infodf
Instituto de Acceso a la Información Pública del Distrito Federal

Ley de Protección de Datos Personales para el Distrito Federal Comentada

Miguel Carbonell (coordinador)
Isabel Davara
Issa Luna

Ciudad de México
Capital en Movimiento
Secretaría de Gobierno
Instituto de Investigaciones Jurídicas UNAM
Asamblea Legislativa del Distrito Federal V Legislatura
TSJDF

Ley de Protección de Datos Personales para el Distrito Federal Comentada

DIRECTORIO

Primera edición, septiembre de 2010
ISBN: 978-607-7702-24-5

IMPRESO Y HECHO EN MÉXICO

www.infodf.org.mx
La Morena No. 865, esquina Av. Cuauhtémoc, Colonia Narvarte Poniente, Delegación Benito Juárez, C.P. 03020, México, D.F.

Ley de Protección de Datos Personales para el Distrito Federal Comentada

Miguel Carbonell (coordinador)
Isabel Davara
Issa Luna

InfoDF
IIJ-UNAM

México, 2010

Nota del coordinador

El propósito fundamental de la obra que el lector tiene entre las manos es servir como herramienta para una mejor interpretación de la temática que gira alrededor de la normatividad local en materia de protección de datos personales, aplicable al Distrito Federal.

Para tal efecto, se ha intentado un abordaje lo más sencillo posible, eliminando las posibles cuestiones de interés meramente teórico y procurando que el lenguaje empleado fuera, hasta donde lo permiten las cuestiones jurídicas estudiadas, accesible para cualquier ciudadano.

Los autores queremos agradecer el apoyo y paciente guía del Comisionado Ciudadano Presidente del Instituto de Acceso a la Información Pública del Distrito Federal, InfoDF, Óscar M. Guerra Ford, y de la Comisionada Ciudadana Areli Cano Guadiana. Sin su decidido apoyo y sus múltiples sugerencias, esta obra no habría sido posible.

Por mi parte, quisiera hacer público mi reconocimiento a Isabel Davara e Issa Luna por su entrega, profesionalismo y compromiso académico con el tema de los datos personales. Son colegas y amigas con las que siempre es un gusto trabajar.

Finalmente, como lo podrá percibir el lector en las páginas siguientes, vale la pena enfatizar la importancia del tema de la protección de datos personales. Se trata de un derecho fundamental de reciente incorporación en nuestro texto constitucional (en el párrafo segundo del artículo 16 de la Carta Magna), pero que está indisolublemente unido al concepto de dignidad humana. En otras palabras, necesitamos tener nuestros datos personales debidamente protegidos para poder llevar una vida autónoma y digna. De ahí la importancia de estudiar y difundir las herramientas que, en el ámbito de lo jurídico, nos permiten acercarnos a ese objetivo.

Coyoacán, junio de 2010.

Índice

Presentación

Asamblea Legislativa del Distrito Federal
María Alejandra Barrales Magdaleno 13

Tribunal Superior de Justicia
Edgar Elías Azar 15

Gobierno del Distrito Federal
Juan José García Ochoa 17

Prólogo

Instituto de Acceso a la Información Pública del Distrito Federal
Oscar M. Guerra Ford 19

Comentarios a los artículos de la Ley de Protección de Datos Personales para el Distrito Federal (LPDPDF) 25

Artículo 1 de la LPDPDF
Miguel Carbonell 27

Artículo 2 de la LPDPDF
Isabel Davara F. de Marcos 30

Artículo 3 de la LPDPDF
Miguel Carbonell 43

Artículo 4 de la LPDPDF
Miguel Carbonell 49

Artículo 5 de la LPDPDF
Isabel Davara F. de Marcos 51

Artículo 6 de la LPDPDF
Issa Luna Pla 61

Artículo 7 de la LPDPDF
Issa Luna Pla 65

Artículo 8 de la LPDPDF
Issa Luna Pla 70

Artículo 9 de la LPDPDF
Isabel Davara F. de Marcos 75

Artículo 10 de la LPDPDF
Miguel Carbonell 82

Artículo 11 de la LPDPDF
Issa Luna Pla 85

Artículo 12 de la LPDPDF
Issa Luna Pla 90

Artículo 13 de la LPDPDF
Isabel Davara F. de Marcos 95

Artículo 14 de la LPDPDF
Isabel Davara F. de Marcos 103

Artículo 15 de la LPDPDF
Isabel Davara F. de Marcos 112

Artículo 16 de la LPDPDF
Isabel Davara F. de Marcos 121

Artículo 17 de la LPDPDF
Issa Luna Pla 128

Artículo 18 de la LPDPDF
Issa Luna Pla 133

Artículo 19 de la LPDPDF
Issa Luna Pla 139

Artículo 20 de la LPDPDF
Miguel Carbonell 143

Artículo 21 de la LPDPDF
Isabel Davara F. de Marcos 145

Artículo 22 de la LPDPDF
Issa Luna Pla 154

Artículo 23 de la LPDPDF
Miguel Carbonell 158

Artículo 24 de la LPDPDF
Issa Luna Pla 168

Artículo 25 de la LPDPDF
Miguel Carbonell 176

Artículo 26 de la LPDPDF
Isabel Davara F. de Marcos 179

Artículo 27 de la LPDPDF
Isabel Davara F. de Marcos 187

Artículo 28 de la LPDPDF
Isabel Davara F. de Marcos 193

Artículo 29 de la LPDPDF
Isabel Davara F. de Marcos 200

Artículo 30 de la LPDPDF
Isabel Davara F. de Marcos 206

Artículo 31 de la LPDPDF
Isabel Davara F. de Marcos 211

Artículo 32 de la LPDPDF
Miguel Carbonell 217

Artículo 33 de la LPDPDF
Issa Luna Pla 221

Artículo 34 de la LPDPDF
Miguel Carbonell 227

Artículo 35 de la LPDPDF
Issa Luna Pla 234

Artículo 36 de la LPDPDF
Issa Luna Pla 241

Artículo 37 de la LPDPDF
Miguel Carbonell 246

Artículo 38 de la LPDPDF
Miguel Carbonell 249

Artículo 39 de la LPDPDF
Miguel Carbonell 252

Artículo 40 de la LPDPDF
Miguel Carbonell 255

Artículo 41 de la LPDPDF
Miguel Carbonell 258

Artículo 42 de la LPDPDF
Miguel Carbonell 271

Análisis de los Lineamientos para la Protección de Datos Personales en el Distrito Federal
Isabel Davara F. de Marcos 277

1. Definiciones 279
2. Información en la recogida de datos 287
3. Medidas de seguridad 292
4. Principios de la protección de datos 300
5. Obligaciones de los entes públicos 307
6. Derechos en protección de datos y procedimiento 315

Presentación

Asamblea Legislativa del Distrito Federal

Sin duda, uno de los aspectos más relevantes en el desarrollo democrático de nuestro país, y especialmente del Distrito Federal, es el avance experimentado en materia de transparencia y acceso a la información pública. Hace apenas unos años, el derecho de todo ciudadano a ser informado y la obligación de las autoridades a proporcionar dicha información, era algo utópico o de difícil materialización.

El impulso desde la sociedad, la evolución en el terreno legislativo y un adecuado marco institucional para su instrumentación, han hecho posible que la información que poseen las instituciones públicas hoy sea de fácil acceso para cualquier habitante de esta capital.

La evolución no es menor. Se ha superado el viejo paradigma; hoy, la información gubernamental no es impenetrable. De forma gradual, hemos tomado conciencia de que en cualquier régimen que se precie de ser democrático, la información pública gubernamental es de los gobernados y sólo es administrada por las instituciones.

No obstante, el derecho a la información tiene una contraparte o reserva: el derecho a la protección de datos personales.

La salvaguarda de datos personales como son el nombre, domicilio, religión, estado civil, historial clínico, preferencias sexuales y afiliación política, entre otras, son referencias que no pueden ser objeto de la información pública por un elemental respeto a la vida privada y porque no constituyen datos generados en el desarrollo institucional.

De ahí que la Declaración Universal de los Derechos Humanos y nuestra Constitución Política establecen con toda claridad la protección de que son objeto este tipo de datos. La primera al señalar que: *Nadie será objeto de injerencias arbitrarias en su vida privada,*

su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. Y la segunda al disponer en el artículo 6º, fracción II, que: *la Información a que se refiere la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes*; y en el artículo 16, segundo párrafo, 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*.

Los alcances de la Ley de Protección de Datos Personales para el Distrito Federal resultan fundamentales no sólo para los estudiosos e interesados en el tema, sino también para colmar dudas tan elementales como quién y de qué forma tutela los datos personales, cuáles son los principios que rigen para su administración, cómo o sobre qué bases operan los sistemas que se implementan para su operación, cuál es el tratamiento que se les da y de qué manera los entes públicos deben protegerlos.

El valor de esta obra editada por el Instituto de Acceso a la Información Pública del Distrito Federal en colaboración con el Tribunal Superior de Justicia del Distrito Federal, el Gobierno del Distrito Federal, la Asamblea Legislativa y el Instituto de Investigaciones Jurídicas de la UNAM, radica en que el lector contará con un instrumento que recoge la interpretación de la normatividad en materia de protección de datos personales, realizada por especialistas y conocedores del tema, para guiarle de forma más efectiva en el ejercicio y defensa de su derecho.

Dip. Alejandra Barrales Magdaleno
Presidenta de la Comisión de Gobierno
Asamblea Legislativa del Distrito Federal, V Legislatura.
Tribunal Superior de Justicia del Distrito Federal

Cuando apareció la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal (en mayo de 2008), una de las preocupaciones que eran recurrentes, tanto para los ciudadanos como para los operadores del derecho, era la protección de los datos personales. Al menos intuitivamente, todos coincidíamos en ciertos puntos sobre qué tipo de datos pueden considerarse como personales (dirección, cuentas bancarias, ideología, etc.) y cómo debíamos de protegerlos (realizando versiones públicas de ciertos documentos, protegiendo las bases de datos, por ejemplo). Sin embargo, nuestras intuiciones no bastaban para resolver todos los problemas que se presentaban. Era necesario que se definiera con precisión tanto el concepto como los mecanismos jurídicos para la protección de esta clase de datos.

Afortunadamente, el tiempo transcurrido entre la aparición de la ley de transparencia y la de protección de datos personales fue sumamente breve. No transcurrieron más de cinco meses entre una y otra. El hecho de que ambas leyes hayan aparecido casi conjuntamente, no sólo se debe entender como un buen ejemplo de lo que significa el efectivo oficio legislativo, sino también como una pertinente reacción ante lo que podríamos calificar como un importante paquete de lagunas jurídicas que nos dejaba la Ley de Transparencia.

Bajo esta perspectiva, entonces, podemos decir que la Ley de Transparencia había dejado muchos huecos jurídicos; es decir, que era sumamente indeterminada en algunas de sus partes. Esta situación, como es claro, no sólo generaba dudas teóricas y doctrinales, sino que, y aún más importante, afectaba la certeza jurídica de los funcionarios que operaban esta Ley. Por ello, la Ley de Protección de Datos Personales fue recibida con amplias expectativas prácticas; expectativas que aún, muchas de ellas, están por confirmarse.

Es verdad que a México todavía le faltan muchos estudios y análisis sobre el tema de protección de datos personales. Empero, con este libro de comentarios se pretende dar un paso más en la discusión; es decir, que pretende ser un ladrillo más para cubrir ciertos vacíos.

Por estas razones, me congratula saber que los líderes sobre el tema, los comisionados del Instituto de Acceso a la Información Pública del D.F., hayan logrado reunir a las autoridades de esta ciudad para publicar este libro de comentarios a la Ley de Protección de Datos Personales; y que hayan encargado los comentarios a tan destacados investigadores del Instituto de Investigaciones Jurídicas de nuestra Universidad Nacional, la UNAM.

Me parece que en este caso, puedo decir, con completa certeza, que el lector tiene en sus manos un libro de mucho interés con comentarios de mucha calidad.

Dr. Edgar Elías Azar
Magistrado Presidente
Tribunal Superior de Justicia del D.F.

En los últimos años, la transparencia y el acceso a la información pública pasó de ser un flanco abierto para el Gobierno del Distrito Federal, en el año 2007, a un área de oportunidad que lo llevó a ser considerado el más transparente de la República.

¿Cómo fue posible que se cambiara esta percepción sobre la transparencia en el Distrito Federal? ¿Qué se ha hecho o qué se ha dejado de hacer para que el Distrito Federal sea calificado como el más transparente?

En primer lugar, debe destacarse que la transparencia fue un compromiso político[1] que se plasmó en el Programa General de Desarrollo del Distrito Federal[2] y que devino en programa sectorial[3].

En ese contexto, se han desarrollado cuatro acciones permanentes, las cuáles son:

- Actualizar el marco jurídico en materia de Transparencia y Acceso a la Información Pública;
- Impulsar el fortalecimiento de las oficinas de información pública;
- Fomentar la actualización permanente de las páginas de transparencia en internet de los entes públicos; y
- Evaluar permanentemente a las oficinas de información pública mediante los indicadores de gestión.

---

[1] Compromiso 20. "Nuevo Contrato Social para la Ciudad de México", Lic. Marcelo Luis Ebrard Casaubón. 26 de octubre de 2005.

[2] Programa General de Desarrollo del Distrito Federal. Eje 1. Derechos plenos para la Ciudad y sus Habitantes.

[3] Programa para el Fortalecimiento de la Transparencia y el Acceso a la Información Pública del Distrito Federal. 21 de noviembre 2007.

La estrategia de actualización permitió dotar a la Ciudad de México con la legislación más avanzada y más completa de toda la República, en cuanto a la garantía de acceso a la información pública, protección de datos personales y organización de archivos, pues a raíz de la promulgación de las reformas del Artículo 6º Constitucional, la Asamblea Legislativa del Distrito Federal aprobó y el Jefe de Gobierno promulgó:

- La Nueva Ley de Transparencia y Acceso a la Información Pública, considerada la mejor del país en 2010; la cual, según estudio de FUNDAR y Artículo XIX, es la que mejor garantiza el Derecho de Acceso a la Información;
- La Ley de Archivos del Distrito Federal;
- La Ley de Protección de Datos Personales para el Distrito Federal; y
- El Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Lo anterior, porque se consideró que era de suma importancia que la Ciudad de México contara con un marco regulatorio específico para cada uno de los tres componentes del acceso a la información, la transparencia y la rendición de cuentas. La Ley de Protección de Datos Personales del Distrito Federal, en consecuencia, tiene como propósito principal garantizar la confidencialidad, seguridad, integridad, legalidad y legitimidad del uso de los datos personales de todas las personas que viven y/o transitan en el Distrito Federal.

La presente obra adquiere particular importancia, en virtud de que tiene como finalidad otorgar una guía para la interpretación de la Ley de Protección de Datos Personales tanto a servidores públicos, investigadores, pero principalmente a la ciudadanía en general, promoviendo la apropiación de la Ley y su mejor uso.

Lic. Juan José García Ochoa
Subsecretario de Gobierno del D.F.

Prólogo

Instituto de Acceso a la Información Pública del Distrito Federal

En un mundo en el que la información puede ser difundida entre un gran número de personas gracias a la tecnología, es imperativo proteger los datos que sobre nosotros detentan las autoridades públicas. La protección de nuestros datos es importante para poder llevar una vida autónoma y digna.

Así como los órganos del Estado están obligados a difundir la información relacionada con el ejercicio del poder público, también tienen el deber de proteger la información de carácter personal que sobre sus gobernados detentan, para asegurar su derecho a la privacidad. Esta protección a la información debe darse de manera independiente a la del ejercicio del derecho de acceso a la información pública.

Esta obra permite identificar claramente las distinciones existentes entre el derecho de acceso a la información, el cual es regulado en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, y el derecho a la protección de los datos personales, que es un derecho plenamente autónomo al derecho de acceso a la información, como lo comprueba su reciente inclusión en el artículo 16 de la Constitución Política Federal.

El derecho a la protección de datos consiste en un poder de disposición y de control sobre los datos personales, los cuales se concretan en la facultad de consentir la recolección, obtención y acceso a los datos para su posterior almacenamiento y tratamiento, así como su uso o usos posibles por un tercero, en este caso por el Estado o un particular que, con motivo de una relación contractual con las autoridades públicas del Distrito Federal, requiera tratar los datos.

Por este motivo, el artículo 16 de la Constitución federal, en su párrafo segundo, establece, de manera autónoma al artículo 6, el derecho

a la protección de los datos personales al estatuir, a partir del 1 de junio de 2009, 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"*.

La relevancia de proteger de manera adecuada los datos personales que tiene en su posesión el gobierno fue advertida oportunamente por el legislador local. Así, la Ley de Protección de Datos Personales para el Distrito Federal dio cabal cumplimiento a la reforma al artículo 6 Constitucional realizada en el 2007 por el H. Congreso de la Unión, al dejar claramente establecida la línea que divide la información pública de la privada y atribuir a la persona un poder de disposición y control sobre los datos personales que sobre ella detentan los entes públicos.

Sin embargo, al optar por dar un tratamiento jurídico a nivel legislativo diferenciado del que se refiere al derecho de acceso a la información, casi un año antes de que lo hiciera la legislatura federal, la Asamblea Legislativa del Distrito Federal emitió una norma que cumple con los parámetros de la reforma realizada al artículo 16 de la Constitución federal en junio de 2009.

La Ley de Protección de Datos Personales para el Distrito Federal fue aprobada por la Asamblea Legislativa el 27 de agosto del 2008 y publicada en la Gaceta Oficial del Distrito Federal el 3 de octubre del mismo año. Esta Ley fue elaborada a partir de dos iniciativas de ley. La primera de ellas fue la "Iniciativa con proyecto de decreto por el que se derogan diversas disposiciones de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y crea la Ley de Protección de Datos Personales para el Distrito Federal", la cual fue presentada el 6 de diciembre de 2007 por los diputados que integran la fracción parlamentaria del Partido Acción Nacional; la segunda, la "Iniciativa que crea la Ley de Protección de Datos Personales del Distrito Federal", que fue presentada el 14 de marzo de 2008 por el

Diputado Isaías Villa González, integrante del Grupo Parlamentario del Partido de la Revolución Democrática.

Durante la elaboración de la Ley, el Instituto dio sus opiniones sobre los diversos títulos que la conforman; en la emisión de opiniones se tomaron en cuenta las experiencias internacionales, particularmente los casos de España y Argentina.

La Ley aprobada se integra de cinco Títulos, el Título Primero contiene una serie de disposiciones generales en las que se delimitan el objeto y el ámbito de aplicación de la Ley, además de una relación de definiciones de expresiones y términos que facilitan la comprensión del texto de la Ley.

La legislación local establece que sólo son sujetos obligados los entes públicos del Distrito Federal, por lo que se excluye de la aplicación de la Ley a los entes privados por considerar que esta materia debía ser regulada en el ámbito federal y no en el local. De esta forma, están obligados a observar las disposiciones de la Ley el Órgano Judicial, Ejecutivo y Legislativo, así como los órganos autónomos y los partidos políticos.

La decisión de excluir de la aplicación de la Ley a los particulares, es consistente con la adición que se hiciera al artículo 73 de la Constitución federal en abril de 2009, para establecer que es facultad del Congreso de la Unión el legislar en materia de protección de datos personales en posesión de los particulares; no obstante que la legislación del Distrito Federal fue publicada antes de la reforma Constitucional aludida.

