitados lineamientos:

> ***"11.*** El registro de cada sistema contendrá los siguientes campos:
>
> "I. Nombre del Sistema y, en su caso, fecha de publicación en la Gaceta Oficial del Distrito Federal;
>
> "II. Nombre y cargo del responsable del sistema;

"III. Finalidades y usos previstos, así como el soporte en el que se encuentra;

"IV. La categoría de los datos personales contenidos en el sistema, forma de recolección y actualización de los mismos;

"V. Unidad administrativa en la que se encuentra el sistema;

"VI. Destino y personas físicas o morales a las que puedan ser transmitidos;

"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.

En el caso de que hubieren existido sistemas de datos personales, previos a la entrada en vigencia de la Ley de Protección de Datos Personales para el Distrito Federal, los entes públicos se encuentran eximidos de la publicación del (los) acuerdo(s) en la Gaceta Oficial, pero sí están obligados a su inscripción en dicho registro, so pena de incumplir con los principios de información y licitud.

2.2.2 Niveles de Seguridad de los Sistemas de Datos Personales

Como empezábamos apuntar, en el apartado anterior, los SDP deben cumplir con el principio de seguridad, que consiste en garantizar que sólo quien esté autorizado para ello tenga acceso a la información ahí tratada, es decir, busca garantizar la confidencialidad de los datos personales objeto de tratamiento, a fin de evitar "… alteración, pérdida, transmisión y acceso no autorizado…"80.

Los tipos de seguridad se encuentran contemplados en el artículo 14 de la Ley de Protección de Datos Personales para el Distrito Federal, que a saber son:

"…

"I. **Física.-** Se refiere a toda medida orientada a la protección de instalaciones, equipos, soportes o sistemas de datos para la prevención de riesgos por caso fortuito o causas de fuerza mayor;

"II. **Lógica.-** Se refiere a las medidas de protección que permiten la identificación y autentificación de las personas o usuarios autorizados para el tratamiento de los datos personales de acuerdo con su función;

[80] Artículo 13 de la Ley de Protección de Datos Personales para el Distrito Federal.

"III. **De desarrollo y aplicaciones.-** Corresponde a las autorizaciones con las que deberá contar la creación o tratamiento de sistemas de datos personales, según su importancia, para garantizar el adecuado desarrollo y uso de los datos, previendo la participación de usuarios, la separación de entornos, la metodología a seguir, ciclos de vida y gestión, así como las consideraciones especiales respecto de aplicaciones y pruebas;

"IV. **De cifrado.-** Consiste en la implementación de algoritmos, claves, contraseñas, así como dispositivos concretos de protección que garanticen la integralidad y confidencialidad de la información; y

"V. **De comunicaciones y redes.-** Se refiere a las restricciones preventivas y/o de riesgos que deberán observar los usuarios de datos o sistemas de datos personales para acceder a dominios o cargar programas autorizados, así como para el manejo de telecomunicaciones.

…"

El listado que arroja el inciso A, del artículo 14 de la Ley, está dirigido tanto a los sistemas de datos personales que se encuentren en soporte físico o electrónico o mixto, los cuales serán aplicables dependiendo de los siguientes niveles de seguridad:

- Nivel básico.
- Nivel medio.
- Nivel alto.

Es de señalar que estos niveles de seguridad son acumulativos, es decir, la aplicación del nivel alto, abarca al nivel medio y básico, los que serán aplicados dependiendo del tipo de dato personal objeto de tratamiento.

Nivel	Tipo de Dato	Aspectos que comprende esa medida de seguridad, esto en los términos del inciso B, del artículo 14 de la Ley		
		Nivel Básico	Nivel Medio	Nivel Alto
Básico	Todos los Datos Personales	• Documento de seguridad; • Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales; • Registro de incidencias; • Identificación y autentificación; • Control de acceso; • Gestión de soportes, • Copias de respaldo y recuperación.		
Medio	La relativa a Infracciones administrativas o penales. Datos personales de tipo hacendario. Datos personales patrimoniales. Datos personales financieros. Aquella información que a través de ella se pueda obtener una evaluación de la personalidad.		• Responsable de seguridad. • Auditoria. • Control de acceso físico. • Prueba de datos reales.	
Alto	Toda aquella información relacionada a los datos sensibles, tales como: • Ideología. • Religión. • Creencias. • Afiliación política. • Origen racial o étnico. • Vida sexual. Dentro de este nivel, también se deberán incluir todos aquellos datos recabados con fines: • Policiales. • Seguridad. • Prevención del delito. • Investigación del delito. • Persecución del delito.			• Distribución de soportes. • Registro de acceso. • Telecomunicaciones.

No se debe perder de vista, como señaló Isabel Davara en la "Ley de Protección de Datos Personales para el Distrito Federal Comentada", que al tener un "… registro de un nivel superior, todo el […] sistema de datos queda declarado del nivel superior"[81], sin importar que sólo contenga un dato que merezca esa protección.

Una de las piezas fundamentales dentro de los niveles de seguridad la localizamos en el nivel básico, que es el documento de seguridad, el cual es un instrumento de carácter confidencial[82]; puede ser definido en los términos de la Guía para la Elaboración de un Documento de Seguridad, publicada por el Instituto Federal de Acceso a la Información y Protección de Datos, como aquel instrumento que:

"… contiene las medidas de seguridad administrativa, física y técnica aplicables a sus sistemas de datos personales con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información personal que éstos contienen…"[83].

De lo anterior, como sigue apuntando dicho órgano garante, el documento de seguridad tiene como propósito identificar el tipo de datos personales que contiene cada uno de los sistemas, los servidores públicos que intervienen dentro del tratamiento de esa información, y las medidas de seguridad previamente enlistadas. No es de olvidar que, de conformidad con el numeral 16, fracción I, inciso a), de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, las disposiciones contempladas en el documento de seguridad son obligatorias para todas las personas que intervienen en el procesamiento de los datos, así como para las personas que en virtud de un servicio tengan acceso al sistema.

Ahora bien, la finalidad última del documento de seguridad se encuentra "… dirigida a que el tratamiento de los datos personales contenidos en los Sistemas […] sean tratados de conformidad con los principios establecidos en

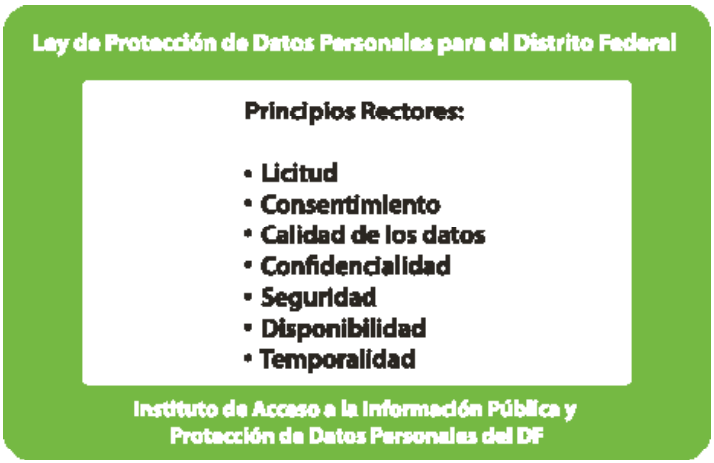
[81] Davara, Isabel "Ley de Protección de Datos Personales para el Distrito Federal Comentada", Gobierno de la Ciudad de México, Secretaría de Gobierno, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, Asamblea Legislativa del Distrito Federal, Tribunal Superior de Justicia del Distrito Federal, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, México D.F. 2010, p. 109

[82] Artículo 15 de la Ley de Protección de Datos Personales para el Distrito Federal.

[83] Guía para la elaboración de un Documento de seguridad v1.4, Instituto Federal de Acceso a la Información y Protección de Datos, 9 de Julio de 2009, p. 5.

Al respecto, los Lineamientos para la Protección de Datos Personales del Distrito Federal definen, en el numeral 3, fracción VI, al Documento de Seguridad como aquel instrumento "… que establece las medidas y procedimientos administrativos físicos y técnicos de seguridad aplicables a los sistemas de datos personales necesarios para garantizar la protección, confidencialidad, integridad y disponibilidad de los datos contenidos en dichos sistemas".

el artículo 5 de la..."[84] Ley de Protección de Datos Personales para el Distrito Federal, los cuales, recordando, son:



En específico, este documento se encuentra relacionado íntimamente con los principios de confidencialidad y de seguridad de los datos personales, esto en virtud de que, como hemos observado, este instrumento tiende a garantizar, de una u otra forma, la integridad de los datos personales objeto de tratamiento.

El documento de seguridad se encuentra conformado por:

- Nombre del sistema[85].
- Cargo y adscripción del responsable[86].
- Ámbito de aplicación[87].

[84] Instituto de Acceso a la Información Pública y Protección de Datos Personales, Dirección de Protección de Datos Personales, "Curso documento de seguridad", expuesto en noviembre de 2011, en el aula de capacitación del Instituto de Acceso a la Información Pública del Distrito Federal; México D.F.

[85] Numeral 16, fracción I, inciso a) de los Lineamientos para la Protección de Datos Personales del Distrito Federal.

[86] El responsable, es definido en los términos del numeral 3, fracción XVI de los citados Lineamientos como "… [e]l servidor público de la unidad administrativa a la que se encuentre adscrito el sistema de datos personales, designado por el titular del ente público, que decide sobre el tratamiento de datos personales, así como el contenido y finalidad de los sistemas de datos personales".

[87] El documento de seguridad deviene de un sistema de datos personales, por lo que, en éste rubro, se deberá indicar a qué sistemas de datos personales es aplicado ese instrumento. Es de aclarar que puede existir un documento de seguridad para dos o más sistemas, siempre y cuando éstos tengan el mismo nivel de seguridad y tengan el mismo responsable; lo anterior, de conformidad con lo expuesto por la Dirección de Datos Personales del órgano garante de la Ley del D.F.; asimismo, se debe indicar si se trata de un sistema automatizado o manual, y el nivel de seguridad aplicable.

- Estructura y descripción del sistema de datos personales[88].
- Especificación de la categoría de datos personales objeto de tratamiento[89].
- Funciones y obligaciones de las personas que intervienen en el tratamiento de los datos personales.
- Las medidas, normas, procedimientos que son empleados para garantizar la integridad del sistema, las cuales dependerán del nivel de seguridad empleado, de conformidad con la Ley y los lineamientos citados.
- Los procesos internos que serán empleados para la notificación, gestión y respuesta de una incidencia ocurrida en el sistema de datos personales[90].
- Los procesos para la realización de las copias de respaldo y recuperación[91].
- Cargo y adscripción del responsable de seguridad[92].
- Auditorías[93].

[88] En este apartado, según lo expuesto por la Dirección de Datos Personales del Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, en los cursos impartidos en el mes de noviembre de 2011, debería contener: la finalidad del tratamiento, el origen de la información, el procedimiento para su obtención, la identificación de los datos del sistema, unidad administrativa responsable, los nombres del encargado y usuarios, origen, destino, interrelación, tiempo de conservación, normatividad aplicable al sistema, cesión (sí se encuentra contemplada), y el nivel de seguridad aplicable.

[89] Las categorías de los datos personales las podemos localizar en los Lineamientos para la Protección de Datos Personales en el Distrito Federal.

[90] Retomando lo expuesto por la Dirección de Datos Personales en la presentación "Curso documento de seguridad", en el mes de Noviembre de 2011, en el aula de Capacitación del Instituto de Acceso a la Información Pública y Protección de Datos Personales, una incidencia, es:

"Cualquier incumplimiento de las normas desarrolladas en el Documento de Seguridad.

"Cualquier anomalía que afecte o pueda afectar a la seguridad los datos de carácter personal en el Sistema.

"Las incidencias deben ser documentadas para delimitar responsabilidades, estableciendo procedimientos que cuenten con un registro."

Por lo que, el documento de seguridad debe contemplar los procesos para dejar evidencia de cualquier incidencia.

[91] En el documento de seguridad se establecerá el proceso (en los términos del numeral 16, fracción I, inciso g, de los Lineamientos) mediante el cual se realizará el respaldo de la información. En el caso de que el sistema de datos personales se encuentre "… en soporte físico, se procurará que el respaldo se efectúe mediante la digitalización de los documentos"; en el supuesto que se encuentren los datos en formato electrónico "… se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida involuntaria o destrucción accidental…".

[92] El responsable de seguridad es designado por el Responsable del SDP, y se encargará de "… coordinar y controlar las medidas…" definidas en el documento de seguridad; lo anterior, con base en el numeral 16, fracción II, inciso a), de los Lineamientos para la Protección de Datos Personales en el Distrito Federal.

[93] Las auditorías se efectúan desde el nivel medio, las cuales deben ser realizadas por personal interno o externo, y en el informe de resultados que se arroje a raíz de este proceso, se:

"… deberá dictaminar sobre la adecuación de las medidas de seguridad previstas en los Lineamientos, así como en las

- Control de acceso[94].
- Pruebas con datos reales[95].
- Distribución de soporte[96].
- Registro de acceso[97].
- Telecomunicaciones[98].

recomendaciones, que en su caso, haya emitido el Instituto. Además, deberá identificar sus deficiencias y proponer las medidas preventivas, correctivas o complementarias necesarias…"

Lo anterior, en los términos del numeral 16, fracción II, inciso b), de los Lineamientos para la Protección de Datos Personales en el Distrito Federal.

Es decir, y tomando como referencia la Guía de Seguridad de Datos, publicada por la Agencia Española de Protección de Datos Personales, en el documento de seguridad, se debe establecer el objetivo de la auditoría, la determinación del alcance de la auditoría, la planificación, recolección de datos, y evaluación de los resultados; así mismo, se debe contemplar las formas de notificación del informe de resultados al Instituto de Acceso a la Información Pública y Protección de Datos Personales.

[94] En términos del multicitado numeral 16, fracción II, inciso c), en el documento de seguridad se debe establecer los mecanismos para garantizar que el acceso se realice exclusivamente por el personal que se encuentra facultado para ello. Ahora bien, en términos de la Guía para la elaboración de un documento de seguridad V1.4, expedida por el Instituto Federal de Acceso a la Información y Protección de Datos, abarca, entre otros elementos, la "… gestión de acceso de los usuarios, control de acceso a redes, control de acceso a sistemas operativos y control de acceso a las aplicaciones y a la información…" (pag.7); agrega en la página 10 de la citada Guía que el control de acceso es una medida "… de seguridad que permite el acceso únicamente a quien está autorizado para ello y una vez que se ha cumplido con el procedimiento de identificación y autenticación…", se debe: "a) Identificar consiste en tomar conocimiento de que una persona es quien dice ser. Lo anterior se logra, por ejemplo, con una identificación que tenga validez oficial y en un ambiente electrónico con el nombre de usuario que se introduce al momento de ingresar al sistema (login). b) Autentificar (o autenticar) a una persona se refiere a comprobar que esa persona es quien dice ser. Ello se logra cuando se cotejan uno o más datos en dicha identificación oficial contra (i) los datos en alguna otra identificación, documento, certificado digital (como el de la firma electrónica) o dispositivo que tenga la persona, (ii) los datos que sepa o tenga memorizados (su firma autógrafa o su contraseña, por ejemplo) o (iii) una o más características que coincidan con lo que es dicha persona (fotografía o huella dactilar, por ejemplo). c) Autorizar se refiere al acceso que se le permite a la persona que se ha identificado y autenticado apropiadamente. Esto depende del o de los permisos que le conceda el responsable de autorizar los accesos".

[95] Esto implica que en el documento de seguridad se deben plantear las acciones que lleve a cabo el Responsable tendientes a: "… verificar la correcta aplicación y funcionamiento de los procedimientos para la obtención de copias de respaldo y de recuperación de los datos, anteriores a la implantación o modificación de los sistemas informáticos que traten sistemas de datos personales, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de datos tratados. Si se realizan pruebas con datos reales, se elaborará con anterioridad una copia de respaldo", esto con fundamento en el numeral 16, fracción II, inciso d) de los Lineamientos para la Protección de Datos Personales en el Distrito Federal.

[96] Implica que la operación por la cual se lleve a cabo la transferencia de un sistema de datos personales que se encuentren en un soporte electrónico, debe realizarse en los términos del numeral 16, fracción III, inciso a), de los Lineamientos.

[97] En este apartado se deben identificar los mecanismos que serán empleados en los accesos realizados a los sistemas cuyo nivel de seguridad sea alto (numeral 16, fracción III, inciso b, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal)

[98] Tomando como referencia, lo establecido en el numeral 16, fracción III, inciso c), de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, la Guía de Seguridad de Datos emitida por la Agencia Española de Protección de Datos Personales, las telecomunicaciones sólo son aplicables a los sistemas de datos personales electrónicos y que son o

La Ley de Protección de Datos Personales para el Distrito Federal, señala que estos niveles de seguridad son los mínimos exigibles, por lo que abre la posibilidad de que el ente público, dependiendo su naturaleza, opte por la adopción de niveles aún mayores, para garantizar el cumplimiento de los principios contemplados en ella. Es de enfatizar que los sistemas de datos personales no se encuentran aislados y tienen una interacción con otra información que sea administrada, generada, o se encuentre en posesión del ente público, por lo que si esa información tiene mayores estándares de seguridad, al sistema de datos personales con el que tiene interacción, también debería complementarse con esos estándares.

En ese orden de ideas, existen diversos estándares de seguridad, por ejemplo, ISO 27000 y sus familias (ISO 2007:2009), que son "… un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña…"[99].

Sin embargo, la adopción de un nivel mayor de seguridad en los sistemas de datos personales dependerá exclusivamente del ente público, en específico, del responsable, quien es el que decide sobre el contenido, finalidad y, por ende, los niveles de seguridad aplicables al sistema que se encuentren bajo su tutela y resguardo.