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

En el Título Segundo, se establecen los principios a los que debe sujetarse el tratamiento de los datos personales; las obligaciones, el ámbito de competencia y las responsabilidades de los sujetos obligados en el tratamiento de los datos personales; se regula la forma en la cual deben crearse, modificarse o suprimirse sistemas de datos personales en posesión de las autoridades públicas del Distrito Federal y se estatuye la existencia de un registro de los sistemas de datos personales habilitado por el Instituto.

En el mismo Título Segundo, se impone a los entes públicos la obligación de implementar medidas de seguridad para garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente de su honor e intimidad personal y familiar, y se establecen las condiciones de excepción al ejercicio de los derechos de acceso, rectificación, cancelación y oposición de sus datos.

El Título Tercero delimita la competencia y ámbito de acción del Instituto de Acceso a la Información Pública del Distrito Federal, cuyas principales responsabilidades son interpretar y vigilar el cumplimiento de la Ley y establecer lineamientos generales para garantizar el desarrollo de los sistemas de seguridad de los ficheros, su registro y su manejo.

El Título Cuarto establece que los particulares tienen derecho a acceder, rectificar y cancelar sus datos personales, así como a oponerse a que éstos sean tratados cuando se opongan a las disposiciones de la Ley de Protección de Datos Personales. Se establece el principio de gratuidad en el acceso a los datos personales y la forma en la cual podrán ser ejercidos estos derechos, así como los medios de defensa que podrá ejercer el titular de los datos cuando considere que sus derechos son vulnerados.

Por último, el Título Quinto instituye un catálogo de conductas que serán consideradas como infracciones a la Ley y que, por ende, deben ser sancionadas en términos de la Ley Federal de Responsabilidades de los Servidores Públicos.

La obra que nos ocupa es una herramienta que ofrece una interpretación de la Ley de Protección de Datos Personales para el Distrito Federal, mediante un lenguaje sencillo y accesible a cualquier ciudadano.

Los comentarios vertidos por los autores en cada artículo ofrecen una perspectiva que integra, para fines de interpretación normativa, las consideraciones establecidas tanto en la Ley de Protección de Datos Personales para el Distrito Federal como en los Lineamientos para la Protección de los Datos Personales en el Distrito Federal, publicados en la Gaceta Oficial el 26 de octubre de 2009.

Adicionalmente, en cada artículo se incluyen referentes nacionales e internacionales acerca de cómo son entendidos o interpretados los supuestos jurídicos contenidos en el artículo, así como ciertos elementos teóricos que son indispensables para facilitar la comprensión y la relevancia jurídica de cada supuesto normativo.

Sin lugar a dudas, este libro contribuirá significativamente a mejorar la comprensión y la interpretación del marco jurídico para asegurar la tutela efectiva del derecho a la protección de los datos personales en posesión de los entes públicos del Distrito Federal.

Mtro. Oscar M. Guerra Ford
Comisionado Presidente
del Instituto de Acceso a la Información
Pública del Distrito Federal.

COMENTARIOS A LOS ARTÍCULOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL

COMENTARIOS A LOS ARTÍCULOS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL DISTRITO FEDERAL[4]

Artículo 1.- La presente Ley es de orden público e interés general y tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos.

Miguel Carbonell

COMENTARIO

El artículo 1 de la Ley de Protección de Datos Personales para el Distrito Federal determina el objeto de regulación del conjunto de sus disposiciones; se refiere a los principios, derechos, obligaciones y procedimientos relativos a la protección y tratamiento de los datos personales.

Respecto de su contenido, vale la pena detenerse en dos aspectos que, estimo, son relevantes para su adecuada comprensión: el concepto de datos personales y el alcance de la Ley en cuanto a la regulación de los tenedores o poseedores de los datos.

Recordemos, preliminarmente, que la materia de datos personales tiene tres distintos fundamentos constitucionales, a partir de disposiciones recogidas en los artículos 6, 16 y 73 de la Carta Magna.

En efecto, por un lado, el artículo 6, fracción II, ordena que "La información que se refiere a la vida privada y los datos personales" sea protegida por la Ley, en los términos y con las excepciones que ésta prevea.

Por otro lado, el artículo 16 párrafo segundo de la Carta Constitucional señala: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos,

---

[4] Publicada en la Gaceta Oficial del Distrito Federal el 3 de octubre de 2008.

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".

La tercera referencia constitucional relevante para nuestro tema se encuentra en el artículo 73, fracción XXIX inciso O, de acuerdo con la cual se faculta al Congreso de la Unión para legislar en materia de "protección de datos personales en posesión de particulares".

Las tres referencias constitucionales que se acaban de señalar son importantes porque, al ser leídas de forma armónica y sistemática, nos dan muchas pistas sobre la manera en que el tema de la protección de los datos personales puede y debe ser estudiado.

Por un lado, la referencia del artículo 6 nos indica que los datos personales se ubican dentro de la temática más amplia del derecho de acceso a la información (que es el tema genérico al que se refiere el propio artículo 6 en su párrafo segundo)[5]. En este contexto, tanto la vida privada como los datos personales (que son los dos bienes jurídicos a los que hace referencia la fracción II del artículo 6 constitucional) serían una suerte de límite al derecho de acceso a la información.

La regla general prevista en la fracción I del artículo señalado sería el acceso a la información, mientras que la vida privada y los datos personales serían límites o excepciones a esa regla, de acuerdo a lo que señale desde luego la ley.

De forma distinta, el artículo 16 párrafo segundo establece un derecho plenamente autónomo (es decir, no vinculado con el derecho fundamental de acceso a la información pública gubernamental) a la protección de los datos personales, en las modalidades de acceso, rectificación, cancelación y oposición de los mismos, así como los ámbitos en los que deben existir principios específicos por razón de la

---

[5] Carbonell, Miguel, *El régimen constitucional de la transparencia*, México, IIJ-UNAM, 2008.

materia de que se trata o del ámbito material en que se pueden aplicar tales principios; tal es el caso de la seguridad nacional, seguridad pública, salud pública y protección de derechos de terceros, tal como lo enuncia el artículo 16 de la Carta Magna.

Finalmente, el artículo 73, al reservar la competencia para legislar en materia de protección de datos personales en posesión de particulares a favor del Congreso de la Unión, lo que hace es dividir en dos la temática que nos ocupa: por un lado estaría lo que se refiere a la protección de datos personales en manos de los órganos, organismos, autoridades o dependencias públicas, cuya regulación compete tanto al Congreso de la Unión (cuando se trate de autoridades federales como lo pueden ser el Instituto Mexicano del Seguro Social o la Procuraduría General de la República, por citar dos ejemplos), como a las entidades federativas cuando se trate de datos personales en posesión de autoridades locales. Por otra parte, la regulación de todos los datos personales que se encuentren en manos de particulares debe realizarse, de forma exclusiva, por el Congreso de la Unión.

La separación de los dos ámbitos (datos personales en posesión de autoridades y en posesión de particulares) tiene ventajas y desventajas, las cuales no pueden ser examinadas con detalle en este momento. Lo que sí es importante es tener presente esa distinción competencial que ordena la Constitución.

Adicionalmente, conviene considerar que el marco jurídico que nos ofrece la Constitución en materia de datos personales nos debe llevar a preguntarnos si la regulación del tema debe hacerse por las leyes de transparencia o bien por leyes específicas en el tema de datos. La solución que fue en su momento elegida por la Asamblea Legislativa del Distrito Federal me parece la más acertada, dado que el derecho a la protección de datos personales tiene su propia sustantividad y merece un tratamiento jurídico a nivel legislativo diferenciado del que se refiere al derecho de acceso a la información.

Artículo 2.- Para los efectos de la presente Ley, se entiende por:

Bloqueo de datos personales: La identificación y reserva de datos personales con el fin de impedir su tratamiento;

Cesión de datos personales: Toda obtención de datos resultante de la consulta de un archivo, registro, base o banco de datos, una publicación de los datos contenidos en él, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta a la interesada, así como la transferencia o comunicación de datos realizada entre entes públicos;

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

Ente Público: 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;

Instituto: El Instituto de Acceso a la Información Pública del Distrito Federal.

Interesado: Persona física titular de los datos personales que sean objeto del tratamiento al que se refiere la presente Ley;

Oficina de Información Pública: La unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los entes públicos, a cuya tutela estará el tramite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida el Instituto;

Procedimiento de disociación. Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona física identificada o identificable;

Responsable del Sistema de Datos Personales: Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos;

Sistema de Datos Personales: Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos;

Usuario.- Aquel autorizado por el ente público para prestarle servicios para el tratamiento de datos personales.

Isabel Davara F. de Marcos[6]

COMENTARIO

El mandato constitucional de proteger los datos personales

De un lado, la reforma al artículo sexto de la Constitución Política de los Estados Unidos Mexicanos incorpora un párrafo destinado a la protección de datos personales que después veremos. Aquí ya tenemos una pequeña "victoria" y reconocimiento al derecho —o mera garantía institucional[7]—, aunque encuadrado dentro de la reforma al acceso a la información pública gubernamental.

De otro, el artículo 16 sí consagra plenamente el derecho a la protección de datos personales y encomienda al legislador su protección en los siguientes términos:

> *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.*

La redacción actual del artículo constitucional, y en particular este párrafo, se debe a la modificación introducida por el Decreto por el que se adiciona un segundo párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos[8], recorriéndose los subsecuentes en su orden.

---

[6] Quiero agradecer desde el inicio la inestimable colaboración del Mtro. Miguel Recio Gayo, sin cuya ayuda estos comentarios no hubieran sido posibles.

[7] Miguel Carbonell opina que en México no son todavía derechos fundamentales, sino bienes jurídicos constitucionalmente tutelados, como garantías institucionales, que deben ser protegidas, pero que aún, por su situación en la Carta Magna, no dan lugar a derechos. Vid Carbonell, M. "La reforma constitucional en materia de acceso a la información: una aproximación general", en *Hacia una democracia de contenidos: la reforma constitucional en materia de transparencia,* Instituto de Investigaciones Jurídicas, UNAM, 2007, página 1.

[8] Publicado en el Diario Oficial de la Federación de 1 de junio de 2009.

A nivel federal, el mandato constitucional encuentra su desarrollo en el sector público en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (en adelante, LFTAIPG)[9] en su Capítulo IV, de su Título I, que está dedicado a la protección de datos personales.

No obstante, al momento de preparar estos comentarios, la publicación en el Diario Oficial de la Federación de la Ley Federal de Protección de Datos en Posesión de los Particulares todavía estaba pendiente. La Ley, después de, al menos, ocho (8) iniciativas en nueve (9) años, fue finalmente aprobada por ambas Cámaras, tanto de Diputados como de Senadores, el 27 de abril de 2010. La Ley Federal de Protección de Datos desarrolla plenamente el derecho a la protección de datos personales en posesión de los particulares. En este sentido, a nivel federal, no había una regulación general del tratamiento de datos de carácter personal, salvo por lo que se refiere a las Sociedades de Información Crediticia[10], puesto que su Ley dedica algunos artículos a las bases de datos relativas al historial crediticio y a la prestación de servicios de información crediticia, además de otras referencias parciales, tal y como ocurre en el caso de la Ley Federal de Telecomunicaciones o la legislación sobre propiedad intelectual.

La normativa básica de protección de datos en el DF

En el Distrito Federal se aprobó el Decreto por el que se expide la Ley de Protección de Datos Personales (citada también como LPDPDF), cuyo objeto es:

> *Artículo 1.- La presente Ley es de orden público e interés general y tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos.*

---

[9] Publicada en el Diario Oficial de la Federación de 11 de junio de 2002.

[10] Ley para Regular las Sociedades de Información Crediticia, publicada en el Diario Oficial de la Federación de 15 de enero de 2002 y última reforma el 20 de enero de 2009.

Podríamos entonces decir que la LPDPDF declara desde su inicio que la protección de datos se compone de una serie de principios que, a modo de declaraciones programáticas, establecen los pilares en los que se basa la protección de datos.

En este sentido, si atendemos por un momento a la regulación federal en materia de protección de datos personales, según los Lineamientos de Protección de Datos Personales (en adelante, Lineamientos PDP), los principios rectores de la protección de datos son la licitud, la calidad, el acceso y corrección, la información, la seguridad, la custodia y el consentimiento para la transmisión. Los Lineamientos fueron publicados en el Diario Oficial de la Federación de 30 de septiembre de 2005.

A modo de ejemplo, en el ámbito internacional, cabe citar algunas normas e instrumentos de diverso rango que incluyen principios en materia de protección de datos:

- la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, 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 (citada como Directiva 95/46/CE), enumera calidad, legitimación en el tratamiento, categorías especiales, información del interesado, derecho de acceso, derecho de oposición, seguridad y confidencialidad, notificación;
- la Asamblea General de la Organización de las Naciones Unidas emitió la Resolución 45/95 en 1990 con una lista básica de principios como el de licitud, exactitud, finalidad, acceso y no discriminación, entre otros;
- la Asociación para la cooperación económica Asia-Pacífico (APEC) emitió en 1998 su Marco de Privacidad con los principios de prevención de daño, aviso, limitación a la recolección de información personal, usos de la información o datos personales, elección, integridad de la información personal, seguridad, acceso y corrección, y responsabilidad;

- el Convenio (108) del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal incluye los principios de calidad, categorías particulares de datos, seguridad de los datos. También prevé garantías complementarias para la persona concernida (acceso, rectificación y borrado);
- por último, en su 31ª Conferencia Internacional, celebrada en Madrid los días 4 a 6 de noviembre de 2009, las Autoridades de Protección de Datos y Privacidad de diversos países aprobaron una Resolución respecto de los Estándares Internacionales sobre Protección de Datos Personales y Privacidad que enumera los principios de lealtad y legalidad, proporcionalidad, calidad, transparencia y responsabilidad, derechos de acceso, rectificación y cancelación, así como oposición.

Los derechos, por su parte, representan la concreción subjetiva del ejercicio de esos principios, es decir, cómo el titular de los datos de carácter personal puede ejercer unos derechos que sintetizan los principios teóricos en los que se basa toda la normativa.

El procedimiento, finalmente, cerrando este triángulo ficticio, concreta la tutela pública a la que el individuo puede recurrir cuando se ve lesionado en el ejercicio de esos derechos como consecuencia de esos principios.

Definiciones del artículo 2

Siguiendo la máxima romana, toda definición en Derecho es peligrosa[11], luego los textos legales tienden a huir de ellas[12].

---

[11] De la conocida máxima latina: "*Omnis definitio in iure civili periculosa est: parum est enim, ut non subverti posset*", es decir, toda definición en Derecho es peligrosa porque hay poco que no pueda ser impugnado. (Javoleno, Digesto, 50, 17, 202).

[12] Aunque en el caso de las normas de Derecho de Nuevas Tecnologías esto no es ni mucho menos cierto, pues probablemente su tecnicidad hace imprescindible contar con definiciones a la hora de su manejo.

Pero, supuestamente, en esta tecnificada materia sí se establecen y, además, la definición de dato de carácter personal es esencial, pues constituye el ámbito de aplicación objetivo de la normativa, es decir, en caso de que consideráramos que algo no es dato de carácter personal, la normativa no se aplicaría.

De manera enumerativa y a la vista de la redacción dada por el legislador, el artículo 2 de la LPDPDF define los siguientes conceptos: bloqueo de datos personales; cesión de datos personales; datos personales; Ente Público; Instituto; interesado; Oficina de Información Pública; procedimiento de disociación; responsable del sistema de datos personales; tratamiento de datos personales; y usuario.

A continuación, analizaremos las definiciones que resultan relevantes a efectos del tratamiento de datos, agrupándolas, si fuera oportuno, y sin que dicho análisis siga necesariamente el orden establecido por la Ley.

Responsable del Sistema de Datos Personales*

El responsable es el ente público, es quien decide sobre la finalidad, contenido y uso de dicho tratamiento[13].

El artículo 2 lo define como:

> *Responsable del Sistema de Datos Personales: Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos;*

---

[13] Nótese que se refiere a quien decide, en ningún caso se está refiriendo a quien trata los datos, o a quien los maneja, sino al que decide qué hacer con esos datos. Éste es el concepto delimitador. Un responsable incluso puede no llegar a manejar nunca esos datos, porque tenga un tercero al que le encargue esa prestación de servicios, y al que se denomina "encargado del tratamiento", pero aún así sigue siendo responsable porque es el que decide sobre lo que hacer, el que da las instrucciones que el tercero sigue.

***Nota aclaratoria del InfoDF**: Es pertinente señalar que, en términos del artículo 2 de la LPDPDF, el responsable del sistema de datos personales es la *"Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos"*. Sin embargo, la autora, en su exposición, considera como responsables a los sujetos obligados o entes públicos.

Es quien "dice lo que se tiene que hacer" con el archivo del que es responsable y, por ende, es una de las figuras sometidas en general a la normativa y, consecuentemente, susceptibles de exigencia de responsabilidad.

El responsable del archivo, sistema de datos personales o tratamiento, es decir el ente público para la LPDPDF, y aunque su titular nombre a efectos internos a una persona física como responsable, tiene la obligación de cumplir con la normativa en protección de datos, respetando todos los principios, facilitando el ejercicio de los derechos por el titular de los datos y, en su caso, sometiéndose al posible procedimiento administrativo, del tipo que sea, como consecuencia de sus actuaciones.

Aunque la Ley no lo define, es necesario distinguir al responsable del encargado.

Dicho encargado[14] es definido en los Lineamientos, ya que, en concreto, el numeral 36 prevé que el tratamiento de los datos pueda ser llevado a cabo por un tercero, pero le denomina usuario, y que, por tanto, accede a los datos para prestar un servicio al ente público.

Es decir, es necesario distinguir claramente entre las siguientes figuras:

- Responsable del sistema de datos personales: Es quien internamente decide sobre la finalidad, contenido y uso del tratamiento. Además, tiene que asegurarse de que se cumpla con las obligaciones establecidas en la Ley y los Lineamientos. En definitiva, es el responsable del tratamiento.
- Usuario: Es un tercero que presta un servicio al responsable y que implica el acceso a los datos personales. Se trata del que otras normativas a nivel internacional denominan como "encargado del tratamiento".

---

[14] Al que en el ámbito internacional otras normativas sobre protección de datos se refieren como encargado del tratamiento. Véanse, por ejemplo, el artículo 2.e) de la Directiva 95/46/CE o el artículo 2.g) de la LOPD.

En definitiva, tanto el responsable del sistema de datos personales como el usuario ("encargado del tratamiento" en otros entornos regulatorios) pueden tratar datos de carácter personal y, por tanto, quedan sujetos al cumplimiento de las obligaciones establecidas por la normativa sobre protección de datos en el Distrito Federal.

Datos personales

La primera definición a la que prestamos atención es a la de datos personales o datos de carácter personal porque entendemos que resulta clave para comprender la regulación efectuada por la Ley.

La definición dada por la LPDPDF es la siguiente:

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

Podemos indicar que se trata de una definición muy amplia, puesto que por dato personal se entiende, en definitiva, cualquier información concerniente a una persona física, identificada o identificable[15].

---

[15] En este sentido, cabe señalar que la LPDPDF sigue la misma definición que han establecido otras normas mexicanas e internacionales. Así, a modo de ejemplo, es posible citar las siguientes definiciones sobre dato personal o dato de carácter personal:

- La LFTAIPG en su artículo 3, fracción II, define los datos personales como *"la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten a su intimidad"*.

Interesado

Si el tratamiento de datos es el objeto de la Ley, el ámbito de aplicación subjetivo gira en torno al titular de los datos, a la persona física[16] cuya información personal es objeto del tratamiento en los términos que hemos analizado.

Así señala el artículo 2:

> *Interesado: Persona física titular de los datos personales que sean objeto del tratamiento al que se refiere la presente Ley;*

La denominación de interesado nos parece adecuada, puesto que existe una persona que tiene interés en el tratamiento de la información personal que le concierne y de la que es titular.