2.3 Tratamiento de los datos personales

Tomando como referencia la Directiva 95/46/CE, podemos decir que el tratamiento de los datos implica:

"… 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"[100]

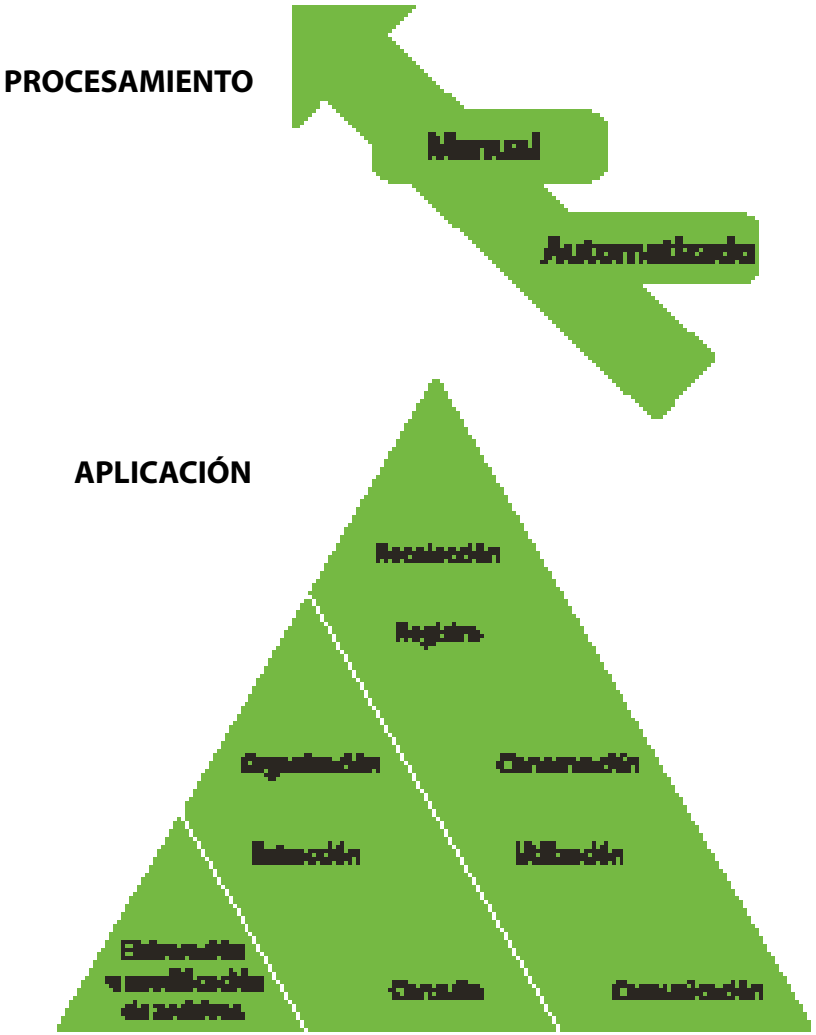
De la anterior definición, podemos desprender diversos elementos:

---

serán objeto de una transmisión por medio de redes públicas (por ejemplo internet) o inalámbricas (acces point, routers, etc. [red privada]), cuya transmisión deberá ser realizada de manera cifrada o utilizando cualquier mecanismo que asegure que los datos personales objeto de transferencia no sean inteligibles ni manipulables por terceros, es decir, que se garantice el cumplimiento de los principios de calidad y confidencialidad. Por lo que, en el documento de seguridad se deberán plasmar esos procedimientos que garanticen lo anterior.

[99] http://www.iso27000.es/iso27000.html

[100] Artículo 2.b. Directiva 95/46/CE



Como se puede observar, el tratamiento de los datos personales abarca todas las posibles acciones que podría realizar el ente público dentro de un sistema de datos personales. Ahora bien, para cumplir con el principio de licitud, dentro del tratamiento de los datos personales, no sólo bastaría observar lo dispuesto en la Ley de Protección de Datos Personales para el Distrito Federal, sino que es necesario que las personas que intervengan en ella ajusten el proceso a la normatividad que dio origen al sistema de datos personales.

La Ley de Protección de Datos Personales para el Distrito Federal dedica un capítulo íntegro al tratamiento de los datos personales, el cual, de una u otra forma, hemos estado abordando a lo largo de esta lectura, pero es de resaltar algunos puntos esenciales, entre éstos destaca la denuncia contemplada en el artículo 17, que señala:

"… En los supuestos de utilización o cesión de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de derechos de las personas, el Instituto podrá requerir, a los responsables de los sistemas de datos personales, la suspensión en la utilización o cesión de los datos. Si el requerimiento fuera desatendido, mediante resolución fundada y motivada, el Instituto podrá bloquear tales sistemas, de conformidad con el procedimiento que al efecto se establezca. El incumplimiento a la inmovilización ordenada por el Instituto será sancionado por la autoridad competente de conformidad por la Ley Federal de Responsabilidades de los Servidores Públicos".

Recordemos que el tratamiento de los datos personales debe regirse bajo los principios contemplados en la Ley de Protección de Datos Personales para el Distrito Federal, por lo que, para actualizar esa hipótesis, es necesario que se ponga en riesgo un bien jurídico mayor del particular, que el perseguido por el ente público con el tratamiento de la información.

Sin embargo, al tratarse de una ponderación de bienes, es necesario que el Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal proceda con cierta cautela, por tal motivo, los Lineamientos de Protección de Datos Personales en el Distrito Federal establecen que, en una primera instancia, una vez recibida la denuncia, deberá requerir al ente público presuntamente responsable del tratamiento ilícito, que suspenda el tratamiento y rinda un informe en el que deberá indicar las medidas que ha adoptado para la suspensión[101]; una vez rendido el informe, el Instituto deberá ponderar esos bienes en juego, analizando cuidadosamente la normatividad aplicable a cada caso, así como los argumentos vertidos por las partes[102]. Una vez teniendo los elementos de convicción, el órgano garante de la materia emitirá una resolución –esto dentro de los 15 días hábiles siguientes a la presentación de la denuncia- en la que podrá:

"**I.** Emitir recomendaciones en las que requiera al ente público se subsanen

[101] Dado el caso de que el ente público desobedezca la orden de suspensión del tratamiento, el órgano garante puede ordenar la inmovilización del sistema de datos personales de que se trate; esto como lo señala el numeral 30 de los Lineamientos para la Protección de Datos Personales del Distrito Federal.

[102] Numeral 29, Lineamientos para la Protección de Datos Personales del Distrito Federal.

las irregularidades detectadas, mismas que tendrán que ser solventadas dentro del plazo y condiciones que al efecto se establezcan;

"**II.** Requerir al responsable la cancelación o rectificación de determinados datos contenidos en el sistema que corresponda;

"**III.** Requerir que el responsable modifique el sistema a efecto de que se ajuste a lo establecido en la Ley y demás normativa aplicable; y

"**IV.** Determinar que no hay elementos que permitan establecer que se actualizan los supuestos a que hace referencia el artículo 17 de la Ley."[103]

Agrega el numeral 29 de los multicitados Lineamientos, que, en caso de las hipótesis señaladas en las fracciones I al IV, en esa resolución podrá señalar el levantamiento de la inmovilización señalada previamente, y en el supuesto de que se hubiere configurado alguna infracción a lo establecido en la Ley de Protección de Datos Personales para el Distrito Federal, el Instituto deberá dar vista al órgano interno de control del ente público correspondiente, esto en los términos del último párrafo del numeral 30 de los Lineamientos para la Protección de Datos Personales del Distrito Federal. Es de señalar, que el Instituto podrá ordenar la visita de inspección al ente público, con el último fin de evaluar su cumplimiento.

Otro aspecto que resalta la Ley de Protección de Datos Personales para el Distrito Federal, sobre el procesamiento de los datos personales, son los datos personales que son tratados por el sector salud. El artículo 18, en la parte que nos interesa para este apartado, señala:

"… El tratamiento de los sistemas de datos personales en materia de salud, se rige por lo dispuesto en la Ley General de Salud, la Ley de Salud para el Distrito Federal y demás normas que de ellas deriven. El tratamiento y cesión a esta información obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera tal que se mantenga la confidencialidad de los mismos, salvo que el propio paciente haya dado su consentimiento para no separarlos…"

Como podemos observar, el tratamiento de los datos personales de esa índole se regirá por lo dispuesto en las normas especializadas en la materia; la Ley General de Salud, cuenta con diversos artículos que ilustran la forma en que los sujetos obligados de esa norma deben tratar los datos personales. El primer artículo, que es importante traer al presente estudio, es el concerniente al

[103] Op. Cit

tratamiento de datos del genoma humano[104], que para la Ley de Protección de Datos Personales del Distrito Federal y sus Lineamientos sería tipificado como un dato personal especialmente protegido[105], el artículo 103 bis 3 de la Ley General de Salud, que establece:

"Todo estudio en este campo deberá contar con la aceptación expresa de la persona sujeta al mismo o de su representante legal en términos de la legislación aplicable.

"En el manejo de la información deberá salvaguardarse la confidencialidad de los datos genéticos de todo grupo o individuo, obtenidos o conservados con fines de diagnóstico y prevención, investigación, terapéuticos o cualquier otro propósito, salvo en los casos que exista orden judicial"

Acoplando lo señalado en ese artículo al "lenguaje" o terminología empleada por la Ley de Protección de Datos Personales del Distrito Federal, la recolección del dato relativo al genoma humano debe ser obtenida por medio del consentimiento expreso del titular de esa información o, en su defecto, del representante legal. Asimismo, el manejo de los expedientes que contengan esa información deberá ser realizado bajo confidencialidad; sin embargo, como hemos observado con anterioridad, el principio de confidencialidad no es absoluto, ya que, ante la existencia de un mandato judicial (previamente fundado y motivado), el ente público que detente esa información deberá proporcionarla a la autoridad requirente, y, si fuere solicitado, deberán estar asociados los datos personales "generales" con los clínico-asistenciales; en caso contrario, siguiendo la lógica planteada por el artículo 18, deberá ser entregada de manera disociada.

Dentro de la idea planteada en el párrafo anterior, el artículo 103 bis 4 de la Ley General de Salud señala, en el rubro de la confidencialidad, que el titular de ese dato personal o su representante legal es el que puede determinar que le sean informados los resultados de los exámenes practicados; lo que inhibe la

[104] El genoma humano, en términos del artículo 103 bis, de la Ley General de Salud, es definido como "… el material genético que caracteriza a la especie humana y que contiene toda la información genética del individuo, considerándosele como la base de la unidad biológica fundamental del ser humano y su diversidad…".

[105] Recordemos que el fin último de la protección de este tipo de datos personales es evitar actos de discriminación; en tal sentido el artículo 103 bis 2, primer párrafo, señala: "…Nadie podrá ser objeto de discriminación, conculcación de derechos, libertades o dignidad con motivo de sus caracteres genéticos…", lo que pone a esta disposición en concordancia con el artículo 1º de nuestra Carta Magna, que señala en la parte conducente:
"… Queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias sexuales, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas…". He aquí la importancia de la protección de los datos personales, ya que, por medio de este tipo, junto con los de ideología, afiliación sindical, política, etc., se pueden generar actos discriminatorios en contra del titular de esa información.

posibilidad del tratante de las secuencias del ADN de revelar esa información a terceros o incluso al propio interesado, sin que exista previamente el consentimiento; exceptuando claro está, la hipótesis de la existencia de una orden judicial.

Ahora bien, otro de los puntos a resaltar dentro de la normatividad que regula los datos personales de índole clínico-asistencial, se encuentra la NOM-040-SSA2-2004 en "materia de información en salud", la cual establece que cada uno de los niveles administrativos que intervengan en el tratamiento de la información que sea almacenada dentro del Sistema Nacional de Información en Salud, deben "… adoptar las medidas necesarias para garantizar la seguridad de la información, evitar su alteración, pérdida, transmisión y acceso no autorizado… "[106]; es decir, en la información que sea almacenada y tratada por medio del Sistema se debe cumplir con algunos estándares que garanticen su integridad, lo que se traduce en el principio de seguridad, contemplado en la Ley de Protección de Datos Personales para el Distrito Federal.

El numeral 13.5 de la citada Norma Oficial Mexicana establece, dentro de la lógica ya planteada desde el análisis somero de la Ley General de Salud, que el manejo de la información estará sujeta al principio de confidencialidad. Es de resaltar que el término de confidencialidad empleado se encuentra circunscrito a lo establecido en el artículo 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que señala:

> "***Artículo 18.*** Como información confidencial se considerará:
>
> "**I.** La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y
>
> "**II.** Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.
>
> "No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público".

El expediente clínico, que es un "… conjunto de documentos escritos, gráficos e imagenológicos o de cualquier otra índole, en los cuales el personal de salud, deberá hacer los registros, anotaciones y certificaciones correspondientes a su intervención…"[107], contiene en gran parte, datos personales sensibles, los cuales en los términos de la NOM-168-SSA1-1998, numeral 5.6, deben ser tratados por el personal de salud bajo confidencialidad; y previo al tratamiento

[106] Numeral 13.4 de la NOM-040-SSA2-2004 en materia de información en salud.

[107] Numeral 4.4 de la NOM-168-SSA1-1998 del Expediente Clínico.

médico del usuario[108], se debe requerir el consentimiento informado para su tratamiento (el cual puede ser revocado hasta antes del inicio del procedimiento que es autorizado).

Dicha aceptación, debe obrar en las "Cartas de consentimiento bajo información", las cuales son definidas en los términos del numeral 4.2, de la NOM citada, como:

"… los documentos escritos, signados por el paciente o su representante legal, mediante los cuales se acepte, bajo debida información de los riesgos y beneficios esperados, un procedimiento médico o quirúrgico con fines de diagnóstico o, con fines diagnósticos, terapéuticos o rehabilitatorios…".

Se trae a colación esta definición, en virtud de que se dará tratamiento a diversos datos sobre salud, que en términos del numeral 5, fracción VIII de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, se conforman, entre otros, por la información relativa a las intervenciones quirúrgicas; las cuales, como observamos en párrafos anteriores, se asientan en el expediente clínico[109].

Otro de los aspectos importantes de llamar la atención, dentro de la fase del tratamiento de los datos personales, radica en el tiempo de conservación; en ese sentido, el primer párrafo del artículo 19 de la ley de la materia desarrolla un poco más el principio de temporalidad[110], al señalar que:

"Los sistemas de datos personales que hayan sido objeto de tratamiento, deberán ser suprimidos una vez que concluyan los plazos de conservación establecidos por las disposiciones aplicables, o cuando dejen de ser necesarios para los fines por los cuales fueron recabados".

Este párrafo plantea dos hipótesis: la primera de ellas implica que el dato personal debe ser dado de baja cuando así lo señale una normatividad específica; por ejemplo, el numeral 5.3 de la NOM-168-SSA1-1998 señala que los expedientes clínicos serán dados de baja al término de cinco años, el cual, será determinado a partir de la fecha del último acto médico.

La segunda hipótesis planteada se encuentra sujeta al cumplimiento de

[108] Entendido este como "… toda aquella persona, paciente o no, que requiera y obtenga la prestación de servicios de atención médica…" (numeral 4.11 de la NOM-168-SSA1-1998).

[109] Para obtener mayor información sobre el tratamiento de los de los datos personales, obrantes en el expediente clínico se recomienda analizar la NOM-168-SSA1-1998 del expediente clínico.

[110] Recordemos que, el principio de temporalidad se encuentra señalado en el artículo 5 de la Ley de Protección de Datos Personales para el Distrito Federal, y señala que "… datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados".

la finalidad del tratamiento, es decir, cuando dicho dato personal haya consumado el objeto por el que fue recolectado debe ser dado de baja del sistema correspondiente.

No es de soslayar que un sistema de datos personales es, en pocas palabras, un conjunto organizado de archivos, por consiguiente, también los entes públicos, antes de proceder a dar de baja, deben observar lo dispuesto en el Catálogo de Disposición Documental, el cual es definido por la Ley de Archivos del Distrito Federal, como el:

"[r]egistro general y sistemático elaborado por la unidad coordinadora de archivos y aprobado por el COTECIAD de cada ente público, en el que se establece en concordancia con el cuadro general de clasificación archivística, los valores documentales, los plazos de conservación, la vigencia documental, la clasificación de la información pública o de acceso restringido ya sea reservada o confidencial y su destino"[111].

Es decir, el ente público debe observar en todo momento el ciclo vital de los documentos en los que obran los datos personales, para determinar, en una primera instancia, el cumplimiento de la finalidad y posteriormente la temporalidad de su conservación, fijada no sólo por el fin del tratamiento, sino también por la ley y/o norma específica que le dio origen al sistema de datos personales, lo dispuesto en la Ley de Archivos del Distrito Federal, y/o lo dispuesto en el instrumento jurídico que dio origen a la cesión, para poder determinar, una vez terminado los "… tiempos en que pueda exigirse algún tipo de responsabilidad[es]", la cancelación y posterior supresión del sistema[112].

Otro aspecto a resaltar dentro del tratamiento de los datos personales son las transferencias nacionales a otras instituciones a nivel estatal o federal, en cuyo caso, el ente público debe:

"… asegurarse que tales instituciones garanticen que cuentan con niveles de protección, semejantes o superiores, a los establecidos en esta Ley y, en la propia normatividad del ente público de que se trate…"[113]

En tal supuesto el ente público debe solicitar al cesionario, un documento por medio del cual garantice la protección del dato personal objeto de transferencia, que debe equivaler al nivel de seguridad plasmado en el Documento Seguridad. Es de subrayar que el cesionario quedará sujeto a las mismas responsabilidades fijadas por la Ley de Protección de Datos Personales

[111] Artículo 4º., Ley de Archivos del Distrito Federal.

[112] Numerales 31 y 32 de los Lineamientos para la Protección de Datos Personales del Distrito Federal.

[113] Artículo 20, Ley Protección de Datos Personales para el Distrito Federal.

para el Distrito Federal y demás normatividad aplicable[114].

Ahora bien, cuando el cesionario se encuentre en el extranjero, el ente público deberá efectuar la transferencia en los términos de la legislación federal aplicable al caso concreto, y, al igual que en el caso de las cesiones señaladas en el párrafo anterior, deberá asegurarse que el cesionario garantice los niveles de seguridad que son aplicados a esos datos personales; esto en los términos del segundo párrafo del artículo 20, de la Ley de Protección de Datos Personales del Distrito Federal. Bajo este contexto, si se trataré de una transferencia a Estados Unidos de Norteamérica, el ente público deberá observar lo dispuesto en la Ley de Privacidad de ese país; en el supuesto de que se trataré de una transferencia al viejo continente, se deberá observar no sólo la ley aplicable en el país receptor, sino que también lo dispuesto en las Directivas analizadas anteriormente.