- El Convenio (108) del Consejo de Europa define en la letra a) de su artículo 2 el concepto de datos de carácter personal como: *"cualquier información relativa a una persona física identificada o identificable ("persona concernida")"*. Convenio (108) del Consejo de Europa, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981.

La Directiva 95/46/CE define en la letra a) del artículo 2 el concepto de datos personales de la siguiente manera: *"toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*". Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, 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 (D.O. L 281, 23/11/1995). En adelante, Directiva 95/46/CE o Directiva europea de protección de datos.

La LOPD define en la letra a) de su artículo 2 los datos de carácter personal como *"cualquier información concerniente a personas físicas identificadas o identificables"*, y la letra f) del artículo 5 del Reglamento que la desarrolla indica que se entiende por datos de carácter personal *"Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"*. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el Boletín Oficial del Estado número 298, de 14 de diciembre. Y Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, publicado en el Boletín Oficial del Estado número 17, de 19 de enero de 2008.

[16] Reiteramos que sólo las personas físicas entran bajo el ámbito de protección de la Ley, excluyendo por tanto a las jurídicas o morales.

En este sentido, resulta curioso observar cómo en la práctica diaria se producen multitud de situaciones en las que se discute hasta la saciedad de quién son los datos, típicamente entre empresas, competidoras o no, que luchan por mantener y acrecentar lo que hoy constituye el activo intangible más importante en la actividad empresarial. Los datos son de su titular. Ni del responsable del sistema de datos personales, ni del usuario. Los datos pertenecen a la persona física de la cual están revelando información personal[17].

Es el principio de la autodeterminación informativa, asentado en la sentencia del Tribunal Federal Alemán[18], en virtud del cual el titular de los datos es el único que tiene derecho a decidir cómo, cuándo, dónde y por quién se tratan sus datos.

De este principio fundamental, que no es un principio legal propiamente dicho[19], parte la doctrina de protección de datos y tiene que servir como referente para cualquier interpretación posible de ésta[20].

Procedimiento de disociación

Aunque esta definición[21] pueda parecer a simple vista muy técnica, si la unimos con la de datos de carácter personal entendemos claramente su razón.

---

[17] En clara referencia a la teoría sobre el derecho a la autodeterminación informativa en la que descansa toda la protección de datos y que ya hemos analizado.

[18] Tal y como señaló ya en su día el famoso ex presidente del Tribunal Constitucional Federal Alemán, Dr. Benda, *"el peligro para la privacidad del individuo no radica en que se acumule información sobre él, sino, más bien, en que pierda la capacidad de disposición sobre ella y respecto a quién y con qué objeto se transmite"*. Sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983.

[19] Aunque, evidentemente, el principio del consentimiento, columna vertebral de la protección de datos, es un claro referente del principio de la autodeterminación informativa.

[20] Vid. López-Ibor Mayor, V., "Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos", *Actualidad Informática Aranzadi* núm. 8, Pamplona: Ed. Aranzadi, 1993, páginas 1 y 2.

[21] Que por otro lado copia literalmente la del artículo 3.f) de la Ley española de Protección de Datos ya citada (LOPD).

El artículo 2 de la LPDPDF establece al respecto:

> *Procedimiento de disociación. Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona física identificada o identificable;*

Como decíamos, un dato de carácter personal es cualquier información concerniente a una persona física, identificada o identificable. Pues bien, si esa información no se puede asociar bajo ningún concepto a una persona física, esa información deja de cumplir con todos los requisitos necesarios para ser considerada un dato de carácter personal, que, por ende, quepa bajo el ámbito de protección de la Ley.

Es por esta razón que, cuando los datos se someten a un procedimiento de disociación, la información deja de ser personal, porque no se puede asociar[22] a ninguna persona física, identificada o identificable, y, por tanto, no tiene sentido establecer ninguna protección, porque pierden su característica más esencial, que es identificar o hacer identificable a una persona. En otras palabras, el dato deja de cumplir una función identificativa de la persona para convertirse en anónimo.

Tratamiento de datos personales

Hay quien ha llegado a plantear que el concepto de archivo/sistema/fichero[23] ya no es pertinente, sobre todo en los nuevos escenarios de "*tratamientos en la nube*".

---

[22] Como decíamos, esto es un imperativo sin excepción: la información no se puede bajo ningún concepto asociar a su titular. Estamos hablando, por ejemplo, de tratamientos estadísticos. Si esta información se puede asociar a una persona física, deja de ser una información disociada para adquirir su carácter de personal y, por ende, estar bajo la tutela de la normativa. Por ejemplo, los códigos o datos similares, en tanto se puedan retrotraer hasta llegar a asociarse a su titular, no pueden considerarse un tratamiento disociado. Tiene que verdaderamente ser imposible llegar a esa asociación.

[23] La LPDPDF define en su artículo 2 como Sistema de Datos Personales: *"Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso"*.

En nuestra opinión, los conceptos de sistema de datos y tratamiento no son incompatibles, puesto que en cualquier caso lo que se tiene que definir es si se puede llegar a tener una información asociada a una persona física en concreto, conforme a un orden. Porque, además, si nos ponemos muy extremistas, en cuanto haya un tratamiento que podamos encontrar, utilizando estos medios tecnológicos —en especial Internet— a los que hacen referencia aquellos que apuestan por la desaparición del concepto de fichero, estaríamos ante un parámetro de búsqueda y/o organización que podría considerarse como fichero, sin importar el número de datos que contenga.

En cuanto a la definición de tratamiento, y aún a riesgo de ser reiterativos, lo más llamativo es su increíble amplitud.

Así señala el artículo 2:

> *Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos automatizados o físicos, aplicados a los sistemas de datos personales, relacionados con la obtención, registro, organización, conservación, elaboración, utilización, cesión, difusión, interconexión o cualquier otra forma que permita obtener información de los mismos y facilite al interesado el acceso, rectificación, cancelación u oposición de sus datos;*

De esta definición lo que se puede decir sin problema es que tratamiento es absolutamente todo: desde el tratamiento más típico hasta la mera consulta de datos a través de una pantalla.

Por último, y para no extralimitarnos en los comentarios a las definiciones de este artículo, nos remitimos a los comentarios que haremos a los Lineamientos, donde se analizan más en detalle algunas definiciones tratadas en la Ley, por ejemplo, las de bloqueo de los datos, sistema de datos personales, tratamiento, cesión de datos, fuentes de acceso público o usuario.

Artículo 3.- La interpretación de esta ley 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.

Miguel Carbonell

COMENTARIO

De una forma absolutamente moderna, pertinente y apropiada, el artículo 3 de la Ley que estamos comentando nos ofrece una "cláusula interpretativa", puesto que hace explícito el mandato de realizar una "interpretación conforme" de su contenido respecto a una serie de normas jurídicas cuyo origen se encuentra, en parte, en el derecho internacional de los derechos humanos. De esta manera, la Ley de Protección de Datos Personales para el Distrito Federal se suma a una corriente cosmopolita claramente aliada con las mejores causas de la humanidad.

La conformidad hermenéutica a la que obliga el artículo 3 se da respecto de cuatro distintos parámetros a los que se deberán sujetar quienes apliquen la Ley en cuestión, y son los siguientes:

- La Constitución Política de los Estados Unidos Mexicanos;
- La Declaración Universal de los Derechos Humanos de la ONU (de 1948);
- El Pacto Internacional de Derechos Civiles y Políticos de la ONU (de 1966);
- La Convención Americana de Derechos Humanos (conocida coloquialmente como Pacto de San José, de 1969);

Adicionalmente, la última parte del artículo 3 hace referencia a los demás instrumentos internacionales suscritos y ratificados por el

Estado mexicano, entre los que se podrían incluir los Convenios de la OIT sobre distintos aspectos de los derechos fundamentales de los trabajadores[24]. En el ámbito de América Latina podemos destacar la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (conocida como "Convención de Belém do Pará") y la Convención Interamericana para la Eliminación de todas las formas de Discriminación de las Personas con Discapacidad, entre muchos otros documentos normativos con plena fuerza jurídica para México.

Respecto de tales instrumentos internacionales (es decir, tanto los que son expresamente mencionados por el artículo 3, como aquellos otros a los que remite sin nombrarlos), se debe tomar en consideración, además, la interpretación que hayan realizado los organismos internacionales especializados: tal interpretación suele estar contenida, por ejemplo, en las llamadas "Observaciones Generales", que son una especie de interpretación general dictada por Comités de expertos creados por mandato de los principales pactos internacionales de derechos humanos. Los Comentarios u Observaciones Generales son de gran interés para los estudiosos de los derechos fundamentales, ya que contribuyen a ampliar el significado de las disposiciones de los Pactos y Tratados, precisando las obligaciones de los Estados y las tareas concretas que deben llevar a cabo para cumplir con lo que disponen los instrumentos internacionales.

Podríamos decir que las Observaciones Generales se asemejan a una especie de jurisprudencia, sólo que no es dictada por órganos propiamente jurisdiccionales sino por órganos de carácter más bien consultivo, integrados por expertos en cada materia[25].

---

[24] Son especialmente importantes los Convenios número 87 (libertad sindical), 89 (derecho de sindicalización), 111 (discriminación en el empleo), 118 (igualdad de trato), 138 (edad mínima para trabajar), 143 (trabajadores migrantes), 169 (pueblos indígenas) y 182 (prohibición del trabajo infantil).

[25] Una selección muy amplia de Observaciones Generales puede verse en Carbonell, Miguel, Moguel, Sandra y Pérez Portilla, Karla (compiladores), *Derecho Internacional de los Derechos Humanos. Textos básicos*, 2ª edición, México, Porrúa, UNAM, CNDH, 2003, tomo I, pp. 389 y ss.

Además de las tareas importantes que realizan los Comités, hay que tener presente que los propios tratados internacionales pueden crear tribunales con competencias contenciosas o de otro tipo[26]; así sucede con la Convención Americana de Derechos Humanos, adoptada en San José de Costa Rica, que crea la Corte Interamericana de Derechos Humanos, cuya sede se encuentra en esa misma ciudad.

Sobre la manera en que los tratados internacionales se deben interpretar, la Suprema Corte de Justicia de la Nación ha sostenido el siguiente criterio:

> **TRATADOS INTERNACIONALES. SU INTERPRETACIÓN POR ESTA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN AL TENOR DE LO ESTABLECIDO EN LOS ARTÍCULOS 31 Y 32 DE LA CONVENCIÓN DE VIENA SOBRE EL DERECHO DE LOS TRATADOS (DIARIO OFICIAL DE LA FEDERACIÓN DEL 14 DE FEBRERO DE 1975)**. Conforme a lo dispuesto en los citados preceptos para desentrañar el alcance de lo establecido en un instrumento internacional debe acudirse a reglas precisas que en tanto no se apartan de lo dispuesto en el artículo 14, párrafo cuarto, de la Constitución General de la República vinculan a la Suprema Corte de Justicia de la Nación. En efecto, al tenor de lo previsto en el artículo 31 de la mencionada Convención, para interpretar los actos jurídicos de la referida naturaleza como regla general debe, en principio, acudirse al sentido literal de las palabras utilizadas por las partes contratantes al redactar el respectivo documento final debiendo, en todo caso, adoptar la conclusión que sea lógica con el contexto propio del tratado y acorde con el objeto o fin que se tuvo con su celebración; es decir, debe acudirse a los métodos de interpretación literal, sistemática y teleológica. A su vez, en cuanto al contexto que debe tomarse en cuenta para realizar la interpretación sistemática, la Convención señala que aquél se integra por: a) el texto del instrumento respectivo, así como su preámbulo y anexos; y, b) todo acuerdo que se refiera al tratado y haya sido concertado entre las partes con motivo de su celebración o todo instrumento formulado por una o más partes con motivo de la celebración del tratado y aceptado por las demás como instrumento referente al tratado; y,

---

[26] Sobre los mecanismos jurisdiccionales de protección de los derechos humanos previsto en los tratados, Villán Durán, Carlos, *Curso de derecho internacional de los derechos humanos*, Madrid, Trotta, 2002, pp. 499 y siguientes, así como Márquez Carrasco, Carmen, *Logros y desafíos en el 60 aniversario de la Declaración Universal de Derechos Humanos*, Bilbao, Universidad de Deusto, 2009, páginas 22 y siguientes.

> como otros elementos hermenéuticos que deben considerarse al aplicar los referidos métodos destaca: a) todo acuerdo ulterior entre las partes acerca de la interpretación del tratado o de la aplicación de sus disposiciones; b) toda práctica ulteriormente seguida en la aplicación del tratado por la cual conste el acuerdo de las partes acerca de su interpretación; y, c) toda norma pertinente de derecho internacional aplicable en las relaciones entre las partes; siendo conveniente precisar que en términos de lo dispuesto en el artículo 32 de la Convención de Viena sobre el Derecho de los Tratados para realizar la interpretación teleológica y conocer los fines que se tuvieron con la celebración de un instrumento internacional no debe acudirse, en principio, a los trabajos preparatorios de éste ni a las circunstancias que rodearon su celebración, pues de éstos el intérprete únicamente puede valerse para confirmar el resultado al que se haya arribado con base en los elementos antes narrados o bien cuando la conclusión derivada de la aplicación de éstos sea ambigua, oscura o manifiestamente absurda. Clave: 2a., Núm.: CLXXI/2002, Amparo en revisión 402/2001. Imcosa, S.A. de C.V. 16 de agosto de 2002. Unanimidad de cuatro votos. Ausente: Guillermo I. Ortiz Mayagoitia. Ponente: Guillermo I. Ortiz Mayagoitia; en su ausencia hizo suyo el asunto Mariano Azuela Güitrón. Secretario: Rafael Coello Cetina.

En la práctica, la aplicación de los tratados internacionales de derechos humanos se enfrenta con muchas dificultades[27]. Una de ellas, quizá no la menor, es el profundo desconocimiento que de su contenido tienen los abogados mexicanos, incluyendo a los jueces. Pese a todo, se trata de una fuente de derechos fundamentales de la mayor importancia, como lo demuestra el hecho de que el legislador del Distrito Federal haya considerado oportuno incluir una mención expresa en el texto del artículo 3 de la Ley local que estamos comentando.

Debe tenerse presente que la "interpretación conforme" no obliga solamente a la "no contradicción" entre normas (en este caso la Ley del DF y las normas señaladas arriba), sino que se debe traducir en

---

[27] Algunas reflexiones sobre el tema se pueden ver en Carmona Tinoco, Jorge Ulises, "La aplicación judicial de los tratados internacionales de derechos humanos" en Méndez Silva, Ricardo (coordinador), *Derecho internacional de los derechos humanos. Memoria del VII Congreso Iberoamericano de Derecho Constitucional*, México, IIJ-UNAM, 2002, pp. 181 y ss. Una aportación de primer nivel a la discusión sobre este tema puede verse en Caballero Ochoa, José Luis, *La incorporación de los tratados internacionales sobre derechos humanos en España y México*, México, Porrúa, 2009.

algo más profundo y complejo: los parámetros que nos ofrece el artículo 3 deben guiar por completo (siempre que sean relevantes al caso concreto que se tiene que resolver) la interpretación de la Ley de protección de datos personales. La conformidad que exige el artículo supone no contradicción, desde luego; pero también obliga a hacer una selección entre las "interpretaciones posibles", de tal forma que la que prevalezca sea aquella que mejor realice los propósitos establecidos en las normas de parámetro.

El intérprete, en esa virtud, no es libre de seleccionar la interpretación que prefiera, cuando se presenten más de una, sino que debe aplicar la que sea más congruente con las normas jurídicas mencionadas por el artículo 3; más congruente en el sentido de que extienda el número de sujetos protegidos por el derecho, o bien que amplíe el perímetro jurídicamente protegido por éste.

Se trata de una técnica interpretativa frecuentemente utilizada en materia de derechos fundamentales; el legislador federal también ha utilizado una referencia parecida alguna vez (por ejemplo en los artículos 6 y 7 de la Ley Federal para Prevenir y Eliminar la Discriminación)[28].

De lo que no cabe ninguna duda es de que con normas como la que estamos comentando, la interpretación jurídica en México da un salto considerable hacia los mejores estándares internacionales en materia de protección de datos personales y obliga a los operadores prácticos de la Ley de protección de datos personales a estudiar, conocer, analizar y saber aplicar toda la normativa internacional. Con ese tipo de medidas legislativas solamente cabe esperar cosas buenas. Muchas otras leyes deberían incorporar disposiciones como las del artículo 3 que comentamos.

---

[28] Ver Caballero Ochoa, José Luis, *La incorporación de los tratados internacionales sobre derechos humanos en España y México*, cit., páginas 307 y siguientes.

Artículo 4.- En todo lo no previsto en los procedimientos a que se refiere esta Ley, se aplicará de manera supletoria la Ley de Procedimiento Administrativo del Distrito Federal y, en su defecto, el Código de Procedimientos Civiles del Distrito Federal.

Miguel Carbonell

COMENTARIO

El artículo 4 de la Ley de Protección de Datos Personales del DF se refiere al importante tema de la supletoriedad.

Si bien es cierto que se trata de un tema siempre importante, lo es todavía más en la Ley que comentamos, precisamente por 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.

La supletoriedad, como institución, busca dar coherencia al sistema, evitando hasta el punto que sea posible las lagunas normativas[29]. Casi siempre la supletoriedad se introduce como un mecanismo en las leyes que tratan temas más o menos específicos, y opera mediante una remisión a leyes de carácter más general. Es el caso, como podemos ver, del artículo 4 que ahora comentamos, el cual remite a la Ley de Procedimiento Administrativo del Distrito Federal y, en su defecto, al Código de Procedimientos Civiles del Distrito Federal.

En la jurisprudencia de los tribunales federales mexicanos hay una cierta tendencia a limitar los casos en los que opera la supletoriedad. Algunas tesis jurisprudenciales estiman que la figura de la supletoriedad se puede aplicar cuando la ley que se ha de suplir prevé expresamente

---

[29] Sobre el concepto de laguna, Guastini, Riccardo, *Estudios sobre la interpretación jurídica*, 6ª edición, México, Porrúa, UNAM, 2004, pp. 83 y siguientes.

una determinada institución jurídica, pero de forma incompleta o deficiente[30].

En el supuesto de que una determinada figura jurídica no estuviera prevista en la ley original (la que se va a suplir), entonces no se puede colmar empleando la supletoriedad[31].

Una tesis especialmente importante para comprender el tema de la supletoriedad es la siguiente:

> 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.

---

[30] Ver por ejemplo, en este sentido, la tesis "Supletoriedad de las leyes procesales. Principios que la rigen", *Apéndice al Semanario Judicial de la Federación 1917-1988*, Primera Parte, Tribunal Pleno, p. 240.

[31] Ver la tesis "Ley, supletoriedad de la", *Semanario Judicial de la Federación y su Gaceta*, 9ª época,IV, septiembre de 1996, p. 442. En el mismo sentido se expresa la tesis "Supletoriedad", *Semanario Judicial de la Federación*, Octava época, XV-II, febrero de 1995, p. 563.

De acuerdo con los criterios jurisprudenciales que se han comentado, la supletoriedad de una ley no es lo mismo que la aplicación de la analogía. La aplicación analógica, como se sabe, se produce cuando se aplica una norma a una situación que no está regulada de forma expresa, pero que guarda similitud con otra que sí es objeto de regulación[32]. Sobre este particular, la jurisprudencia impediría trasladar una norma, por vía analógica, hasta un caso concreto invocando el concepto de supletoriedad, dado que no sería aplicable.