Como hemos mencionado, el tratamiento de los datos personales, no sólo puede ser realizado directamente por el ente público que los detenta, sino que también lo puede realizar por medio de un usuario[115], bajo tal hipótesis, el ente debe tener previamente firmado un contrato (escrito o por cualquier otro medio que permita verificar la relación contractual), el cual, entre otros elementos, debe contener los niveles de seguridad que deberán implementarse para el tratamiento, y el señalamiento del destino que tendrán los datos personales, una vez terminado el contrato, es decir, deberá indicar si el usuario debe regresar los datos personales al ente público o si debe proceder a su baja[116].

2.4 El procedimiento de los Derechos ARCO y los principios inmersos

Una de las piezas fundamentales, como se observó cuando analizamos las Directivas y algunas leyes extranjeras, para el adecuado funcionamiento de la autodeterminación informativa son los derechos de Acceso, Rectificación, Cancelación y Oposición. Estos derechos se encuentran expresamente reconocidos tanto en el artículo 16 constitucional, como en la Ley de Protección de Datos Personales para el Distrito Federal. Estos derechos permiten al titular de la información:

[114] Numeral 33 de los Lineamientos para la Protección de Datos Personales del Distrito Federal.

[115] El usuario es definido en el artículo 4 de la Ley de Protección de Datos Personales para el Distrito Federal, como "[a]quel autorizado por el ente público para prestarle servicios para el tratamiento de datos personales".

[116] Numeral 36, Lineamientos para la Protección de Datos Personales del Distrito Federal.

A	Derecho de Acceso	Procede para "… solicitar y obtener información de los datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las cesiones realizadas o que se prevén hacer…" (Artículo 27, de la Ley de Protección de Datos Personales para el Distrito Federal).
R	Derecho de Rectificación	Procede cuando los "…datos resulten inexactos o incompletos, inadecuados o excesivos…" (Artículo 28, de la Ley de Protección de Datos Personales para el Distrito Federal).
C	Derecho de Cancelación	Procede "… cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en los lineamientos emitidos por el Instituto, o cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente …" (Artículo 29, de la Ley de Protección de Datos Personales para el Distrito Federal).
O	Derecho de Oposición	Procede "… en el supuesto en que los datos se hubiesen recabado sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario…" (Artículo 30, de la Ley de Protección de Datos Personales para el Distrito Federal).

2.4.1 Principios

Dentro del derecho de acceso a datos personales, podemos señalar que se encuentra inmerso el deber o principio de información; lo anterior, en virtud de que no todos los datos personales que se encuentran actualmente bajo el tratamiento fueron recolectados una vez entrada en vigencia de la Ley de Protección de Datos Personales para el Distrito Federal, por lo que el ente público no se encontraba obligado a dar cumplimiento a lo dispuesto en el numeral 12 de los multicitados Lineamientos. Es decir, este derecho permite al titular de la información tener conocimiento de la existencia de un tratamiento, y los mecanismos empleados para la recolección de éstos.

Una forma de controlar nuestros datos personales que se encuentren en posesión de los entes públicos es por medio del derecho a la rectificación, el cual se actualiza cuando los datos personales no respondan necesariamente a la realidad del titular de esos datos, o no se encuentren adecuados al objeto de tratamiento, o resulten descomunales para éste, por lo tanto, el principio que presuntamente se vería afectado sería el de calidad de los datos, que implica que los datos personales son adecuados, pertinentes y responden a la realidad del titular de estos.

Es importante resaltar, que en este derecho se considera que los datos personales reunirán las últimas características señaladas, cuando se trate de información que: "…reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos…"[117].

[117] Artículo 28. Op. Cit.

De la definición aportada en el cuadro anterior, podemos desprender diversas hipótesis de procedencia del derecho de cancelación, las cuales a saber son:

No se encuentre adecuado el tratamiento a lo dispuesto en la ley o lineamientos.
Se halla ejercitado previamente el derecho de oposición.

En la primera hipótesis, podemos señalar que el principio que se encuentra disminuido o dejó de estar adecuado a éste es el de licitud; esto tomando como referencia lo estipulado en el artículo 5 de la multicitada Ley, que señala, en la parte conducente, que el ente público sólo podrá dar tratamiento al dato personal cuando obedezca a sus atribuciones. Ahora bien, observando lo dispuesto en el numeral 19, fracción I, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, también se puede afirmar que otro de los principios que pudieran estar disminuidos, cuando se ejercita el derecho de cancelación, podría ser el de finalidad, que, recordando lo dispuesto por la Resolución 45/95 de las Naciones Unidas, implica:

> "La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que:
>
> "Todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados;
>
> "Ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados;
>
> "El período durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados.
>
> …"[118]

De lo anterior, se infiere que también podría proceder este derecho cuando el ente público no haya cumplido con el principio de información, es decir, no haya puesto a la vista del particular la leyenda contemplada en el artículo 9 de la Ley y, por ende, también se podría ver inmiscuido el principio del consentimiento.

[118] Resolución 45/95 Principios rectores aplicables a los ficheros computarizados de datos personales. (Resolución 45/95 de 14 de diciembre, de la Asamblea General de las Naciones Unidas). http://www.informatica-juridica.com/anexos/Principios_rectores_aplicables_ficheros_computarizados_datos_personales_Resolucion_45_95_14_diciembre_Asamblea_General_Naciones_Unidas.asp

La segunda hipótesis planteada se actualiza cuando el ente público haya contestado de manera afirmativa el derecho de oposición, que se materializa cuando el titular de los datos solicita al ente público que:

1. No se lleve a cabo el tratamiento.
2. Cese el tratamiento[119].

Bajo esos supuestos, podemos determinar que el derecho de oposición se puede ejercitar en dos tiempos, el primero cuando da inicio al procesamiento del dato y, el segundo, durante el tratamiento del dato personal; ejercitable bajo la única causal de procedencia, consistente en la ausencia del consentimiento del titular de esa información.

El efecto del ejercicio de estos últimos derechos, cuando la respuesta del ente público hubiere sido positiva a los intereses del particular, es el bloqueo; al respecto el artículo 29 de la Ley de Protección de Datos Personales para el Distrito Federal establece la obligación del ente público de mantenerlos en sus archivos hasta que hayan fenecido las "… responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el plazo deberá procederse a su supresión, en términos de la normatividad aplicable…", observando en todo momento lo señalado en lo estudiado en la última parte del apartado anterior.

2.4.2 Procedimiento

Antes de iniciar el estudio del presente apartado, es necesario puntualizar que el ejercicio de los derechos ARCO no se encuentra condicionado al ejercicio de alguno de ellos previamente, es decir, para el ejercicio del derecho de rectificación, no será necesario que previamente el particular haya utilizado el derecho de acceso[120], así mismo, su ejercicio sólo podrá ser realizado por el titular de los datos personales, o en su defecto por su representante legal[121].

El derecho a la protección de datos personales, regulado por la Ley multicitada, para su ejercicio, se basa, en parte, en la infraestructura creada por la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, en específico, en la figura de la Oficina de Información Pública (OIP), ante la cual se deberá presentar la solicitud de alguno de los derechos ARCO.

Los medios y formas para la presentación de las solicitudes ARCO, son:

[119] Numeral 51 de los Lineamientos para la Protección de Datos Personales del Distrito Federal.
[120] Artículo 26, Op.cit.
[121] Numeral 42 de los Lineamientos para la Protección de Datos Personales del Distrito Federal.

Medios	Formas
INFOMEX	Electrónica.
TEL-INFODF	Verbal.
PRESENCIAL (ante la OIP)	Por escrito físico, verbal, por correo electrónico.

Los requisitos formales de procedencia de las solicitudes ARCO, los localizamos en el artículo 34 de la Ley de Protección de Datos Personales para el Distrito Federal, que a saber son:

- Nombre del ente público.
- Nombre del titular de los datos o en su defecto, el representante legal.
- Descripción de lo requerido.
- Cualquier información que pudiera facilitar la localización de lo requerido.
- Domicilio (físico o electrónico) para recibir notificaciones.
- La modalidad en la que se requiere la información (esto de manera opcional).

Ahora bien, una vez presentada la solicitud ARCO, el ente público debe dar inicio a la sustanciación del requerimiento, sin embargo, si ésta no es precisa o no reúne alguno de los requisitos señalados anteriormente, el ente público, por medio de su OIP, debe prevenir al particular dentro de los 5 días hábiles siguientes, para que, en un término igual, el titular de los datos subsane esa deficiencia. En el caso de que la solicitud se presente de manera verbal ante la propia OIP, en ese momento se debe prevenir al particular, orientándolo de la manera más adecuada para la consecución de ese fin.

Es de señalar que, los entes públicos, durante la sustanciación de la solicitud, deben observar lo dispuesto en los Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales a través del Sistema INFOMEX del Distrito Federal, el cual establece, entre otros elementos, que la personalidad se acreditará al momento en que se entregue la respuesta recaída a la solicitud ARCO, ante la OIP[122].