Es importante tener en cuenta que son dos las leyes a las que remite el artículo 4 para efecto de una posible aplicación supletoria: la Ley de Procedimiento Administrativo del Distrito Federal[33] y el Código de Procedimientos Civiles del Distrito Federal[34]. Se trata de normas generales, una aplicable sobre todo a las formalidades que deben observar los órganos administrativos locales (incluyendo las cuestiones generales relativas a los actos administrativos, como lo son sus elementos y requisitos de validez, su eficacia y ejecutividad, su nulidad, anulabilidad y revocación, etcétera); la otra referida principalmente a las cuestiones procesales (notificaciones, elementos de prueba, plazos, etcétera).

---

[32] Guastini, Riccardo, *Estudios sobre la interpretación jurídica*, 6ª edición, México, Porrúa, 2004, pp. 93 y siguientes. Afirma Guastini que "En el lenguaje jurídico, suele llamarse 'aplicación analógica' a la aplicación de una norma a un supuesto de hecho *no* contemplado por ella, pero *semejante* al previsto por la misma" (p. 93).

[33] Publicada en la *Gaceta Oficial del Distrito Federal* el 21 de diciembre de 1995 y en el *Diario Oficial de la Federación* el 19 de diciembre de 1995.

[34] Publicado en el *Diario Oficial de la Federación* el 26 de mayo de 1928.

Artículo 5.- Los sistemas de datos personales en posesión de los entes públicos se regirán por los principios siguientes:

Licitud: Consiste en que la posesión y tratamiento de sistemas de datos personales obedecerá exclusivamente a las atribuciones legales o reglamentarias de cada ente público y deberán obtenerse a través de medios previstos en dichas disposiciones.

Los sistemas de datos personales no pueden tener finalidades contrarias a las leyes o a la moral pública y en ningún caso pueden ser utilizados para finalidades distintas o incompatibles con aquella que motivaron su obtención. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

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.

Calidad de los Datos: Los datos personales recabados 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.

Confidencialidad: Consiste en garantizar que exclusivamente la persona interesada puede acceder a los datos personales o, en caso, el responsable o el usuario del sistema de datos personales para su tratamiento, así como el deber de secrecía del responsable del sistema de datos personales, así como de los usuarios.

Los instrumentos jurídicos 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.

Los datos personales son irrenunciables, intransferibles e indelegables, por lo que no podrán transmitirse salvo disposición legal o cuando medie el consentimiento del titular y dicha obligación subsistirá aún después de finalizada la relación entre el ente público con el titular de los datos personales, así como después de finalizada la relación laboral entre el ente público y el responsable del sistema de datos personales o los usuarios.

El responsable del sistema de datos personales o los usuarios podrán ser relevados del deber de confidencialidad por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la seguridad nacional o la salud pública.

Seguridad: 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.

Disponibilidad: Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado.

Temporalidad: Los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los que hubiesen sido recolectados.

Queda exceptuado el tratamiento que con posterioridad se les dé con objetivos estadísticos o científicos, siempre que cuenten con el procedimiento de disociación.

Únicamente podrán ser conservados de manera íntegra, permanente y sujetos a tratamiento los datos personales con fines históricos.

Isabel Davara F. de Marcos
COMENTARIO

Principios de la protección de datos

A la vista del artículo, podemos especificar que los principios que rigen en el tratamiento de datos de carácter personal son los de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad. Estos principios, que tienen que darse en todo tratamiento de datos, son los que legitiman dicho tratamiento. Si bien el artículo enumera estos principios, consideramos que hay otros como el de información, que posteriormente se incluye y desarrolla en el artículo 9 de la Ley, que también son necesarios con la finalidad de garantizar que el titular de los datos pueda conocer en todo momento dicho tratamiento.

Principio de licitud

El tratamiento de los datos tiene que ser lícito. Es necesario recordar que el tratamiento incluye cualesquiera operaciones relacionadas con los datos personales, que van desde su obtención, pasando por su posesión, hasta su utilización en la comunicación o transferencia. Es decir, el tratamiento incluye cualquier uso de la información, pasando por todas las fases en que se puede dividir.

La licitud del tratamiento, tal y como indica este artículo, implica garantizar que los entes públicos traten en sus sistemas de datos personales aquellos que sean necesarios para el cumplimiento de las atribuciones legales o reglamentarias que les correspondan.

Al mismo tiempo, la licitud del tratamiento también se concreta en que no puedan crearse sistemas de datos con finalidades que resulten contrarias a la Ley o a la moral pública. Igualmente, los datos no podrán utilizarse con fines distintos o incompatibles con aquellos para los que fueron obtenidos.

De cualquier modo, el procesamiento de los datos con fines históricos, estadísticos o científicos, no se considera incompatible de manera que resulta lícito, lo que significa que no es necesario obtener el consentimiento del interesado puesto que dicho tratamiento, con esta finalidad, está previsto en la propia Ley. No obstante, será necesario cumplir con el resto de principios que puedan resultar aplicables en este caso.

Principio del consentimiento

El artículo 5 señala el principio del consentimiento como uno de los que tienen que garantizarse en el tratamiento de datos de carácter personal, siendo uno de los que legitiman el tratamiento de datos de carácter personal en las normativas internacionales sobre protección de datos.

En concreto, el artículo que comentamos señala que, como regla general, el tratamiento de datos de carácter personal requiere el consentimiento del interesado. El titular tendrá que autorizar el tratamiento de sus datos, a menos que, tal y como veremos, concurra alguna de las excepciones previstas en la Ley. Entre estas excepciones, la primera y más general es la que regula este principio en el artículo 16, por lo que se refiere al desarrollo de las funciones de los entes públicos, es decir, que el tratamiento se encuentre previsto en las atribuciones legales o reglamentarias del ente público.

Conforme a lo dispuesto en el artículo, el consentimiento del interesado consiste en una declaración de voluntad que tiene que cumplir con las siguientes características:

- Libre: Esto es, no sometida a coacción alguna en tanto que el interesado debe tener la posibilidad de otorgarlo y oponerse al mismo, siempre que una Ley no disponga lo contrario.

- Inequívoca: De manera que no haya lugar a dudas. El interesado consentirá el tratamiento de sus datos de carácter personal sin que de su manifestación se pueda interpretar que no quiso otorgar dicho consentimiento o que no conocía la finalidad o finalidades.
- Específica: Para una finalidad determinada. Es decir, el interesado tendrá que recibir la información sobre la finalidad o finalidades con la que se van a tratar sus datos de carácter personal para poder consentir o no dicho tratamiento.
- Informada: Con base en la información que se proporciona al interesado sobre el tratamiento de sus datos personales. Por tanto, la información será la que conste en la cláusula o leyenda informativa que, en su caso, se proporcione al interesado en el momento de recabar u obtener sus datos de carácter personal. Dicha información será proporcionada conforme a lo indicado en el apartado 9 de la Ley que posteriormente se comenta y al que nos remitimos.

Principio de calidad de los datos

El derecho a la protección de datos se asegura al garantizar su calidad.

Los datos personales objeto de tratamiento tienen que ser los necesarios para la finalidad con la que se obtienen y además responder con veracidad a la situación actual del interesado, procediendo a su rectificación cuando fuera necesario.

Por este motivo, el artículo 5 de la LPDPDF establece que los datos objeto del tratamiento tienen que ser:

- Ciertos: Deben 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.
- Adecuados: En relación con la finalidad o finalidades del tratamiento que haya sido establecido. Esto significa que los datos resultan adecuados para la finalidad para la que se tratan.
- Pertinentes: La pertinencia del dato también debe concordar con la finalidad del tratamiento, puesto que los datos resultarán pertinentes en atención a la finalidad con que sean tratados. Es así que el responsable tiene que analizar los datos que va a tratar en atención a la finalidad o finalidades indicadas, solicitando sólo aquellos datos que resulten ser pertinentes.
- No excesivos: Al igual que en los dos casos anteriores, los datos deben estar acordes con la finalidad o finalidades para las que se solicitan a efectos de determinar si son excesivos o no. Por tanto, sólo se tratarán los datos que resulten necesarios para la finalidad o finalidades para las que se solicitan, buscando siempre obtener los mínimos datos necesarios (minimización) para evitar un tratamiento que resulte inadecuado.

La adecuación y pertinencia del dato hay que ponerla en relación con la finalidad con la que se va a tratar. Es decir, atendiendo a la finalidad del procedimiento se podrá determinar si los datos son adecuados, pertinentes y no excesivos.

Además, los datos tienen que estar en todo momento actualizados, de manera que *"respondan con veracidad a la situación actual del*

interesado". De no ser así, los datos podrán ser rectificados, sea de oficio o a instancia del interesado cuando éste ejercite su derecho de rectificación.

Principio de confidencialidad

La confidencialidad del tratamiento resulta también esencial para garantizar el derecho a la protección de datos.

La confidencialidad supone que sólo el interesado, el responsable o el usuario puedan acceder a los datos. En particular, la Ley impone al responsable del sistema de datos personales y al usuario un deber específico de secrecía.

Y decimos que es un deber específico puesto que éste se refiere, en concreto, al tratamiento de datos personales y a la obligación de guardar secreto sobre ellos. En consecuencia, dicho deber es independiente de cualquier otra obligación de secreto que pueda recaer sobre quien trata los datos de carácter personal.

El artículo prevé expresamente que el deber de confidencialidad se haga constar en aquellos instrumentos jurídicos que regulen el tratamiento de datos, bien sea por el responsable del sistema de datos personales o por los usuarios. Incluso tienen que establecerse las penas convencionales si la obligación de secrecía fuera incumplida por quien trate los datos de carácter personal.

No obstante, este deber de confidencialidad o secrecía no es absoluto y cederá en caso de que un juez así lo ordene mediante la correspondiente resolución judicial o existan razones de seguridad pública, seguridad nacional o salud pública que obliguen a revelar datos personales que sean objeto del tratamiento. Es decir, el deber de confidencialidad es un principio que tiene por objeto proteger los datos, si bien resulta claro que la secrecía no puede ser utilizada como argumento para impedir el acceso a los datos por quienes lo

requieren, siempre y cuando se cumpla con las garantías previstas en la Ley. No se trata, por tanto, de que cualquiera pueda acceder a los datos, puesto que ello dejaría sin efecto la protección conferida por la Ley, sino de permitir el acceso a los datos objeto de tratamiento por las autoridades competentes, en los casos en los que la causa esté justificada, ya sea por una resolución judicial o por una situación prevista en la Ley.

Principio de seguridad

Una de las facetas de la seguridad de los datos, como se verá con más detenimiento, consiste en garantizar que sólo quien esté autorizado para ello tenga acceso a tal información.

Al respecto, el artículo 5 incide de manera específica en dicha circunstancia al indicar que la seguridad se garantiza si sólo quienes están autorizados para ello tratan los datos de carácter personal.

En concreto, cabe destacar el hecho de que el artículo se refiera específicamente al responsable del sistema de datos personales y a los usuarios autorizados. Tal y como se analizará en el apartado correspondiente al cual nos remitimos, sólo las personas autorizadas para ello podrán tener acceso a los datos.

La seguridad de los datos se concreta, en la práctica, a través del documento de seguridad. Es decir, el documento de seguridad es el instrumento que permite dejar constancia de las medidas de seguridad y, por tanto, aplicar el principio de seguridad. En consecuencia, el documento de seguridad se convierte en el instrumento a través del que el responsable de seguridad cumple y hace cumplir las medidas de seguridad previstas en la Ley y aquellas otras que permiten proteger los datos personales.

Principio de disponibilidad

La disponibilidad de los datos pasa fundamentalmente, tal y como indica el artículo comentado, por garantizar que éstos sean almacenados de modo que su tratamiento permita el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

Por tanto, el tratamiento de los datos tendrá 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 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.

No cabe duda que la Ley tiene que ser interpretada conforme a otras normas que puedan resultar aplicables a los archivos. En este sentido, es necesario tener en consideración la relación que pueda existir entre la protección de datos y el acceso a la información que consta en un archivo. Resulta relevante la Ley de Archivos del Distrito Federal así como la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, de manera que la Ley de Protección de Datos Personales tiene que ser interpretada en el marco de esta realidad jurídica, sin obviar los límites a los que se encuentra sujeta y tomando en cuenta la necesidad de encontrar un equilibrio.

Principio de temporalidad

El último de los principios a los que se refiere el artículo 5 de la LPDPDF es el de la temporalidad de los datos que son objeto de tratamiento.

El citado artículo establece una regla general y excepciones en relación con el tratamiento de datos de carácter personal en los sistemas de datos. En concreto, cabe señalar lo siguiente:

- *Regla general:* Tal como indica el primer párrafo, cuando los datos dejen de ser necesarios o pertinentes para la finalidad con la que hubieran sido recabados, serán destruidos. Es decir, la necesidad o pertinencia del dato, como ya hemos señalado con anterioridad, tiene que ser analizada en relación con la finalidad con la que se tratan los datos. Cuando la finalidad se ha cumplido o no se tratan con dicha finalidad, entonces los datos dejan de ser necesarios o pertinentes, lo que implica que tenga que considerarse la opción de ser cancelados o la obligación de cumplir con otros principios que resulten aplicables, tales como el consentimiento.
- *Excepciones:* Cabe señalar dos excepciones a la regla general:

    - Cuando el tratamiento posterior de los datos tenga fines estadísticos o científicos, siempre que éstos hayan sido sometidos previamente a un procedimiento de disociación.
    - Cuando el tratamiento tenga fines históricos, en cuyo caso podrán conservarse de manera íntegra. Este tratamiento específico tendrá que cumplir, además, con aquellas normas que resulten aplicables y en particular con la Ley de Archivos del Distrito Federal ya citada. Es decir, los datos personales objeto de tratamiento se encuentran incorporados en archivos, los que, a su vez, tienen que cumplir con la normativa aplicable en la materia, que establecerá plazos de conservación y disposición final de los documentos, conforme a lo que se disponga en el catálogo de disposición documental.

Artículo 6.- Corresponde a cada ente público determinar, a través de su titular o, en su caso, del órgano competente, la creación, modificación o supresión de sistemas de datos personales, conforme a su respectivo ámbito de competencia.

Issa Luna Pla

COMENTARIO

El artículo 6 de la Ley de Protección de Datos Personales para el Distrito Federal se inserta en el capítulo que define la creación y mantenimiento de los sistemas de datos personales. Los sistemas de datos personales son aquellas bases de datos en ficheros físicos y electrónicos que se crean al interior del ente público obligado por la Ley en comento, tal como lo definen en el numeral 4 los Lineamientos para la Protección de Datos Personales en el Distrito Federal, publicados en la Gaceta Oficial del Gobierno del Distrito Federal del día 26 de octubre de 2009.

En este apartado conviene tener siempre presente algunos elementos fundamentales para las acciones de las cuales la Ley de Protección de Datos Personales faculta a los titulares de cada ente público.

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. Piénsese, por ejemplo, en la facultad del fisco para resguardar datos de los contribuyentes, función que es sustancial a su misión recaudatoria.

Asimismo, en concordancia con los Lineamientos para la Protección de Datos Personales en el Distrito Federal, la creación, modificación o supresión de sistemas de datos personales de los entes públicos deberá efectuarse mediante acuerdo emitido por el titular del ente u órgano competente, publicado en la Gaceta Oficial. Esto significa

que el legislador no previó en ningún caso y por ningún motivo injustificado que la autoridad tuviera facultades discrecionales para recolectar datos personales y conformar nuevos sistemas de datos fuera del ámbito de su competencia. Es, sin embargo, por magisterio de ley o de un acuerdo del titular de la entidad, y bajo ciertas reglas que los mismos Lineamientos establecen, que se podrá hacer uso de la acción de creación, modificación o supresión de datos.

Por lo anterior, el presente artículo no faculta a las entidades obligadas a la Ley de Protección de Datos Personales para crear sistemas de datos personales discrecionalmente o de naturaleza clandestina. Resulta únicamente un mandato derivado de una facultad que otra ley o acuerdo normativo ha otorgado para crear sistemas de datos personales en correspondencia con su función dentro del gobierno.

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. A continuación se analiza la interpretación del artículo 6 en concordancia lógica y razonada con los principios de la tutela de los datos personales contenidos en sistemas de datos.

Para el presente artículo se entiende el principio de *licitud* como aquel que norma el comportamiento de la autoridad que administra los sistemas de datos personales. La creación de los sistemas de datos conlleva las acciones de: i) recolectar los datos personales y ii) conformarlos en sistemas automatizados o físicos que constituyan como tal un sistema de datos personales. Por lo anterior, el principio de licitud se extiende hacia los actos de recaudación de datos y a la conformación del sistema. No sería un acto *lícito* que el ente obligado sustraiga datos personales de bases de datos que no conforman el Registro de Sistemas de Datos Personales del Distrito Federal, o de bases de datos ilegales o clandestinas en manos de privados o públicos. Tampoco sería *lícito* que el ente público conformara un sistema de datos previo al mandato legal o por acuerdo, o que dicho sistema obedeciera a intereses ajenos a los objetivos y facultades de la propia entidad pública para el desempeño de sus funciones públicas. En cuanto a la modificación o supresión de los datos, el ente y organismo público deberá contar con mandato o acuerdo para actuar en concordancia con el principio de licitud que la Ley establece.

El artículo 6 de la Ley de Protección de Datos Personales para el Distrito Federal se interpreta conforme al principio de *consentimiento,* siempre que el titular de los datos personales se encuentre enterado e informado libremente del tratamiento de sus propios datos personales. Ello implica que el ente u organismo público que origine, modifique o suprima datos personales debe enterar al titular de la información sobre el "tratamiento" que hace la autoridad de sus propios datos. No sería coherente con el principio de consentimiento que un ente público conforme un nuevo sistema de datos sin antes comunicar al interesado de su acto y del uso y tratamiento que se le dará.

El principio de *finalidad* se encuentra relacionado con el de licitud en la Ley de Protección de Datos Personales para el Distrito Federal. Así, la capacidad de los entes públicos de crear, modificar y suprimir sistemas de datos personales tendrá que obedecer a la finalidad de los datos derivada expresamente de una ley o acuerdo del titular. De esta manera, el legislador evitó la existencia de sistemas de datos personales carentes de finalidad y que puedan ser utilizados como "bases comodines" que respondan a diversos objetivos públicos o privados. Este principio se considera fundamental en el derecho

comparado de la protección de datos personales, toda vez que limita el ámbito de acción de la autoridad para crear, modificar o sustraer datos personales, reconociendo que la titularidad de los datos pertenece al sujeto de la información que, mediante su consentimiento, autoriza al ente público el tratamiento de sus datos.

El principio de *seguridad* se aplica al artículo 6 de la Ley en comento en tanto que, para la creación, modificación y sustracción de datos personales, se requiere contar con un servidor público responsable, capaz de enfrentar las consecuencias del incumplimiento o violación al derecho de la protección de los datos personales de los individuos. Con ello, el legislador garantizó que las responsabilidades no se diluyeran para el tratamiento de los sistemas de datos personales, y colocó a funcionarios habilitados para dichos efectos. Asimismo, la modificación y sustracción de los datos personales podrá hacerse por los usuarios autorizados que por acuerdo de la autoridad queden facultados para tales efectos. En el derecho comparado, el principio de la seguridad también implica que los entes públicos cuenten con medidas de seguridad electrónica y física para el resguardo de los sistemas, en el supuesto caso de que un tercero no facultado y no responsable de los datos interfiera en los sistemas. Ello implica la colocación de software de acceso restringido, programas de antivirus y anti piratas informáticos. Para el caso de los ficheros físicos, la práctica internacional apunta que deben ser resguardados bajo las normas de archivos públicos y digitalizados.