No se puede perder de vista que, a diferencia del procedimiento equivalente, contemplado en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, las respuestas que se emitan con motivo de una solicitud

[122] Numeral 18, de los Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales a través del Sistema INFOMEX.

ARCO no son entregadas por medio de INFOMEX o algún otro medio de comunicación remota, sino por el medio señalado por el particular; se notificará la disponibilidad de una respuesta con el señalamiento que se encuentra a su disposición en las instalaciones de la OIP, previa acreditación de la personalidad[123].

El artículo 34 de la Ley de Protección de Datos Personales para el Distrito Federal, con relación al numeral 18 de los Lineamientos previamente citados, establece que en el caso de que se hubiere presentado una solicitud de rectificación de datos personales, el particular debe indicar el dato incorrecto y acompañar la documentación que sustente su requerimiento, y dado el supuesto que no se hubiere presentado esta prueba, la OIP sólo contará con 3 días hábiles para requerirle al particular que presente esa probanza.

Una vez realizadas las gestiones internas en el ente público, para satisfacer el requerimiento del particular, y en el caso de que no se hubiere localizado la información en el o los SDP, el ente, por conducto de la OIP, el responsable del sistema de datos personales (en el que se haya buscado el dato) y un representante del órgano interno de control del mismo ente, levantarán una acta circunstanciada, en la que señalarán los sistemas de datos personales que fueron objeto de la búsqueda. Una vez levantada el acta, el ente público notificará la disponibilidad de una respuesta, y, previa acreditación de personalidad, como observamos anteriormente, proporcionará el acta[124] al titular de los datos personales.

Ahora bien, en el caso de que no sea procedente la solicitud ARCO, el ente público debe, en los términos del artículo 36 de la Ley:

"… notificar al peticionario de manera fundada y motivada las razones por las cuales no procedió su petición. La respuesta deberá estar firmada por el titular de la oficina de información pública y por el responsable del sistema de datos personales…"

Cualquier respuesta emitida por el ente público debe ser notificada al particular, dentro de los 15 días hábiles siguientes a los que fue presentada la solicitud ARCO; dado el caso, deberá indicar el costo de reproducción de la información[125], para que, en un plazo no mayor de 10 días hábiles, el titular

[123] Artículo 34. Op. Cit y numeral 18 de los Lineamientos para la Gestión de Solicitudes de Información y de Datos Personales a través del INFOMEX.

[124] Último párrafo, del artículo 32. Op.cit.

[125] Numeral 20, Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales a través del Sistema INFOMEX.

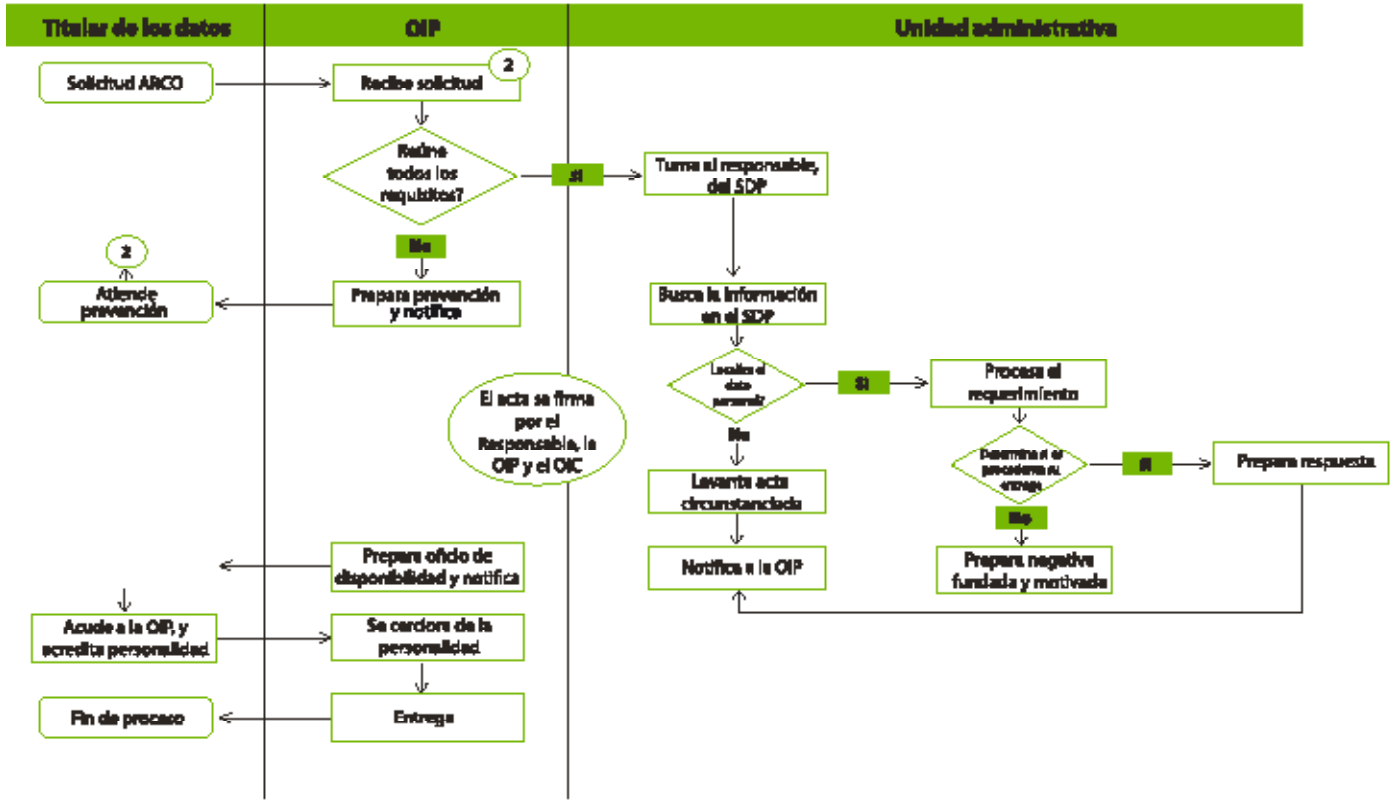
de los datos personales o, en su caso, el representante legal, acrediten la personalidad ante la OIP correspondiente[126].

La acreditación de la personalidad, en los términos del numeral 18 de los Lineamientos para la Gestión de Solicitudes de Información Pública y Protección de Datos Personales, a través del Sistema INFOMEX, será por medio de una identificación oficial, tales como:

- Credencial para votar.
- Pasaporte (vigente).
- Cartilla de servicio militar.
- Cédula Profesional, etc.

En la siguiente gráfica se ejemplifica el procedimiento de una solicitud ARCO:

[126] Numeral 21, Op.cit.


Titular de los datos
OIP
Unidad administrativa
Solicitud ARCO
Recibe solicitud
2
Reúne todos los requisitos?
SI
Turna al responsable del SDP
No
2
Atiende prevención
Prepara prevención y notifica
Busca la información en el SDP
Localiza el dato personal?
SI
Procesa el requerimiento
El acta se firma por el Responsable, la OIP y el OIC
No
Determina si es procedente su entrega
SI
Prepara respuesta
Lavanta acta circunstanciada
No
Notifica a la OIP
Prepara negativa fundada y motivada
Prepara oficio de disponibilidad y notifica
Acude a la OIP, y acredita personalidad
Se cerciora de la personalidad
Entrega
Fin de proceso

2.5 El Recurso de Revisión[127]

El Título Cuarto, Capítulo III, de la Ley de Protección de Datos Personales del Distrito Federal contempla el medio de defensa que tiene el titular de los datos personales ante[128]:

Tomando como referencia el artículo 40 de la Ley en estudio, se puede determinar que los elementos que debe contener el escrito por el que se interponga el recurso de revisión son los establecidos en el artículo 78 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal:

"I. Estar dirigido al Instituto;

"II. El nombre del recurrente y, en su caso, el de su representante legal o mandatario, acompañando el documento que acredite su personalidad, y el nombre del tercero interesado, si lo hubiere;

"III. El domicilio o medio electrónico para oír y recibir notificaciones y en su caso, a quien en su nombre autorice para oírlas y recibirlas; en caso de no haberlo señalado, aún las de carácter personal se harán por estrados;

"IV. Precisar el acto o resolución impugnada y la autoridad responsable del mismo;

"V. Señalar la fecha en que se le notificó el acto o resolución que impugna, excepto en el caso a que se refiere la fracción VIII del artículo 77[129];

"VI. Mencionar los hechos en que se funde la impugnación, los agravios que le cause el acto o resolución impugnada; y

"VII. Acompañar copia de la resolución o acto que se impugna y de la

[127] Para obtener mayor información sobre el proceso sustanciación del recurso de revisión, remitirse a la información proporcionada en el módulo anterior.

[128] Artículo 38, Op.cit.

[129] La fracción VIII del artículo 77 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, señala: "… Contra la falta de respuesta del Ente Obligado a su solicitud, dentro de los plazos establecidos en esta Ley…"

notificación correspondiente. Cuando se trate de solicitudes que no se resolvieron en tiempo, anexar copia de la iniciación del trámite.