Finalmente, el principio de *temporalidad* se integra en el artículo 6 comentado en cuanto a la posibilidad de sustracción y modificación de datos personales. Se entiende aquí que en el momento de la creación de los sistemas de datos, la autoridad competente establecerá una finalidad y temporalidad del sistema, por ello, esta temporalidad queda definida por la autoridad desde el decreto de creación del sistema. Asimismo, se podrán modificar o sustraer los datos sólo cuando dicha temporalidad, previamente establecida, extinga las causas que dieron origen a la creación del sistema. Quedan exceptuados de dicho principio aquellos datos que se destinen a un uso estadístico, científico o histórico, pues a dichos datos les corresponde ser regulados por las leyes específicas de cada materia, como las leyes de estadística y de archivos públicos.

Artículo 7.- La integración, tratamiento y tutela de los sistemas de datos personales se regirán por las disposiciones siguientes:

I. Cada ente público deberá publicar en la Gaceta Oficial del Distrito Federal la creación, modificación o supresión de su sistema de datos personales;

II. En caso de creación o modificación de sistemas de datos personales, se deberá indicar por lo menos:

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;

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.

III. En las disposiciones que se dicten para la supresión de los sistemas de datos personales, se establecerá el destino de los datos contenidos en los mismos o, en su caso, las previsiones que se adopten para su destrucción.

IV. De la destrucción de los datos personales podrán ser excluidos aquellos que, con finalidades estadísticas o históricas, sean previamente sometidos al procedimiento de disociación.

Issa Luna Pla
COMENTARIO

El presente artículo se encarga de desarrollar a detalle las disposiciones que deben contener los acuerdos por los cuales los titulares de los entes públicos y organismos competentes pueden crear, modificar o suprimir los sistemas de datos personales. El artículo desarrolla inicialmente la validez normativa del acto de decisión por medio del cual se garantiza la tutela de la protección de datos personales en manos de los entes públicos. En seguida, delimita los requisitos mínimos que debe contener el acto de decisión sobre el tratamiento de los sistemas de datos, en virtud de legitimar la decisión de la autoridad competente y de tutelar conforme a derecho la protección de los datos personales. Por último, en el artículo se prevé la inclusión de las disposiciones para la supresión y destrucción de los datos personales contenidos en los sistemas.

En principio, cabe recalcar que para el legislador el acto de creación, modificación o supresión de los sistemas de datos personales debe realizarse por fuerza de un acuerdo del titular del ente público, que deberá ser publicado en la Gaceta Oficial del Distrito Federal y notificado al Instituto de Acceso a la Información Pública del Distrito Federal. Esto implica que para crear, modificar o suprimir los sistemas de datos personales no necesitará de una voluntad legislativa, sino que desde el nivel de gestión pública podrán definirse los lineamientos y criterios para el tratamiento de sistemas de datos. Sin embargo, la vía de acuerdo no queda al arbitrio del titular de la entidad pública, sino que para constituir un acuerdo en materia de tratamiento de sistemas de datos personales, deberá cumplir con las disposiciones derivadas de la Ley de Protección de Datos Personales para el Distrito Federal en su artículo 7 y de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, publicados en la Gaceta Oficial del Gobierno del Distrito Federal del día 26 de octubre de 2009.

Para los acuerdos que versen sobre la creación o modificación de un sistema de datos personales, la Ley en comento prevé los siguientes requisitos en la fracción II del artículo 7 y ésta es desarrollada a detalle por los Lineamientos en la materia en su numeral 7:

a) *La finalidad del sistema de datos personales y los usos previstos para el mismo*, lo que implica que en el acuerdo debe establecerse con toda claridad la finalidad para la que será destinado el sistema de datos personales y los usos que se autoriza a los entes públicos dar a dichos datos.

b) *Las personas o grupos de personas sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos,* esto es, que las bases de datos no podrán contener datos de personas que no guardan alguna relación con la finalidad y propósito de la creación y modificación de un sistema de datos.

c) *El procedimiento de recolección de los datos de carácter personal,* la importancia de que el acuerdo señale el procedimiento de recolección de los datos radica en que la autoridad no puede sustraer datos de bases ilícitas o ilegales, por lo que este requisito se alinea a los objetivos que persigue el principio de licitud de la tutela y protección de los datos que establece la presente Ley en su artículo 5.

d) *La estructura básica del sistema de datos personales y la descripción de los tipos de datos incluidos en el mismo*, en aras de transparentar la creación y tratamiento que reciben los sistemas de datos personales, es imprescindible que se haga público, mediante acuerdo publicado en la Gaceta Oficial del Distrito Federal, la estructura y descripción del contenido de los sistemas de datos. Esta información debe incluir, en concordancia con los Lineamientos en la materia, si se trata de datos de carácter facultativo u obligatorio, y las categorías de datos a que corresponden de entre las establecidas en el artículo 5 de los Lineamientos.

e) *De la cesión de las que pueden ser objeto los datos,* esto es, la posibilidad de transferencia o intercambio de información que forma parte de la descripción del uso y finalidad del sistema de datos personales.

f) *Las instancias responsables del tratamiento del sistema de datos personales,* ello con el afán de definir con precisión la línea de responsabilidades que trae consigo la tutela y protección de los sistemas y los datos personales contenidos en cada uno de ellos.

g) *La unidad administrativa ante la que podrán ejercitarse los derechos de acceso, rectificación, cancelación u oposición*, dicho derecho se conoce en la legislación internacional como el derecho de hábeas data, como una prerrogativa de las personas a acceder, modificar, cancelar u oponerse a que sus datos sean tratados y administrados por el Estado. Para el mejor ejercicio de dicho derecho, se debe proporcionar el domicilio oficial y la dirección electrónica de la oficina de información pública que funge como ente a través del cual se ejercen los derechos ARCO.

h) *El nivel de protección exigible,* por último, el acuerdo debe contener el nivel de protección que se debe guardar para cada sistema de datos, definidos por los Lineamientos en la materia como: básico, medio y alto.

La fracción III del artículo 7 en comento prevé, en complemento con el numeral 9 de los Lineamientos para la aplicación de la Ley, la forma en la que se suprimirán los sistemas de datos personales. Esta disposición es importante porque en la experiencia internacional se sabe que el tráfico y mercado ilícito de bases de datos personales es un negocio de amplios rendimientos que saca provecho especialmente de aquellos sistemas o bases de datos que son suprimidos al término de su finalidad. Así, la comentada fracción, complementada por las disposiciones de los Lineamientos, establece que en los acuerdos publicados en la Gaceta Oficial en que se decida la supresión o

preservación por fines históricos de los sistemas deberá establecerse el destino que vaya a darse y las especificaciones sobre el proceso de su destrucción, que deberá guardar concordancia con la Ley de Archivos del Distrito Federal, en relación con los procesos documentales y archivísticos.

Por último, la fracción IV del artículo 7 aquí comentado, establece que aquellos datos personales que por acuerdo deban ser destruidos, pueden encajar en la categoría de nuevas bases de datos con finalidades estadísticas o históricas; en este caso, la Ley de Protección de Datos Personales para el Distrito Federal determina que dichos datos deberán ser *previamente sometidos al procedimiento de disociación*. Igualmente, en esta fracción el legislador procuró que el acto de destrucción de los datos personales sea conforme al principio de licitud y finalidad de los datos personales.

En la forma de tratamiento de datos personales que consta en la destrucción de éstos, existe comúnmente la sobreposición de normas jurídicas que pueden inducir a la contrariedad. Si bien la Ley de Protección de Datos Personales para el Distrito Federal no es clara en determinar los preceptos normativos que deberán primar sobre otras normas que pudieran establecer igualmente disposiciones en materia de destrucción o supresión de datos personales, el Instituto de Acceso a la Información Pública del Distrito Federal previó en el numeral 9 de los Lineamientos para la Protección de Datos Personales en el Distrito Federal que ante la existencia de otra norma que contenga previsión expresa exigiendo la preservación, no procederá la supresión de los datos personales previsto en la Ley en comento. Este es el caso de la preservación de datos con fines históricos y estadísticos, cuyas razones pueden estar fundadas en derecho sin contravenir la norma, tal como lo define la fracción IV del artículo en comento.

Artículo 8.- Los sistemas de datos personales en posesión de los entes públicos deberán inscribirse en el registro que al efecto habilite el Instituto.

El registro debe comprender como mínimo la información siguiente:

I. Nombre y cargo del responsable y de los usuarios;

II. Finalidad del sistema;

III. Naturaleza de los datos personales contenidos en cada sistema;

IV. Forma de recolección y actualización de datos;

V. Destino de los datos y personas físicas o morales a las que pueden ser transmitidos;

VI. Modo de interrelacionar la información registrada;

VII. Tiempo de conservación de los datos, y

VIII. Medidas de seguridad.

Issa Luna Pla

COMENTARIO

El artículo 8 de la Ley de Protección de Datos Personales para el Distrito Federal prevé la creación de un Registro de Sistemas de Datos Personales y faculta directamente al InfoDF para instituir el registro y administrarlo. Asimismo, el texto normativo del artículo 8 delinea los requisitos mínimos que debe contener la información que se ingrese a dicho Registro de sistemas de datos, lo que otorga uniformidad, orden, catalogación y organización de los sistemas de datos personales que hubieren en los entes públicos y organismos del Estado.

El Diccionario de la Real Academia de la Lengua Española define el término "registro" como el lugar donde se puede registrar o ver algo, un padrón o matrícula. Pero cuando la palabra "registro" se relaciona con información, entonces se define como un "conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos". Así pues, un "Registro de Sistemas de Datos Personales" es no menos que un lugar donde todos los sistemas de datos se compilan (un sistema de sistemas), agrupando unidades que guardan una similitud entre sí y catalogándolas homogéneamente para organizar los sistemas.

Un registro de sistemas de datos personales cumple una función elemental dentro de un régimen de protección de datos personales y su existencia y operatividad son centrales para el ejercicio del derecho de acceso a la información. El registro es un instrumento para velar por el derecho a la vida privada de las personas y para garantizar que las personas puedan acceder a sus propios datos personales. Esto es, sin el conocimiento sobre la existencia de los sistemas que administra el Estado y el tratamiento que se les da, los sujetos de la información se encuentran en discapacidad para ejercer su derecho a la protección de sus datos y sus derechos ARCO establecidos en la Ley en comento.

En la experiencia comparada, existen registros de datos personales en aquellos países que cuentan con leyes de protección de datos personales y que deben, por lo tanto, cumplir con una responsabilidad sobre el tratamiento de éstos. Es el caso del Registro de Datos Personales que administra el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires, Argentina; el Registro de Ficheros de Datos de carácter personal a cargo de la Agencia de Protección de Datos de la Comunidad de Madrid; y, la Oficina del Comisionado para la Información en Londres mantiene un Registro Público de Protección de Datos.

Ahora bien, quien administra los registros son institutos o comisiones con un mandato expreso por ley de proteger y supervisar el cumplimiento de las normas en relación con el derecho de acceso a la información, la protección de datos personales y, en general, los derechos humanos. Así, el Instituto de Acceso a la Información Pública del Distrito Federal cuenta con un mandato establecido en el artículo 23 de la Ley de Protección de Datos Personales para el Distrito Federal que lo faculta para "dirigir y vigilar el cumplimiento de la presente Ley, así como de las normas que de ella deriven". En esta misma lógica, el artículo 24, fracción I, de la Ley en comento otorga al Instituto, entre otras, la atribución de establecer "políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales". Igualmente, la fracción IV del artículo 24 de la misma Ley prevé que el Instituto tiene la atribución de: "Llevar a cabo el registro de los sistemas de datos personales en posesión de los entes públicos".

Envestido de dichas facultades y obligaciones, el Instituto creó a través de los Lineamientos para la Protección de Datos Personales, publicados en la Gaceta Oficial del Distrito Federal del 26 de octubre de 2009, el *Registro Electrónico de Sistemas de Datos Personales*. El Registro se define en los propios Lineamientos como una "aplicación informática desarrollada por el Instituto para la inscripción de los sistemas de datos personales en posesión de los entes públicos" (numeral 3, fracción XV, de los Lineamientos).

Una vez que se ha explicado el origen y vigencia normativa del Registro, así como de su utilidad y justificación en el contexto del régimen de protección de datos personales para el Distrito Federal, es pertinente continuar con las características de dicho Registro. Ante esto, surge a menudo la pregunta básica: ¿en qué momento se registran los sistemas de datos personales?

Los Lineamientos en la materia prevén en el numeral 10 que todos los sistemas deberán inscribirse en el Registro a cargo del Instituto, en un plazo no mayor de 10 días hábiles siguientes a la publicación del Acuerdo de creación, modificación o supresión de sistemas de datos

personales publicado en la Gaceta Oficial. Lo fundamental aquí es que ni un solo sistema de datos personales quede fuera del Registro, por lo que aquellos sistemas existentes previos a la Ley de Protección de Datos Personales para el Distrito Federal y a cualquier acuerdo, deben inscribirse en el Registro inmediatamente después de que el Instituto ponga en funcionamiento dicha herramienta informática.

El artículo 8 de la Ley en comento prevé la información mínima que debe contener cada uno de los registros de las unidades de sistemas de datos personales que se inscriban en el Registro, a saber:

I. Nombre y cargo del responsable y de los usuarios;

II. Finalidad del sistema;

III. Naturaleza de los datos personales contenidos en cada sistema;

IV. Forma de recolección y actualización de datos;

V. Destino de los datos y personas físicas o morales a las que pueden ser transmitidos;

VI. Modo de interrelacionar la información registrada;

VII. Tiempo de conservación de los datos, y

VIII. Medidas de seguridad.

A estos requisitos, el Instituto de Acceso a la Información Pública del Distrito Federal añadió, vía los Lineamientos en la materia aludidos, los siguientes más:

- Nombre del sistema y, en su caso, la fecha de publicación en la Gaceta Oficial del Distrito Federal (numeral 11, fracción I, de los Lineamientos);

- Los usos previstos y el soporte en que se encuentran (numeral 11, fracción III, de los Lineamientos);
- La categoría de los datos personales contenidos en el sistema, forma de recolección y actualización de los mismos (numeral 11, fracción IV de los Lineamientos);
- Unidad Administrativa en la que se encuentra el sistema (numeral 11, fracción V, de los Lineamientos);
- Teléfono y correo electrónico del responsable (numeral 11, fracción VIII, de los Lineamientos);
- Normatividad aplicable al sistema (numeral 11, fracción IX, de los Lineamientos);
- Indicación del nivel de seguridad aplicable: básico, medio o alto (numeral 11, fracción X de los Lineamientos).

Es importante mencionar que el acto de inscripción de los sistemas de datos personales en el Registro genera un folio que la Unidad Administrativa y el responsable del sistema conservarán para los efectos de que funja como comprobante del registro del sistema de datos personales.

En correspondencia con la creación del Registro y su manejo, se encuentra el derecho de las personas a conocer de su existencia y, sobre todo, de su contenido. Por ello, el Registro debe, a su vez, ser público y estar colocado en un lugar visible que permita su acceso fácil y amigable para los sujetos de la información y, en general, para la ciudadanía, en concordancia con el principio de máxima publicidad de los actos del Estado que establece la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, así como el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos.

El *Registro Electrónico de Sistemas de Datos Personales* es pues la manera más correcta de transparentar hacia la ciudadanía la existencia de sistemas de datos personales, su tratamiento y contenido, en cumplimiento con los principios de legitimidad, finalidad y seguridad de los datos personales que la propia Ley en comento establece.

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;

II. Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas;

III. De las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos;

IV. De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por disposición de una Ley sean considerados públicos;

V. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y

VI. Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

Cuando se utilicen cuestionarios u otros impresos para la obtención de los datos, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el presente artículo.

En caso de que los datos de carácter personal no hayan sido obtenidos del interesado, éste deberá ser informado de manera expresa, precisa e inequívoca, por el responsable del sistema de datos personales, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad de lo previsto en las fracciones I, IV y V del presente artículo.

Se exceptúa de lo previsto en el presente artículo cuando alguna ley expresamente así lo estipule.

Asimismo, tampoco regirá lo dispuesto en el presente artículo cuando los datos personales procedan de fuentes accesibles al público en general.

Isabel Davara F. de Marcos

COMENTARIO

Información en la recogida de datos

El artículo 9 regula el principio de información en el momento de recabar los datos. Tras enumerar los principios en el artículo anterior, algunos son desarrollados a lo largo del Capítulo II, relativo a los sistemas de datos personales, tal y como por ejemplo ocurre con el principio de información que es objeto de este artículo.

El principio de información es un principio esencial de la protección de datos que al mismo tiempo se convierte en una obligación del responsable del tratamiento.

Los titulares de los datos tienen derecho a conocer los tratamientos que sobre éstos se hacen, aun cuando no se necesite su consentimiento para ello.

Es así que el citado principio de información puede ponerse en relación con el de la lealtad del tratamiento establecido en el principio de calidad de los datos, pues esta obligación vendría más de la exigencia de un tratamiento leal que de uno legal. Se trata de que el interesado pueda estar en disposición de conocer el tratamiento de sus datos, No obstante, evidentemente pueden existir casos en los que haya una ley que exima de dicho conocimiento; por ejemplo, por razones de seguridad.

Es decir, el conocimiento del interesado sobre el tratamiento de sus datos tiene que garantizarse siempre[35], aunque el consentimiento haya sido excepcionado[36].

---

[35] No obstante, la necesidad de información puede quedar igualmente excepcionada en supuestos concretos, tales como la necesidad de seguridad pública, etc.

[36] Si se atiende a las normas internacionales en materia de protección de datos, todas contemplan el principio de información en la recogida de datos de carácter personal, lo que demuestra claramente que se trata de un principio que legítima el tratamiento de datos de carácter personal.

Datos recabados del interesado o de un tercero

Este artículo se encuentra dividido en dos grandes supuestos: que la recogida de datos provenga del titular, que sea el que preste la información, o que dichos datos se recaben de un tercero.

En ese sentido, cuando los datos se recaban del propio interesado, es necesario que el responsable del tratamiento le informe[37], con carácter previo, de los siguientes aspectos:

I. De la existencia de un sistema de datos personales, del tratamiento de datos personales, de la finalidad

---

[37] Resulta muy interesante, en nuestra opinión, unir el estudio de este artículo con lo prescrito en la Resolución (73) del Comité de Ministros del Consejo de Europa:

> *29. This principle seeks to establish a balance between the legitimate interests of the individuals concerned and the general interests served by electronic data banks. It was drafted after due consideration of the following questions*
>
> *(a) whether an individual should have the right to be informed of the nature of the data stored on him ;*
>
> *(b) whether he should have the right to be informed of the actual data stored on him;*
>
> *(c) whether he should have the right to be informed of the use of the data stored on him and, particularly, of any provision of information that has taken place;*
>
> *(d) whether there should be any duty for those responsible for the data bank to keep an individual informed about the data held concerning him.*
>
> *30. The committee thought that the questions at (a), (b) and (c) above should be answered, in principle, in the affirmative. Some provision for a person to learn what information is held about him was considered to be an essential minimum element in the protection of privacy. However, there are cases in which knowledge about certain kinds of information, such as a medical or psychiatric file, may be harmful to the individual.*
>
> *31. The question posed under (d) has been answered in the negative. The committee recognised that it would be appropriate to expect the individual to acquaint himself at the data bank about the information held concerning him.*
>
> *In many cases, a person will have very little interest in knowing what information is stored about him. Moreover the provision of automatic print-outs might harm the cause of privacy (e.g. because print-outs may get misdirected in the mail); finally a general right of print-out might unreasonably hamper the development of data processing, for it could place a heavy burden on the users."*

De lo anterior, creemos importante resaltar cómo se ha unido el principio de la información con el derecho de acceso, que, evidentemente, es acceso a información. Y así, vemos que es responsabilidad del responsable del fichero informar de una serie de extremos al titular de los datos, pero que, el Comité de Ministros entiende que es el titular de los datos el que tiene que dirigirse al responsable del fichero para conocer la información que de él se trata.

de la obtención de éstos y de los destinatarios de la información;

II. Del carácter obligatorio o facultativo de responder a las preguntas que les sean planteadas;

III. De las consecuencias de la obtención de los datos personales, de la negativa a suministrarlos o de la inexactitud de los mismos;

IV. De la posibilidad para que estos datos sean difundidos, en cuyo caso deberá constar el consentimiento expreso del interesado, salvo cuando se trate de datos personales que por disposición de una Ley sean considerados públicos;

V. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y

VI. Del nombre del responsable del sistema de datos personales y en su caso de los destinatarios.

Si los datos se recogen a través de un tercero, distinto al propio interesado, entonces el responsable del tratamiento tiene obligación de informar al interesado, dentro de los tres meses siguientes al registro de los datos[38], de los siguientes extremos:

a) de la existencia de un sistema de datos personales,

b) del tratamiento de datos personales,

c) de la finalidad de la obtención de los datos,

d) de los destinatarios de la información,

e) 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;

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

Es decir, se trata de garantizar en todo momento que el interesado, aun cuando los datos no hubieran sido obtenidos del mismo, esté

[38] De nuevo, siguiendo la Ley española.

en condiciones de conocer el tratamiento de sus datos de carácter personal a través de la información que recibe; consentir, en su caso, la comunicación a terceros; y ejercitar los derechos que le reconoce la Ley.

Cuestionarios u otros impresos

Siguiendo con el análisis del artículo, éste se refiere a la inclusión de la información en aquellos documentos que se utilicen para la recogida de datos personales, indicando lo siguiente: *"Cuando se utilicen cuestionarios u otros impresos para la obtención de los datos, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el presente artículo."* En este caso, resulta claro que la Ley ha venido a copiar una previsión de la Ley española en materia de protección de datos. Esta previsión tiene que leerse en sentido amplio, puesto que por cuestionario u otro impreso debe entenderse tanto el soporte papel como electrónico.

La interpretación es necesaria por ser ésta una norma de Nuevas Tecnologías y porque ya a la fecha muchas de las relaciones que se establecen entre la Administración con los ciudadanos se llevan a cabo a través de medios electrónicos.

Es así que cualquiera que sea el formato en el que se encuentre el formulario, cuestionario u otro documento que se utilice para la recogida de datos, es necesario que éste incluya una cláusula o leyenda informativa que contenga los requisitos establecidos en este artículo, a efectos de informar al interesado sobre el tratamiento de sus datos de carácter personal.

Unido a lo anterior, el apartado específicamente establece que los requisitos en materia de información tienen que figurar "en forma claramente legible". Dicha previsión nos recuerda varias cosas. En primer lugar, que el interesado sólo puede dar un consentimiento informado, cuando éste sea necesario, conforme la información que se le proporcione y, en particular, en cuanto a la finalidad o finalidades con la que se tratarán los datos, así como, en su caso, las cesiones de datos a terceros. Y en segundo lugar, que en aras de garantizar que el interesado comprende las consecuencias del tratamiento de sus

datos de carácter personal, es necesario proporcionarle información clara y sencilla, sin utilizar términos complejos o sin remisiones a otros lugares para obtenerla.

Las Administraciones Públicas tienen que asegurarse de que todos los formularios o cuestionarios que utilicen para la recogida de datos de carácter personal incluyen una cláusula informativa, ya que de otra manera el tratamiento no cumpliría con este principio dejando al interesado desprotegido al no saber quién y para qué se tratarán sus datos.

Excepciones al principio de información

La regla general de información al interesado también tiene sus excepciones, entre las que destacamos el hecho de que una ley así lo prevea. Por ejemplo, por razones de seguridad de cualquier tipo, en el que proporcionar dicha información al afectado implicaría no poder cumplir con la finalidad de dicho tratamiento.

Si bien hay supuestos en los que claramente la información pondría en riesgo la finalidad del tratamiento, por razones de seguridad u otras que requieran un tratamiento sin informar al interesado, es necesario distinguir caso por caso cuándo la información tiene o no tiene que ser facilitada.

Es decir, puede haber supuestos en los que si bien el tratamiento viene obligado por la Ley (y por lo tanto no es forzoso el consentimiento del titular), aun así es necesario informar al interesado de éste con la finalidad de que pueda conocerlo y ejercitar sus derechos, de manera que no pierda control sobre el tratamiento de sus datos.

Es importante que se prevean aquellos supuestos en los que la Ley puede requerir el tratamiento de datos que no sean obtenidos directamente del propio interesado, de manera que habrá que evaluar también caso por caso la obligación de informar a los interesados del tratamiento de sus datos de carácter personal en estas situaciones o si queda exceptuada por exigir un esfuerzo desproporcionado.

Llama la atención el hecho de que el artículo que venimos comentando indique: "*tampoco regirá lo dispuesto en el presente artículo cuando los datos personales procedan de fuentes accesibles al público en general*"[39].

Si bien la previsión anterior supone una excepción a la obligación de informar al interesado cuando sus datos sean obtenidos de una fuente de acceso público[40], ésta supone que el interesado no pueda saber quién trata sus datos y, por tanto, a quién dirigirse para ejercitar sus derechos de acceso, rectificación, cancelación y oposición. Entendemos que el legislador ha querido liberar al responsable del tratamiento de la obligación de dirigirse al interesado para informarle, puesto que ello sería costoso y, en ocasiones, demasiado complejo.

Un análisis completo del principio de información requiere tener en consideración lo dispuesto en los Lineamientos de la Ley, a los que nos remitimos expresamente, dado que en ellos se incluyen previsiones sobre el deber de información, un modelo de leyenda informativa y, por último, las excepciones al deber de información cuando los datos no hayan sido obtenidos directamente del interesado.

Estas excepciones, unidas al último párrafo del artículo 9, dejan claro que el legislador ha eximido al responsable del tratamiento de informar al interesado sobre el tratamiento de sus datos de carácter personal cuando éstos no se hayan obtenido directamente de él. Excepción ésta que se aplicará conforme a lo previsto tanto en la Ley como en los Lineamientos, si bien no podemos dejar de señalar que ambas utilizan conceptos jurídicos indeterminados y que, por tanto, será necesario atender a la práctica seguida en la materia para ver en qué casos procede o no dicha excepción.

---

[39] Previsión que de nuevo nos recuerda el último apartado del artículo 5 de la LOPD que establece *"tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público"*.

[40] En relación con el concepto de fuente de acceso público es necesario atender a los Lineamientos de la Ley, que lo define en la fracción IX de su apartado 3.

Artículo 10.- Ninguna persona está obligada a proporcionar datos personales considerados como sensibles, tal y como son: el origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual.

Queda prohibida la creación de sistemas de datos personales que tengan la finalidad exclusiva de almacenar los datos personales señalados en el párrafo anterior y sólo pueden ser tratados cuando medien razones de interés general, así lo disponga una ley, lo consienta expresamente el interesado o, con fines estadísticos o históricos, siempre y cuando se hubiera realizado previamente el procedimiento de disociación.

Tratándose de estudios científicos o de salud pública el procedimiento de disociación no será necesario.

Miguel Carbonell

COMENTARIO

En la teoría de la protección de datos personales se suelen distinguir dos conceptos: el de datos personales en sentido amplio y el de información sensible. En este segundo caso se trataría también de datos personales, pero por su importancia y estrecha vinculación con el principio de dignidad de la persona, algunas legislaciones estiman que merecen una protección reforzada.

Es el caso del legislador del Distrito Federal, que para fortalecer la protección de ciertos datos que se califican como "sensibles", establece en el artículo 10, que ahora comentamos, la posibilidad de que toda persona se niegue a proporcionar información sobre su origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual.

¿Qué es lo que justifica que, sobre tales datos, el titular pueda guardar una reserva absoluta, negándose, incluso, a hacerlos del conocimiento de cualquier autoridad y aun de cualquier particular?

Si lo analizamos con cierto detenimiento veremos que se trata de características que corresponden a la llamada privacidad o vida privada de las personas[41].

Se trata de características que configuran nuestra identidad y que nos permiten diferenciarnos de las demás personas. Pero además, son cuestiones que no tienen relevancia (o no deberían tenerla) en la esfera pública. Es decir, para efecto de cualquier trámite o asunto que se ventile ante los órganos del Estado mexicano, da igual nuestro origen étnico o racial, nuestras características morales, nuestra ideología, nuestras preferencias sexuales, etcétera.

En esa virtud, dada la indiferencia con que se deben tratar esas características, no tiene sentido que se nos pida información sobre ellas. De hecho, si una persona cuenta con ese tipo de información sobre nosotros, corremos el riesgo de ser discriminados[42]. El conocimiento de información que pertenece a la vida privada es un factor de potencial trato discriminatorio y por eso tiene plena justificación y sentido lo que dispone el artículo 10 de la Ley que estamos analizando.

---

[41] Para las cuestiones conceptuales sobre la intimidad, la vida privada y la publicidad, ver Garzón Valdés, Ernesto, "Lo íntimo, lo privado y lo público" en Carbonell, Miguel (coordinador), *Problemas contemporáneos de la libertad de expresión*, México, Porrúa, CNDH, 2004, pp. 39 y siguientes. Una aproximación jurídico-constitucional al tema en Carbonell, Miguel, *Los derechos fundamentales en México*, 3ª edición, México, Porrúa, CNDH, UNAM, 2009, pp. 455 y siguientes (con bibliografía adicional).

[42] Sobre el régimen constitucional del derecho a la no discriminación, Carbonell, Miguel, *Los derechos fundamentales en México*, cit., pp. 183 y siguientes.

Ahora bien, el segundo párrafo del mismo artículo añade un matiz interesante, que sirve para aclarar el alcance del párrafo primero. Los datos que corresponden a la llamada "información sensible" no pueden ser almacenados en sistemas de datos personales. Es decir, la Ley contempla la posibilidad de que tales datos, si el titular voluntariamente los proporciona, pueden estar en manos de alguna autoridad, pero limita los supuestos en los que eso puede llegar a darse.

Señala el párrafo segundo del artículo 10 que el tratamiento de tales datos solamente puede ocurrir cuando medien razones de interés general, cuando así lo disponga una ley, cuando exista consentimiento del titular o cuando sean solicitados para efectos estadísticos o históricos (debiendo existir un procedimiento de disociación, que es definido por el artículo 2 de la Ley que comentamos de la siguiente manera: "Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a una persona física identificada o identificable").

El procedimiento de disociación se exceptúa cuando se trate de estudios científicos o de salud pública.

La comprensión global del alcance del artículo 10 nos permite llegar a concluir que, como regla general, ninguna autoridad debe nunca pedirnos información acerca de los temas a los que se refiere el párrafo primero del propio artículo. Si esa información llega a manos de alguna autoridad local, se deberá observar lo dispuesto en los párrafos segundo y tercero del citado precepto.

Sería mejor que nunca se diera esa información, salvo casos muy precisos y que estén plenamente justificados, dado que se trata de información que ni siquiera para efectos estadísticos parece relevante. Por ejemplo, sólo será relevante el tratamiento de datos personales relativos al origen étnico para el acceso a programas sociales o apoyos para grupos específicos de población como personas de alguna comunidad indígena.

Artículo 11.- Los archivos o sistemas creados con fines administrativos por las dependencias, instituciones o cuerpos de seguridad pública, en los que se contengan datos de carácter personal, quedarán sujetos al régimen general de protección previsto en la presente Ley.

Los datos de carácter personal obtenidos para fines policiales, podrán ser recabados sin consentimiento de las personas a las que se refieren, pero estarán limitados 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, debiendo ser almacenados en sistemas específicos, establecidos al efecto, que deberán clasificarse por categorías en función de su grado de confiabilidad.

La obtención y tratamiento de los datos a los que se refiere el presente artículo, podrán realizarse exclusivamente en 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.

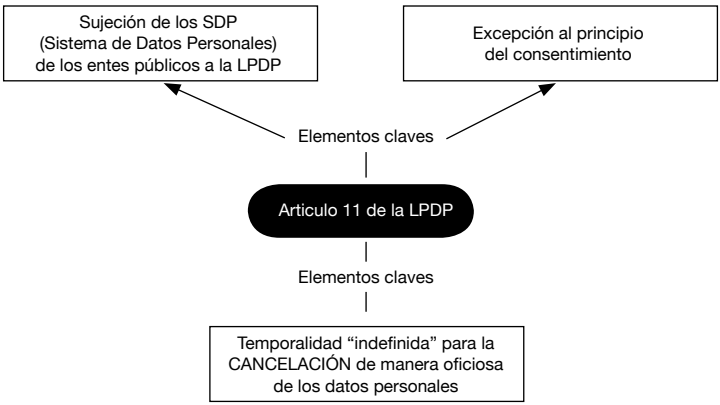
Los datos personales recabados con fines policiales se cancelarán cuando no sean necesarios para las investigaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del interesado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Issa Luna Pla

COMENTARIO

Del artículo 11 de la Ley de Protección de Datos Personales para el Distrito Federal (LPDP), podemos desprender diversos elementos clave que es posible ilustrar en el siguiente esquema:



El primer párrafo del artículo en comento establece que todos los sistemas de datos personales creados por los entes públicos deberán sujetarse a lo establecido por la Ley de Protección de Datos Personales para el Distrito Federal, haciendo un especial énfasis en los sistemas creados por las instituciones y cuerpos de seguridad pública.

Entre los sistemas de datos creados por las instituciones o cuerpos de seguridad del Distrito Federal, a pesar de estar sujetos a todos los principios y modalidades del resto de los sistemas en posesión de los otros entes públicos, existen someras diferencias que podrían distinguirlos del resto. Una de estas primeras diferencias es la excepción al principio del consentimiento, ya que la primera parte del párrafo segundo del artículo en comento señala que los datos personales "podrán ser recabados sin consentimiento de las personas a las que se refieren…", es decir, establece una facultad optativa, la cual podría considerarse una excepción al principio del consentimiento establecido en el artículo 5 de la misma Ley. Sin embargo, si realizamos una lectura armónica del resto de los demás artículos, podemos ver que esta diferencia se podría desvanecer al momento de observar la fracción I del artículo 16 de la Ley, que establece la excepción a este principio del consentimiento, al señalar que los entes públicos quedan exentos de requerirlo "cuando se recaben (datos personales) para el ejercicio de las atribuciones legales conferidas…", no obstante, la diferencia real radica en que esta excepción será aplicable exclusivamente "… 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…"[43]. Así, es una singularidad que se encuentra supeditada a la finalidad de datos personales que son estrictamente necesarios para el cumplimiento de una de las misiones fundamentales que tiene el Estado, que es la preservación del orden público.

El artículo en comento no se circunscribe exclusivamente a señalar la posibilidad de la creación o legitimación de los sistemas de datos personales de este tipo, sino que establece la obligación de las instituciones o cuerpos de seguridad de implementar los niveles de seguridad idóneos para la custodia y conservación de este tipo de datos personales, que por el contexto en el que se encuentran localizados presentan un nuevo estatus, por lo que son los especialmente protegidos. Dentro de ese tenor de ideas, la Ley de Protección de Datos Personales para el Distrito Federal señala que los niveles de seguridad que deben emplearse, son el medio y alto. El primer nivel señalado aplica a aquellos sistemas que contengan las infracciones penales, donde es pertinente aclarar que el artículo en comento no sólo se restringe a las investigaciones en curso, sino que también es aplicable a aquellas que se han concluido, tal como lo señalan el penúltimo y el último párrafos. El siguiente nivel de seguridad es el alto, y será aplicable a datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos, e incluso, debido a los avances de las ciencias y de la tecnología, también se deberá aplicar al ADN, datos Biométricos, reconocimiento facial, etc.; el límite en la recolección de este tipo de datos personales se encontrará íntimamente relacionado con el objetivo de la investigación que se encuentre realizando la institución o cuerpo de seguridad[44].

La Agencia Española de Protección de Datos Personales, en la resolución R/00753/2007, ha reconocido que el reconocimiento facial 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…" que válidamente encuadra dentro de la hipótesis contemplada en el artículo 22.2 de la

---

[43] Párrafo segundo del artículo 11, de la Ley.

[44] Párrafo tercero del artículo 11 de la Ley.

Ley Orgánica 15/1999[45]; con lo cual, se abre la posibilidad de que una infinidad de datos personales sean recolectados por las instituciones o cuerpos de seguridad. Es de resaltar que, hasta este momento, el Instituto de Acceso a la Información Pública del Distrito Federal no ha emitido un criterio específico sobre la interpretación y alcances del segundo párrafo del artículo 11 de la Ley en comento.

La doctrina del *Habeas Data* ha señalado que este tipo de sistemas de datos personales, al tener una reserva al principio de excepción, no implica que los legisladores los hayan exceptuado de los demás principios inmersos en la materia, es decir, los principios de legalidad, calidad, confidencialidad, deber de secreto, entre otros. Dentro de este contexto de seguridad pública, toman una mayor relevancia estos principios, ya que en su omisión o inobservancia, podrían afectarse la credibilidad y la honra de las personas y la procuración de la justicia, no sólo en el ámbito del Distrito Federal, sino también en el ámbito nacional e internacional; lo anterior, en virtud de los diversos convenios de colaboración que se tienen firmados sobre la materia.

Por último, el artículo en comento, señala que los datos personales que se encuentran almacenados dentro de este tipo de sistemas de datos personales, deberán ser cancelados[46] cuando ya no sean necesarios para la investigación que motivó su recolección en una primera instancia, agregando que para tal efecto se deberán tomar en consideración diversos elementos:

---

[45] El artículo 22.2 de la Ley Orgánica 15/1999, contempla la misma excepción que el artículo 11 de la LPDP, al señalar:
"Artículo 22. Ficheros de las Fuerzas y Cuerpos de Seguridad.
…
"2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad…"

[46] El Instituto de Acceso a la Información Pública del Distrito Federal, ha señalado en el lineamiento 3, fracción III, de los Lineamientos para la Protección de Datos Personales en el Distrito Federal, lo que se deberá entender por el término de cancelación:

> "…Eliminación de determinados datos de un sistema de datos personales previo bloqueo de los mismos"

1. Edad del interesado

2. El carácter de los datos personales

3. La necesidad de mantenerlos hasta la conclusión de la investigación o procedimiento concreto.

4. La emisión de una resolución judicial firme (en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidades).

Como se puede observar en los numerales anteriores, los elementos a considerar son amplios, y no sólo basta que los datos recabados ya no sean idóneos para la investigación en concreto; esto se debe al tipo de sistemas de datos que se aborda en el artículo en comento. Sirva de ejemplo de lo anterior, la resolución antes citada de la Agencia Española de Protección de Datos Personales, en donde la autoridad responsable, señaló que:

> *… La [Dirección General de la Policía y de la Guardia Civil] ha informado que, tras haberse formulado diversas denuncias por frecuentes hurtos de carteras en el trayecto de dos líneas de autobuses urbanos de la ciudad de (.....), por parte de la Comisaría de (.....) se inició una investigación consistente en la localización de un individuo que había sido detenido recientemente por hurtos de carteras en autobuses y de su acompañante habitual (de los que se disponía de una fotoreseña)…*

En este caso, la información que obraba previamente en el SDP de la Dirección General de la Policía y de la Guardia Civil ha servido de base para la persecución de un delito.