…"

Es importante señalar que, en términos de lo señalado en la Ley de Protección de Datos Personales para el Distrito Federal, el procedimiento será sustanciado en los términos de la segunda ley señalada en el párrafo anterior. Bajo lo anterior, podemos determinar que el término para interponer el recurso de revisión será de 15 días hábiles, contados a partir de la entrega de la información sobre la que versa la queja del titular de los datos personales o, en su caso, contados a raíz de la configuración de la omisión.

Ahora bien, una de las piezas fundamentales dentro de este capítulo la localizamos en el artículo 39 de la ley, que plantea tres hipótesis cardinales en este tipo de procedimientos administrativos, que se jactan de regular un Derecho Humano; estas hipótesis son:

1. El Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, durante el proceso de sustanciación, podrá tener acceso al o los sistemas de datos personales en que se encuentre albergada la información objeto de la queja.

2. Las resoluciones que pongan fin al recurso de revisión son inatacables, vía administrativa, para ambas partes.

3. El titular de los datos personales podrá interponer el juicio de amparo ante la resolución que emita el Instituto.

El primer eje cardinal señalado se traduce en la misma facultad de "… acceso que los funcionarios encargados de resguardar los datos personales [lo que resulta] indispensable para que [el Instituto] ejerza de forma completa y apropiada su tarea de supervisión respecto de los entes públicos obligados… "[130].

El segundo eje establece, en pocas palabras, el principio de definitividad de las resoluciones que emita el Instituto, es decir, el ente público no podrá interponer otro recurso administrativo, contemplado en una ley secundaria, para revocar la resolución que no le haya sido favorable.

Ahora bien, el tercer eje cardina, establece la posibilidad que tiene el titular de los datos personales de interponer el juicio contemplado en el artículo 105

[130] Comentario de Carbonell, Miguel; Op.cit. p. 252.

y 107 de la Constitución Política de los Estados Unidos Mexicanos, es decir, el juicio de amparo, cuya procedencia requiere que se haya agotado todo recurso y medio ordinario de defensa, tal como lo señala la siguiente tesis aislada:

PRINCIPIO DE DEFINITIVIDAD. NO PUEDE EXIGIRSE EL AGOTAMIENTO PREVIO DEL RECURSO ORDINARIO, SI EL INTERESADO NO ESTUVO EN POSIBILIDAD MATERIAL DE INTERPONERLO.
El principio de definitividad consiste en que antes de acudir al juicio de garantías deben agotarse todos los recursos y medios ordinarios de defensa existentes. igualmente es conocido que tal principio tiene contadas excepciones, esto es, casos en que no existe la obligación de intentar previamente dichos recursos o medios de defensa (por ejemplo, los amparos en materia penal, tratándose de terceros extraños, cuando se reclame una ley de inconstitucional, etcétera). luego, si para poder interponer el recurso o el medio de defensa respectivo es necesario expresar los agravios que la resolución cause al interesado, es indudable que este no podría formular motivos de inconformidad si acaso no tuvo oportunidad de leer la resolución afectatoria. en la especie, el recurrente sostiene que hizo muchos intentos infructuosos por lograr se le facilitara el expediente a fin de enterarse del contenido del auto que reclama. si se aceptara lo que sustenta el juez federal (que forzosamente debió agotar aquel el recurso ordinario correspondiente), sin atender, como de hecho lo hace este último, la afirmación relativa a la imposibilidad material de tener a la vista la resolución, se privaría al agraviado de la oportunidad de justificar su aserto. consiguientemente, el presente asunto debe ser incluido entre uno de tales casos de excepción, porque no puede exigirse el agotamiento previo del recurso ordinario si acaso el interesado no estuvo en posibilidad de interponerlo.

TERCER TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL TERCER CIRCUITO.
IMPROCEDENCIA 646/96. GUILLERMO RUIZ BECERRIL. 22 DE AGOSTO DE 1996. UNANIMIDAD DE VOTOS. PONENTE: JORGE FIGUEROA CACHO. SECRETARIO: ROBERTO MACIAS VALDIVIA.
SEMANARIO JUDICIAL DE LA FEDERACION Y SU GACETA, NOVENA EPOCA, TOMO IV, OCTUBRE DE 1996, P. 588.

Es importante señalar que el ente público, en los términos del tercer párrafo del artículo 39 de la Ley de Protección de Datos Personales, no podrá interponer este juicio constitucional, en virtud de que:

"… la protección de datos personales en México es un derecho fundamental de acuerdo a lo que señala el artículo 16, párrafo segundo, de la Carta Magna. En ese contexto, resulta evidente que su titular es siempre un particular,

no una autoridad. El amparo es un instrumento de defensa de derechos fundamentales, no de defensa del ámbito de atribuciones de las entidades públicas…"[131]

Como hemos observado hasta este momento, las resoluciones que emita el Instituto y que pongan fin al recurso de revisión son inatacables; sin embargo, las resoluciones no definitivas podrán ser atacadas por el titular de los datos personales, mediante el recurso de revocación[132], regulado en el artículo 89 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, el cual será resuelto por el Pleno del Instituto, y se sujetará a las siguientes normas:

> "I. Se iniciará mediante escrito en el que deberán expresarse los agravios que a juicio del recurrente le cause la resolución, acompañando copia de ésta, así como las pruebas que considere necesario rendir, dicho escrito deberá presentarse dentro de los tres días hábiles siguientes a los que surta efectos la notificación del acuerdo o resolución recurrida;
>
> "II. El Instituto dentro de los tres días hábiles siguientes a la recepción acordará sobre la procedencia del recurso, así como de las pruebas ofrecidas, desechando de plano las que no fuesen idóneas para desvirtuar los hechos en que se basa la resolución;
>
> "III. Desahogadas las pruebas, si las hubiere, el Instituto emitirá resolución dentro de los cinco días hábiles siguientes, notificando al interesado en un plazo no mayor a tres días hábiles; y
>
> "IV. Una vez cerrada la instrucción, únicamente se admitirán pruebas supervenientes
>
> …"

Cuando se interponga este recurso, los plazos ordinarios que tiene el Instituto para emitir la resolución definitiva serán suspendidos hasta que se termine de solventar ese medio de impugnación.

Los plazos que tiene el Instituto para emitir la resolución definitiva son:

---

[131] Carbonell, Miguel; Op.cit p. 253.

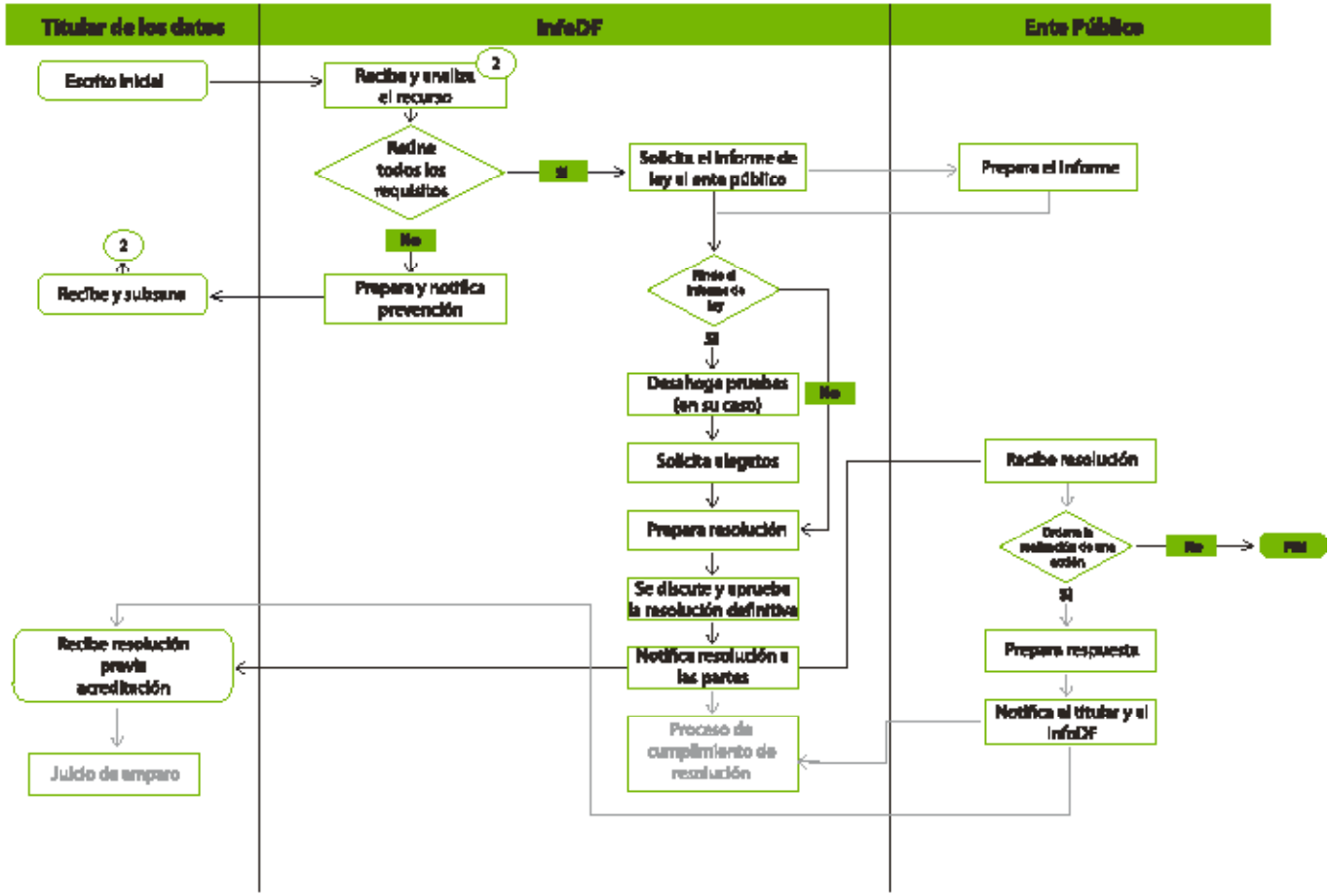
[132] Artículo 40, Op.cit.