En conclusión, el artículo 11 de la Ley de Protección de Datos Personales para el Distrito Federal establece los requisitos esenciales para los sistemas de datos personales en materia de seguridad pública, es decir, da la forma y parámetros dentro de los cuales las instituciones o cuerpos de seguridad deben moverse en la materia de datos personales, así como los límites y temporalidades de custodia y conservación.

Artículo 12.- Los responsables de los sistemas de datos personales con fines policiales, para la prevención de conductas delictivas o en materia tributaria, podrán negar el acceso, rectificación, oposición y cancelación de datos personales en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, así como cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones.

Issa Luna Pla

COMENTARIO

El artículo 12 de la Ley de Protección de Datos Personales está localizado en el Capítulo II de los Sistemas de Datos Personales y trata de un tipo excepcional de la tutela de los datos personales. El texto normativo que a continuación se analiza se inserta dentro de las causales de excepción al acceso de los datos personales que puede ser legalmente fundamentada y motivada ante un solicitante o titular de los datos.

Sirva primero situar el tipo de mandato de excepción que el artículo 12 de la Ley en comento promueve en el marco de la doctrina internacional de la protección de datos personales. Inicialmente, en el derecho comparado de las leyes en la materia se identifican dos tipos de excepciones a los derechos de acceso, rectificación, cancelación y oposición, conocidos como los derechos ARCO, así como a la protección y tutela de los datos.

Por un lado, en la doctrina encontramos que existen excepciones legales para la recolección de los datos. Esto es, cuando se trata de fines de seguridad pública, seguridad nacional, defensa militar, o actividades del Estado relacionadas con la procuración de justicia penal, donde las leyes de protección de datos personales permiten que sea el mismo Estado el que, al margen del principio de consentimiento del titular de los datos, recolecte datos y conforme sistemas. Aunque esta facultad del Estado es amplia cuando un bien jurídico mayor se debe proteger, tal como la seguridad nacional, dichos sistemas de datos creados *excepcionalmente* no deberán apartarse del principio

de finalidad, que da naturaleza a su creación, ni faculta al ente público para violar las garantías de la protección de los datos personales.

Ahora bien, en la doctrina internacional existen también excepciones a la norma para el ejercicio de los derechos ARCO y este es precisamente el referente jurídico al que obedece el artículo 12 de la Ley en comento. Tanto a los titulares de los datos personales, como a otros interesados en conocerlos, el Estado podrá negar el acceso cuando un bien jurídicamente mayor a los derechos ARCO se pretende proteger.

Del presente artículo analizado, es posible deducir cuáles son aquellos bienes jurídicos mayores a los derechos ARCO que la Ley de Protección de Datos Personales contempla:

I. Datos personales con fines policiales;
II. Con fines de prevención de conductas delictivas;
III. En materia tributaria.

Los primeros datos personales se refieren a aquellos que detenta la autoridad policial del Distrito Federal con motivo del uso y ejercicio de sus facultades de garantizar la seguridad pública de los ciudadanos. Pero también hay autoridades que cumplen una función de prevención del delito, y para ello la segunda causal de excepción faculta a las entidades públicas para negar el acceso a los datos, siempre y cuando cuenten con el magisterio de la ley para tales efectos. En ambos supuestos, el I y II, se entiende que el legislador otorgó prioridad al derecho de todos los ciudadanos a la seguridad pública y nacional, en comparación con el derecho fundamental individual del acceso, rectificación, corrección y oposición. Es decir, que la excepción al acceso es efectiva cuando abrir o revelar datos personales pueda contribuir de manera determinante a poner en riesgo la seguridad pública del Distrito Federal o la nacional.

El supuesto III de excepción al ejercicio de los derechos ARCO en el artículo 12 de la Ley en comento, es donde se presenta la reserva a datos en materia tributaria. Este supuesto de excepción es quizás uno de los más antiguos donde la confidencialidad se considera absoluta

y el resguardo de los datos recae en la autoridad tributaria. El Fisco detenta toda la información que los contribuyentes le entregan, en cumplimiento con la obligación de tributar de los mexicanos, prevista en el artículo 31 de la Constitución Política de los Estados Unidos Mexicanos. Siendo este el origen de los sistemas de datos personales y no mediante un acuerdo emitido por el titular de alguna entidad pública, nos encontramos, en este caso, ante una materia de peculiares características.

El Código Fiscal de la Federación establece en el artículo 69, sobre las obligaciones de los servidores públicos, la de la confidencialidad absoluta de los datos del contribuyente, a saber:

> El personal oficial que intervenga en los diversos trámites relativos a la aplicación de las disposiciones tributarias estará obligado a guardar *absoluta reserva* en lo concerniente a las declaraciones y datos suministrados por los contribuyentes o por terceros con ellos relacionados, así como los obtenidos en el ejercicio de las facultades de comprobación…

Pero esta reserva absoluta sobre los datos personales en materia fiscal tiene ciertas excepciones que el mismo artículo 69 prevé y que se basan en criterios ajenos al régimen de protección de datos personales que novedosamente la Ley para el Distrito Federal propone. Así, la reserva no aplica en aquellos casos donde deba suministrarse información de los contribuyentes a funcionarios encargados de la defensa y administración de los intereses fiscales y a las autoridades judiciales en procesos del orden penal; a los tribunales competentes que conozcan de pensiones alimentarias; a quienes autorice el Secretario de Hacienda y Crédito Público; los que se entreguen a las Sociedades de Información Crediticia; y al Consejo Técnico del Instituto Federal Electoral, entre otros.

Cabe aclarar que en ninguno de estos casos, y puesto que el régimen de confidencialidad de la información de los contribuyentes es póstumo al de protección de datos personales, se aplica el principio de la finalidad de los datos personales. Sin embargo, recordando el mandato del artículo 12 en comento, la excepción al acceso para

el Distrito Federal se entenderá en el marco de las actividades de orden penal con motivo de la persecución de delitos tributarios y del ejercicio eficiente de las atribuciones de la autoridad.

Dicho lo anterior, de las tres causales de excepción al ejercicio de los derechos ARCO, el legislador asumió la restricción al ejercicio de los derechos ARCO sobre los datos personales que se pudieran encontrar en alguna de las tres casillas de excepción consideradas en el artículo 12 de la Ley, las consecuencias o peligros que impliquen para:

- La defensa del Estado;
- La seguridad pública;
- La protección de los derechos y libertades de terceros;
- Las necesidades de las investigaciones que se estén realizando;
- Que obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones.

Es así que los límites al ejercicio de los derechos ARCO vienen a ser determinados en cierta forma dentro del texto normativo del artículo 12 de la Ley, establecidos como intereses que pudieran ponerse en peligro. Sin embargo, el tratamiento que el legislador dio a dichos intereses fue a raja tabla cuando en la experiencia comparada se ha demostrado que no todos pueden ser demostrados por las mismas vías, ni tampoco llevan a las mismas consecuencias jurídicas.

De esta forma, la defensa del Estado y la seguridad pública son casos del llamado "interés público". Se trata de un concepto que requiere de una justificación de los principios socialmente aceptados mediante la interpretación de la ley, acto que corre a cargo de un tribunal supremo con las facultades para dirimir la interpretación constitucional. En términos prácticos, la doctrina ha definido el interés público como la norma ética suprema aplicable a los asuntos políticos que afectan a la sociedad en general. Por tanto, negar el ejercicio de los derechos ARCO por causas que puedan dañar al interés público de la defensa nacional y la seguridad pública, debidamente fundamentado y motivado, no

equivale a poner en peligro los derechos de terceros individuales y los procesos de toma de decisiones políticas, por ejemplo.

Para las leyes de Transparencia y Acceso a la Información Pública, las causales de reserva de información cuando pueden dañar la defensa y seguridad del Estado o pública, son demostradas a través de herramientas del derecho denominadas como "pruebas de daño", que no son otra cosa que la aplicación de principios objetivos y certeros para probar que revelar la información causaría un daño probable y presente. Pero en el caso de la afectación de derechos de la personalidad, el tipo de pruebas se conocen como "pruebas de interés público", donde se demuestra que existe un interés general supremo por conocer la información que se reserva a costa del interés individual del titular de los datos personales.

Ahora bien, el artículo 12 de la Ley en comento también autoriza a la entidad pública para negar el ejercicio de los derechos ARCO en los casos donde se lleven a cabo procesos de investigación judicial o que "obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones". Igualmente, estos dos tipos de intereses susceptibles a ser dañados son necesarios para asegurar la adecuada conducción de los procesos judiciales, así como los procesos de toma de decisiones de la autoridad cuando los datos personales podrían obstaculizarlos. Estos supuestos deben demostrarse con razonamiento fundamentado y motivado de la autoridad a cuyo cargo se desarrollen dichos procesos.

Finalmente, cabe aclarar que tanto la Ley de Protección de Datos Personales como sus Lineamientos no consideran en ninguna de sus partes las pruebas de interés público o las pruebas de daño, aunque si es posible encontrar dicha prueba en la Ley de Transparencia de la entidad. Por tanto, el proceso de balance de los intereses y los derechos quedaría a cargo del mecanismo de recurso de revisión que el Instituto de Acceso a la Información Pública está facultado para ejecutar en el caso de inconformidad por parte del titular de los datos en el ejercicio de sus derechos ARCO. En caso de agotar este recurso, el interesado en los datos podrá recurrir a la vía jurisdiccional donde buscará que una autoridad competente acuda al control de proporcionalidad para balancear los derechos en conflicto.

Artículo 13.- Los entes públicos establecerán las medidas de seguridad técnica y organizativa para garantizar la confidencialidad e integralidad de cada sistema de datos personales que posean, con la finalidad de preservar el pleno ejercicio de los derechos tutelados en la presente Ley, frente a su alteración, pérdida, transmisión y acceso no autorizado, de conformidad al tipo de datos contenidos en dichos sistemas.

Dichas medidas serán adoptadas en relación con el menor o mayor grado de protección que ameriten los datos personales, deberán constar por escrito y ser comunicadas al Instituto para su registro.

Las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público o, en su caso, la persona física o moral que intervengan en el tratamiento de datos personales con el carácter de responsable del sistema de datos personales o usuario, según corresponda. Cuando se trate de usuarios se deberán incluir los datos del acto jurídico mediante el cual, el ente público otorgó el tratamiento del sistema de datos personales.

En el supuesto de actualización de estos datos, la modificación respectiva deberá notificarse al Instituto, dentro de los 30 días hábiles siguientes a la fecha en que se efectuó.

Isabel Davara F. de Marcos

COMENTARIO

Dada su importancia, especialmente en la práctica, la Ley dedica a las medidas de seguridad un capítulo entero.

Así, el Capítulo III, artículos 13 al 15, regula las medidas de seguridad que tienen que adoptar los entes públicos que traten datos de carácter personal.

El principio de seguridad[47] de datos es quizá uno de los más llamativos[48] dentro de la normativa sobre protección de datos[49]. Por una parte, porque, como dijimos, la Ley le dedica un Capítulo entero, y, por otra, como consecuencia, a su vez, de la anterior, porque constituye uno de los más susceptibles en cuanto a la comisión de infracciones.

De lo anterior, cabe destacar varias cosas:

1. Tanto el responsable del sistema de datos como el encargado del tratamiento de los datos por cuenta de aquél, es decir, todos los que accedan o traten datos de carácter personal, tienen la obligación de adoptar y observar las medidas de seguridad.

2. Las medidas tienen que ser tanto técnicas como organizativas.

3. Lo que se persigue es garantizar la seguridad de los datos. En concreto, evitar su alteración, pérdida, tratamiento, transmisión o acceso no autorizado.

---

[47] Davara Rodríguez dice así: *"Queremos referirnos a la seguridad en tres aspectos: seguridad lógica, seguridad física y seguridad jurídica que deben ocupar un lugar prioritario en la implantación de los nuevos servicios y en todo tratamiento automatizado y/o telemático de datos de carácter personal, siendo importante el papel que debe jugar la seguridad y, consecuentemente, la auditoría de la seguridad."*, Davara Rodríguez, M. A., *Guía Práctica de Protección de datos para las PYMEs*, Madrid: Ed. Dafema, 2002, página 93.

[48] Que también podemos encontrar en la Resolución R (73) del Comité de Ministros del Consejo de Europa:

> *8. Precautions should be taken against any abuse or misuse of information. Electronic data banks should be equipped with security systems which bar access to the data held by them to persons not entitled to obtain such information, and which provide for the detection of misdirection of information, whether intentional or not.*

[49] El Convenio (108) que venimos analizando, también recoge este principio, aunque de manera más enunciativa, como corresponde a una norma de su tipo:
Artículo 7. Seguridad de los datos
Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

4. El parámetro de valoración para estas medidas es 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.

Además de lo anterior, el artículo establece otras previsiones relevantes, como, por ejemplo, que las medidas de seguridad deberán constar por escrito y ser comunicadas al Instituto para su registro. No obstante, esta previsión del artículo comentado debe ponerse en relación con el artículo 15 de la Ley, que indica que sólo se informará al Instituto de los niveles de seguridad.

El documento de seguridad

Por lo que se refiere a que las medidas de seguridad consten por escrito, la práctica seguida a nivel internacional, por el IFAI a nivel federal, y asimismo planteada por la Ley a nivel estatal, aconsejan la elaboración de un documento de seguridad que desarrolle las medidas de seguridad de índole técnica y organizativa a aplicar en cada situación.

En el caso de la Administración Pública Federal, el IFAI ha elaborado y publicado[50] una Guía para la elaboración de un Documento de Seguridad que permitirá a las dependencias y entidades públicas tener un documento de referencia a efectos de cumplir con la obligación de adoptar medidas de seguridad.

Nótese que la Guía debe entenderse como un modelo; queda claro que es obligación del ente público cumplir con las medidas de seguridad que le son exigibles en virtud de la normativa aplicable y que la Guía no sustituye al documento de seguridad, puesto que el responsable del sistema de datos personales y, en su caso, el usuario, tienen que adecuar las medidas de seguridad a los tratamientos que lleven a cabo.

---

[50] Véase la dirección de Internet http://www.ifai.org.mx/Ciudadanos/#datos_personales.

Las medidas de seguridad son las que establece la Ley y posteriormente se detallan en sus Lineamientos, de manera que tendrán que ser adoptadas por el responsable del sistema de datos personales y, en su momento, por el usuario. En este sentido, el documento es una obligación de quien trata datos personales.

La elaboración del documento de seguridad plantea algunas cuestiones que tendrán que ser consideradas en la práctica. Entre otras, cabe citar la actualización de dicho documento, lo que podría dar lugar a que pueda incluso plantearse qué partes de éste estarán impresas y cuáles se mantendrán en soporte electrónico, tanto por razones de operativa interna como por la necesidad de actualizarlas frecuentemente. La actualización es necesaria y supone que el documento de seguridad no sea un documento estático, sino vivo. En este sentido, cabe señalar que el documento de seguridad puede conservarse en soporte electrónico o en papel, y su actualización estará condicionada a los cambios que se establezcan en las políticas, o la rotación del personal involucrado en el cumplimiento de este documento.

Además, la práctica plantea varias alternativas, ya que quien tenga que cumplir con las medidas de seguridad puede optar por elaborar un único documento de seguridad para todos los sistemas de datos o archivos que contengan datos de carácter personal o, por el contrario, elaborar un documento de seguridad que agrupe los sistemas de datos o archivos a los que sea aplicable el mismo nivel de medidas de seguridad, teniendo en consideración que la Ley prevé tres niveles tal y como veremos más adelante.

Reiteramos, como ya hemos dicho en varias ocasiones en este trabajo, que el hecho de que el documento o partes de él se encuentren en soporte electrónico no supone un impedimento al cumplimiento de la obligación de que esté "por escrito".

Comunicación de las medidas de seguridad al Instituto

El artículo que analizamos establece también que las medidas de seguridad serán comunicadas al Instituto para su registro.

Consideramos que tal previsión debe ser analizada con el fin de aclarar su significado.

Por un lado, a efectos del registro de los sistemas de datos, cabe considerar que lo que se comunicará es el nivel de medidas de seguridad aplicable[51].

En la práctica, la obligación queda cumplida poniendo el documento de seguridad a disposición del Instituto cuando se suscite una visita de inspección, donde se establezca la revisión de las medidas de seguridad establecidas.

Igualmente, se reportarán al Instituto los cambios que se produzcan en las medidas de seguridad, reservándose sus tipos y características. Cumpliendo con estas obligaciones se garantiza que el responsable mantiene actualizadas las medidas de seguridad en todo momento, puesto que en caso de que se produzca una inspección tiene que garantizarse que se correspondan con las que hubieran sido registradas.

Adopción de medidas de seguridad por el responsable y el usuario

Siguiendo con el análisis del artículo es necesario analizar la previsión sobre la adopción de las medidas de seguridad por el responsable del sistema de datos personales y por el usuario que accede a datos de aquél para prestarle algún servicio.

No cabe duda de que ambos, como sujetos obligados por la normativa sobre protección de datos, tienen obligación de cumplir con las medidas de seguridad que les sean exigibles. Es así que ambos tienen acceso y tratan datos de carácter personal, de manera que el documento de seguridad tendrá que contemplar dicha circunstancia.

---

[51] Y así lo confirma la fracción X del numeral 11 de los Lineamientos, relativo al contenido del registro, que indica que constará la "indicación del nivel de seguridad aplicable: básico, medio o alto", sin que en ningún momento establezca la obligación de notificar el documento de seguridad al Instituto.

Se trata, por tanto, de una previsión a establecer y hacer cumplir en el instrumento jurídico que regule la relación que se establezca entre el responsable y el tercero que acceda a los datos personales para prestarle un servicio que implique el tratamiento de éstos.

Por lo que se refiere al responsable del tratamiento o sistema de datos personales, la Ley indica que:

> *Las medidas de seguridad que al efecto se establezcan deberán indicar el nombre y cargo del servidor público o, en su caso, la persona física o moral que intervengan en el tratamiento de datos personales con el carácter de responsable del sistema de datos personales.*

Esta previsión plantea varias cuestiones que vamos a ir desgranando para intentar aclarar su significado y alcance.

En primer lugar, entendemos que la referencia a las medidas de seguridad es al documento de seguridad, puesto que será en éste en el que se identifique al responsable del tratamiento, así como a las personas que tienen acceso a datos de carácter personales para tratarlos en el desarrollo de sus funciones.

Unido a lo anterior, la Ley busca que en todo momento esté identificado quién es el responsable del tratamiento, lo que resulta lógico.

No obstante, cuando la Ley hace referencia a la persona física que *intervenga en el tratamiento de datos personales con el carácter de responsable del sistema de datos personales, entendemos que se está haciendo referencia al que puede denominarse como "responsable interno", puesto que en todo caso responsable será un ente público conforme a la definición dada en la Ley*[52]. Este responsable interno es

---

[52] Volviendo por un momento al artículo 1, queda claro que son los entes públicos quienes poseen los datos y quedan, por tanto, sujetos al cumplimiento de los principios y obligaciones establecidas en la Ley. Asimismo, el artículo 2 define como ente público a *"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*

quien en el día a día actúa como responsable del manejo y tratamiento del Sistema de datos personales, pudiendo coincidir o no con la figura del responsable de seguridad.

Y también este párrafo del artículo hace referencia a quienes traten datos de carácter personal y al usuario. Obviamente el documento de seguridad deberá contener una referencia a aquellos tratamientos que sean llevados a cabo por terceros para prestar un servicio al responsable del tratamiento. Tal circunstancia resulta relevante, puesto que el documento de seguridad contendrá una relación de los archivos o sistemas de datos personales, señalando cuáles serán tratados por terceros para los efectos oportunos.