Hipótesis	Plazo
El ente público no rinde el informe de ley.	20 días hábiles
Se interpone el recurso de revisión por falta de respuesta	10 días hábiles
En el supuesto que se haya interpuesto por inconformidad:	40 días hábiles
Hipótesis	**Plazo**
En el supuesto anterior, el plazo podrá ser ampliado por:	10 días hábiles

En la resolución definitiva, el Instituto podrá, en los términos del artículo 82 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal:

1. Desechar por improcedente.
2. Sobreseerlo.
3. Confirmar la respuesta.
4. Revocar la respuesta.
5. Modificar la respuesta.
6. Ordenar la emisión de una respuesta.

El procedimiento del recurso de revisión (simplificado) sería:


Titular de los datos
InfoDF
Ente Público
Escrito inicial
Recibe y analiza el recurso
2
Realna todos los requisitos
Si
No
Solicita el informe de ley al ente público
Prepara el informe
2
Recibe y subsana
Prepara y notifica prevención
Rinde el informe de ley
Si
No
Desahoga pruebas (en su caso)
Solicita alegatos
Prepara resolución
Se discute y aprueba la resolución definitiva
Notifica resolución a las partes
Recibe resolución
Ordena la realización de una acción
No
Fin
Si
Prepara respuesta
Notifica al titular y al InfoDF
Recibe resolución previa acreditación
Juicio de amparo
Proceso de cumplimiento de resolución

2.6 De las infracciones a la Ley de Protección de Datos Personales para el Distrito Federal.

Toda aquella transgresión a los principios y demás disposiciones contempladas en la Ley de Protección de Datos Personales del Distrito Federal serán sancionadas en los términos del Título Quinto de esa disposición, las cuales pueden ser clasificadas de la siguiente manera:

	Artículo 41 de la Ley de Protección de Datos Personales para el Distrito Federal
Principios	"… "III. Recabar datos de carácter personal sin proporcionar la información prevista en la presente Ley "IV. Crear sistema de datos de carácter personal, sin la publicación previa en la Gaceta Oficial del Distrito Federal "V. Obtener datos sin el consentimiento expreso del interesado cuando éste es requerido "VI. Incumplir los principios previstos por la presente Ley. "VII. Transgredir las medidas de protección y confidencialidad a las que se refiere la presente Ley" … "X. Obtener datos personales de manera engañosa o fraudulenta
Tratamiento	"I. La omisión o irregularidad en la atención de solicitudes [ARCO]; "II. Impedir, obstaculizar o negar el ejercicio de derechos a que se refiere la presente Ley; "VII. Transgredir las medidas de protección y confidencialidad a las que se refiere la presente Ley; … "XI. Transmitir datos personales, fuera de los casos permitidos, particularmente cuando la transmisión haya tenido por objeto obtener un lucro indebido; … "XIII. Destruir, alterar, ceder datos personales, archivos o sistemas de datos personales sin autorización"

Otras	"VIII. Omitir total o parcialmente el cumplimiento de las resoluciones realizadas por el Instituto, así como obstruir las funciones del mismo; "IX. Omitir o presentar de manera extemporánea los informes a que se refiere la presente Ley; "XII. Impedir u obstaculizar la inspección ordenada por el Instituto o su instrucción de bloqueo de sistemas de datos personales "XIV. Incumplir con la inmovilización de sistemas de datos personales ordenada por el Instituto… "XV. El incumplimiento de cualquiera de las disposiciones contenidas en esta Ley…"

Desde un punto de vista administrativo, la determinación de la actualización de alguna de las infracciones señaladas previamente le corresponderá al órgano interno de control, quién deberá actuar bajo lo dispuesto en la Ley Federal de Responsabilidades de los Servidores Públicos[133]. El Instituto o el titular[134] de los datos personales podrán, en todo momento, solicitar la intervención de dicho órgano; claro está, aportando todas las pruebas que se consideren pertinentes para comprobar su actualización.

La resoluciones que pongan fin al procedimiento administrativo sancionador deben, en los términos del artículo 42 de la Ley de Protección de Datos Personales para el Distrito Federal, ser notificadas por el órgano de control a:

1. El titular del ente público.

2. El responsable del sistema de datos personales.

3. Al titular de los datos personales que se hubiere visto afectado.

Estas sanciones administrativas son independientes, en los términos del citado artículo, a las penales y/o civiles que se pudieran actualizar.

Una medida de control, como lo señala el Dr. Carbonell, es la obligación que tienen los órganos fiscalizadores consistentes en proporcionar al órgano

[133] Artículos, 41 y 42. Op.cit.

[134] El Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, excitará la intervención del órgano interno de control por medio de una "denuncia", la cual es definida como "… la manifestación de hechos presuntamente constitutivos de responsabilidad administrativa, por conductas u omisiones de algún servidor público, y que se hacen del conocimiento de la Contraloría General del Distrito Federal o de los Órganos de Control Interno…" (fuente: Glosario de términos aplicables en el ámbito del Distrito Federal [http://cgservicios.df.gob.mx/glosario/seleccion.php])

garante de la materia, de manera semestral, un reporte estadístico de los procedimientos iniciados y sus resultados, lo que evita:

"… que en el entramado burocrático de las contralorías y demás órganos internos las violaciones a la Ley queden en la más absoluta bruma, sin que nadie pueda saber a ciencia cierta qué va pasando con la imposición, en su caso, de las sanciones correspondientes…"[135]

Dicho reporte debe ser integrado, por mandato de ley, en el informe anual que rinde el Instituto de Acceso a la Información Pública y Protección de Datos Personales a la Asamblea Legislativa, ambos del Distrito Federal.

[135] Op.cit. p. 272.

Bibliografía

Agencia Española de Protección de Datos Personales.

Carbonell, Miguel (Coordinador); Isabel Davara; Issa Luna Pla. "Ley de Protección de Datos Personales para el Distrito Federal: Comentada"; Asamblea Legislativa del Distrito Federal, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, Instituto de Acceso a la Información Pública y de Protección de Datos Personales del Distrito Federal, Secretaría de Gobierno del Distrito Federal, Tribunal Superior de Justicia del Distrito Federal; México, Distrito Federal, 2010.

Instituto Federal de Acceso a la Información y Protección de Datos Personales, Guía para la Elaboración de un Documento de Seguridad.

Glosario de términos aplicables en el ámbito del Distrito Federal http://cgservicios.df.gob.mx/glosario/seleccion.php

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Ley General de Salud.

Ley de Archivos del Distrito Federal.

Ley de Protección de Datos Personales para el Distrito Federal.

Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Lineamientos para la Protección de Datos Personales del Distrito Federal.

Lineamientos para la Gestión de Solicitudes de Información Pública y de Datos Personales a través del Sistema INFOMEX.

NOM-168-SSA1-1998.

NOM-040-SSA2-2004.

ISO-2007: www.iso27000.es/iso27000.html

Resolución 45/95 de las Naciones Unidas: www.informatica-juridica.com/anexos/principios_rectores_aplicables_ficheros_computarizados_datos_personales_resolucion_45_95_14_diciembre_asamblea_general_naciones_unidas.asp

Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, Dirección de Datos Personales. Presentación, Cursos impartidos en Noviembre 2011.

Instituto de Acceso a la Información Pública y
Protección de Datos Personales del Distrito Federal, INFODF

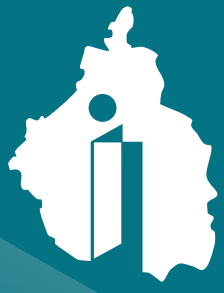
Transparencia y Datos Personales en el Distrito Federal,
Texto de apoyo a la formación de servidores públicos en el conocimiento de las leyes de transparencia y protección de datos personales

Impreso en los talleres de Servicio Editorial Gráfico y/o Omar Aguilar Sánchez
Calle 1513, No. 139, Col. Unidad Sexta San Juan de Aragón
Delegación Gustavo A. Madero
C.P. 07918, México, D.F.

1,000 ejemplares impresos
en papel bond de 90 gramos, forros en papel couché de 250 gramos

México, D.F., diciembre de 2011

Transparencia y Datos Personales en el Distrito Federal



infodf

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

infodf