La organización de los archivos de manera que permita un acceso rápido a los datos personales es esencial, toda vez que facilita el ejercicio de los derechos, la adopción y aplicación de las medidas de seguridad, así como el cumplimiento de otra normativa que resulte aplicable. En este sentido, una vez más, la organización documental del archivo está relacionada con las disposiciones de la Ley de Archivos del Distrito Federal.

De esta forma, el usuario tendrá que cumplir con las medidas de seguridad que sean exigibles, de nuevo atendida la naturaleza de los datos que sean tratados y conforme a lo que se prevea en el instrumento jurídico que le vincule con el responsable del tratamiento.

En concreto, en el documento de seguridad se incluirá una referencia al acto jurídico (ya sea contrato, convenio u otro documento de naturaleza análoga) que regule la relación entre el responsable del sistema de datos personales y el usuario.

Y en dicho acto jurídico tendrá que establecerse también la obligación del usuario de adoptar y aplicar las medidas de seguridad, puesto que

---

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".

accede a los datos para tratarlos y prestar un servicio al responsable del sistema de datos personales. E incluso, avanzando más en la práctica, sería conveniente prever que el encargado del tratamiento se someterá a las auditorías que el responsable del tratamiento estime oportunas en aras de garantizar que las medidas de seguridad se cumplan.

Actualización de los datos del responsable y notificación al Instituto

El último apartado del artículo establece lo siguiente:

> *En el supuesto de actualización de estos datos, la modificación respectiva deberá notificarse al Instituto, dentro de los 30 días hábiles siguientes a la fecha en que se efectuó.*

Si bien la referencia a la "actualización de estos datos" resulta genérica, entendemos que hay que ponerla en conexión con el párrafo precedente, de manera que los datos actualizables serían, en principio, los del responsable del tratamiento, cuando se haya identificado a través de nombre y cargo del servidor público, así como los del encargado del tratamiento. Se trata, por tanto, de que el Instituto conozca en todo momento quién está tratando los datos por si tuviera que dirigirse a él.

La obligación de notificación supone que el Instituto tenga que establecer el procedimiento a tal fin, puesto que se trata, por un lado, de una modificación en el documento de seguridad y, por otro lado, de la indicación de quién actúa como responsable del tratamiento a efectos de la adopción de dichas medidas.

Por último, el plazo de treinta (30) días establecido parece suficientemente amplio, aunque, en todo caso, habría que interpretarlo en conjunción con la notificación de otras medidas de seguridad o cambios que puedan producirse en relación con el tratamiento de los datos de carácter personal en los sistemas notificados al Instituto.

Artículo 14.- El ente público responsable de la tutela y tratamiento del sistema de datos personales, adoptará las medidas de seguridad, conforme a lo siguiente:

A. Tipos de seguridad:

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;

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.

B. Niveles de seguridad:

I. **Básico.-** Se entenderá como tal, el relativo a las medidas generales de seguridad cuya aplicación es obligatoria para

todos los sistemas de datos personales. Dichas medidas corresponden a los siguientes aspectos:

a) Documento de seguridad;

b) Funciones y obligaciones del personal que intervenga en el tratamiento de los sistemas de datos personales;

c) Registro de incidencias;

d) Identificación y autentificación;

e) Control de acceso;

f) Gestión de soportes, y

g) Copias de respaldo y recuperación.

II. **Medio.-** Se refiere a la adopción de medidas de seguridad cuya aplicación corresponde a aquellos sistemas de datos relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo. Este nivel de seguridad, de manera adicional a las medidas calificadas como básicas, considera los siguientes aspectos:

a) Responsable de seguridad;

b) Auditoria;

c) Control de acceso físico; y

d) Pruebas con datos reales.

III. **Alto.-** Corresponde a las medidas de seguridad aplicables a sistemas de datos concernientes a la ideología, religión,

creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos. Los sistemas de datos a los que corresponde adoptar el nivel de seguridad alto, además de incorporar las medidas de nivel básico y medio, deberán completar las que se detallan a continuación:

a) Distribución de soportes;

b) Registro de acceso; y

c) Telecomunicaciones.

Los diferentes niveles de seguridad serán establecidos atendiendo a las características propias de la información.

Isabel Davara F. de Marcos
COMENTARIO

El artículo 14 de la Ley está dedicado a los tipos de seguridad y a los niveles de medidas de seguridad aplicables a los datos que sean tratados por los entes públicos.

Adopción de las medidas de seguridad

El artículo señala que la obligación de adoptar medidas de seguridad corresponde al ente público responsable de la tutela y tratamiento del sistema de datos personales, lo cual significa que el responsable del tratamiento tiene obligación de garantizar la integridad, confidencialidad y disponibilidad de los datos personales.

Es necesario tener en consideración que, en la práctica, la adopción de las medidas de seguridad será realizada por el responsable de seguridad como consecuencia de la delegación de funciones. Es

decir, será el responsable o responsables de seguridad, incluso con la participación del responsable del tratamiento, quien adopte e implante las medidas de seguridad.

Además del responsable del sistema de datos personales, también el encargado del tratamiento, en aquellos casos en los que intervenga en el tratamiento de los datos, tendrá que cumplir con las medidas de seguridad que sean exigibles por la Ley, puesto que accede a los datos personales para tratarlos y prestar así un servicio al responsable del tratamiento. Las medidas de seguridad son una de las cuestiones a acordar con el encargado del tratamiento, máxime cuando en la práctica puede darse el hecho de que el responsable del tratamiento ni siquiera tiene o trata los datos, dado que es el encargado quien realiza todos los tratamientos necesarios.

De cualquier modo, las medidas de seguridad serán adoptadas por el responsable y, en su caso, por el usuario. Es decir, las medidas de seguridad serán adoptadas por quien trate los datos personales, siendo siempre una obligación del responsable del tratamiento, dado que es quien decide sobre la finalidad, contenido y uso del tratamiento, con independencia de que trate los datos o haya contratado con un tercero para tal efecto.

Tipos de seguridad

La Ley distingue varios tipos de seguridad, citando expresamente los siguientes: física, lógica, de desarrollo y aplicaciones, de cifrado y de comunicaciones y redes[53].

Cabe señalar que las medidas de seguridad previstas en la Ley y sus Lineamientos[54], en la práctica, se aplicarán atendiendo a la configuración del sistema de datos personales. Esto es, habrá que

---

[53] Si bien podríamos reducir el listado a seguridad física, lógica y jurídica, puesto que desarrollo, aplicaciones, cifrado, comunicaciones y redes pueden ser consideradas como parte de la seguridad física y lógica.

[54] Los cuales serán analizados posteriormente y a ellos nos remitimos aquí.

tener en consideración cómo se organiza éste, tanto desde un punto de vista físico como lógico. Es así que un sistema de datos puede encontrarse en diferentes ubicaciones físicas, interconectadas entre sí por medios electrónicos; y aunque estuviera en un único lugar, puede estar organizado en diferentes archivos o bases de datos desde un punto de vista lógico, atendiendo, por ejemplo, a la naturaleza de los datos que sean objeto de tratamiento o a las necesidades de acceso para el tratamiento de los datos.

Niveles de seguridad

Las medidas de seguridad se clasifican en tres niveles: básico, medio y alto, según la naturaleza de la información tratada y en relación con la necesidad de garantizar su confidencialidad e integridad en los sistemas de datos personales.

Todos los archivos que contengan datos de carácter personal tienen que cumplir las medidas de seguridad calificadas de nivel básico. Los de nivel medio deben cumplir, además, las calificadas de nivel medio. Los de nivel alto tienen que cumplir, además de las dos anteriores, las calificadas de nivel alto. Los niveles, como decíamos, tienen la condición de mínimos exigibles. Así, es posible resumir los niveles de seguridad previstos en el artículo 14 de la siguiente manera:

> Nivel Básico: Todos los sistemas que contengan datos de carácter personal.
>
> Nivel Medio: Los sistemas que contengan datos relativos a:
>
> - La comisión de infracciones administrativas o penales.
> - Hacienda Pública.
> - Servicios financieros.
> - Datos patrimoniales.
> - Archivos que permitan obtener una evaluación de la personalidad del individuo.

Nivel Alto: Los sistemas que contengan datos relativos a:

- Ideología.
- Afiliación política.
- Religión.
- Creencias.
- Origen racial o étnico.
- Salud, biométricos o genéticos.
- Vida sexual.
- Recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.

Llama la atención el hecho de que la Ley haya seguido, casi literalmente, la clasificación que establecía el artículo 4 del derogado Reglamento español de medidas de seguridad[55]. El tiempo y la aplicación práctica serán determinantes para saber si el modelo seguido resulta adecuado o si hubiera sido preferible aprovechar la ocasión para desarrollar un modelo distinto basado en otros estándares internacionales, tanto desde un punto de vista jurídico como técnico. En este sentido, resulta destacable, en particular, la norma ISO 27001 sobre sistemas de gestión de la seguridad de la información.

Las medidas de seguridad son mayores según el nivel, atendiendo a la naturaleza de los datos objeto de tratamiento.

Además, como hemos dicho, son acumulables, esto es, los archivos de nivel alto tienen que cumplir todas las medidas de seguridad aplicables para los de nivel básico y medio.

---

[55] Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad, y que fue derogado por el Real Decreto 1720/2007.

Finalmente, con sólo tener un registro de un nivel superior, todo el archivo o sistema de datos queda declarado del nivel superior.

Si bien la Ley se limita a enumerar las medidas de seguridad exigibles para cada uno de los niveles, recordando su carácter acumulable, si se ponen en relación con los Lineamientos es posible resumirlas brevemente tal y como se hace a continuación.

Al intentar resumir el contenido en la práctica, es decir, las obligaciones que en cuanto a medidas de seguridad necesitan adoptarse, podemos ver que el nivel básico exigiría la creación, por el responsable del tratamiento, de un documento de seguridad que contendrá:

a) Las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido,

b) Las funciones y obligaciones del personal, a los que deberá informar y formar sobre las normas de seguridad que afecten al desarrollo de sus funciones y

c) Las consecuencias en caso de incumplimiento, así como

d) Tener una relación actualizada de usuarios (sujetos y procesos que están autorizados para acceder a datos o recursos),

e) Estableciendo procedimientos de identificación y autenticación de dicho acceso,

f) La estructura de los archivos con datos de carácter personal,

g) El procedimiento de notificación, gestión y respuesta de las incidencias, creando un registro de éstas,

h) Establecimiento de un control de acceso y

i) De un mecanismo de gestión de soportes y

j) Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

El nivel medio, por su parte, además de cumplir las mencionadas en el nivel básico, deberá incluir:

a) La identificación del responsable o responsables de seguridad,

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y

c) Las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado,

d) Un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema y

e) La verificación de que está autorizado, limitándose la posibilidad de intentar reiteradamente el acceso no autorizado, junto con otras limitaciones, en este caso de acceso físico a los locales donde se encuentren ubicados los sistemas de información, permitiéndolo solamente a aquellas personas autorizadas, y

f) Otras normas para la gestión de soportes, o procedimientos de recuperación de datos y

g) Pruebas con datos reales que no estarán permitidas salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

Además, hay que destacar que tendrán que someterse a una auditoría interna o externa que verifique el cumplimiento de la normativa y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años[56].

---

[56] El numeral 16.II.b) de los Lineamientos indica que: *"Las medidas de seguridad implementadas para la protección de los sistemas de datos personales se someterán a una auditoría interna o externa, mediante la que se verifique el cumplimiento de la Ley, de los presentes Lineamientos y demás procedimientos vigentes en materia de seguridad de datos, al menos, cada dos años."*

El nivel alto, finalmente, además de cumplir las de nivel medio, que a su vez implican las de nivel básico, tendrá que cumplir otras medidas complementarias relativas a:

a) La distribución de soportes,

b) El registro de accesos,

c) Las copias de respaldo y recuperación y,

d) En caso de que se realice transmisión de datos a través de redes de telecomunicaciones, se exige el cifrado de éstos[57].

Aplicación de los niveles de seguridad

El último párrafo del artículo establece cómo se aplican los diferentes niveles de seguridad, repitiendo en cierta medida lo ya indicado por el artículo 13, en cuanto a que las medidas de seguridad se adoptarán atendiendo al menor o mayor grado de protección que ameriten los datos personales.

Es así que los niveles de seguridad se aplican atendiendo a la naturaleza de los datos personales o, tal y como literalmente indica el artículo 14, *"atendiendo a las características propias de la información."*

[57] Esta medida, en concreto, resulta especialmente llamativa por la dificultad de su implementación en la práctica. Además, debe entenderse que ésta es sólo exigible cuando se haga uso de servicios de comunicaciones electrónicas disponibles para el público, de manera que si los datos viajan a través de una red privada, no se requerirá su cifrado ya que se entiende que no quedan expuestos a terceros que pudieran interceptar dicha comunicación.

Artículo 15.- Las medidas de seguridad a las que se refiere el artículo anterior constituyen mínimos exigibles, por lo que el ente público adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales. Por la naturaleza de la información, las medidas de seguridad que se adopten serán consideradas confidenciales y únicamente se comunicará al Instituto, para su registro, el nivel de seguridad aplicable.

Isabel Davara F. de Marcos

COMENTARIO

Mínimos exigibles

La Ley insiste nuevamente en el carácter de mínimos exigibles de las medidas de seguridad aquí previstas.

Así, tal y como indica el artículo, las medidas de seguridad indicadas en la Ley *"constituyen mínimos exigibles"*.

Dicho de otra manera, la adopción de las medidas de seguridad previstas en la Ley no supone que se cumpla con la seguridad de la información, puesto que quien trate los datos personales, ya sea el ente público como responsable del sistema de datos personales o, en su caso, un usuario, tiene que adoptar las medidas de seguridad necesarias para garantizar la confidencialidad e integridad de la información. En consecuencia, los "mínimos exigibles" a los que se refiere la Ley constituyen el nivel de seguridad que tienen que cumplir todos los entes públicos, de manera que ya se está garantizando la seguridad de los datos personales. Sin embargo, atendida la naturaleza de los datos personales y otros factores relativos a su tratamiento, estos mínimos pueden requerir ser complementados en aras de garantizar de manera efectiva los datos personales.

Por tanto, con la adopción de medidas de seguridad únicamente se cumple con la obligación prevista en la Ley, pero sigue siendo necesario que se adopten aquellas que eviten la alteración, pérdida o acceso no autorizado a los datos de carácter personal.

De nuevo, las medidas de seguridad serán adoptadas atendiendo a la naturaleza de los datos que sean objeto de tratamiento, lo que determinará el nivel de medidas de seguridad aplicable. Y, como decimos, aun así habría que atender a la necesidad de adoptar otras medidas adicionales en aras de garantizar la seguridad de los datos. Incluso estas medidas pueden ser exigibles en virtud de otra normativa que resulte aplicable, ya que las medidas de seguridad aquí previstas se refieren únicamente a la seguridad de los datos, puesto que el legislador se ha centrado en los sistemas de datos personales.

En este sentido, recordemos que las medidas de seguridad previstas en la Ley no son las únicas a cumplir. La LPDPDF no particulariza los casos de las medidas de seguridad de acuerdo con los sistemas tutelados, y concede a los entes la atribución de establecer las medidas que resulten necesarias para otorgar mayor seguridad en casos especiales. No hay que dejar de lado que los entes públicos están obligados a establecer las medidas necesarias para proteger los datos que están bajo su tutela.

El responsable y, en su caso, el usuario, tendrán que adoptar aquellas medidas que sean exigibles por la normativa aplicable y que permitan garantizar la seguridad de los datos. Tales medidas pueden ser aplicables a los datos, como información que es, a las personas que tratan los datos, a los sistemas de datos personales o a las aplicaciones que se utilizan en el tratamiento de datos.

Por ejemplo, podría tenerse en consideración la serie ISO/IEC 27000[58] que establece una gama de normas de gestión de la seguridad de la información, o también la norma ISO/IEC 17799:2005 sobre seguridad tecnológica y técnicas de seguridad. Resulta obvio que el objeto de estas normas de seguridad es más amplio que los datos de carácter personal, ya que se refieren, en general, a la información que es objeto de tratamiento en un sistema de información, entre

[58] ISO *(International Organization for Standards)* es la organización internacional de estandarización y, entre otros estándares, ha desarrollado varias normas que son aplicables en materia de seguridad de la información y de los sistemas de información.

la que pueden encontrarse los datos de carácter personal como un activo de la entidad. En cualquier caso, las normas ISO constituyen herramientas muy importantes para regular y garantizar las medidas de seguridad, pero no constituyen medidas en sí mismas.

Debemos reafirmar que la Ley deja abiertas todas las posibilidades, siempre y cuando se cumpla con los mínimos establecidos en ella, al mismo tiempo que se cumple con la obligación de adoptar medidas de seguridad.

Es decir, la Ley es aplicable a una amplia variedad de sistemas de información en los que se tratan datos de carácter personal, que puede ir desde una escuela pública hasta un hospital público. Por tanto, quien trate datos de carácter personal, ya sea como responsable o como usuario, tendrá que adecuar las medidas de seguridad al tratamiento que lleve a cabo.

Medidas adicionales

A continuación, la Ley indica que *"el ente público adoptará las medidas adicionales que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales"*.

Puesto que el objetivo último de las medidas de seguridad es evitar cualquier pérdida, alteración o acceso no autorizado a los datos, resulta claro que el ente público o quien trate los datos personales por cuenta de éste, tiene la obligación de adoptar las medidas de seguridad necesarias.

A este respecto, es importante recordar, una vez más y aunque sea casi de manera insistente, que las medidas de seguridad previstas en la Ley, y que posteriormente se desarrollan en los Lineamientos, son los mínimos exigibles, si bien será cada ente público quien tendrá que adaptarlas al tratamiento que lleva a cabo, atendiendo en particular a la necesidad de garantizar la seguridad de los datos.

Es decir, así establecidas, las medidas de seguridad son aplicables a cualquier ente público, lo que implica en la práctica que las mismas previsiones pudieran aplicarse a cualquier sistema de datos personales con independencia de quién sea el ente público que trate los datos o cómo sea el sistema de información o se hayan estructurado los sistemas de datos personales.

Resulta obvio que, si bien la finalidad de las medidas de seguridad es la misma en todos los casos, esto es, la seguridad de los datos, no ocurre lo mismo atendiendo a los tratamientos y la naturaleza de los datos en uno y otro caso.

Por lo tanto, el responsable de adoptar las medidas de seguridad, es decir, el responsable del sistema de datos o el usuario que acceda a los datos para prestarle un servicio, tiene que atender a todos los aspectos de dicho tratamiento con la finalidad de garantizar la seguridad de los datos y, de esta manera, proteger al interesado cuyos datos son objeto de tratamiento.

Es necesario tener claro que la Ley atribuye al responsable el compromiso de su cumplimiento, lo cual significa que el responsable del tratamiento responderá, en cualquier caso, del tratamiento de los datos y del cumplimiento de las obligaciones establecidas en la Ley, con independencia de que internamente pueda exigir la responsabilidad correspondiente a quien incumplió con la obligación de que se trate.

Tal y como prevé la Ley, será el responsable del tratamiento quien en última instancia adopte las decisiones oportunas sobre las medidas de seguridad a establecer, cumpliendo siempre con las previstas en la Ley y en los Lineamientos. Dicho de otra manera, con la adopción de estas medidas de seguridad se cumple sólo con una obligación, siendo necesario adoptar las medidas que garanticen efectivamente la seguridad de los datos de carácter personal que son objeto de tratamiento.

¿Qué medidas de seguridad adicionales adoptar y cómo aplicarlas?

A la vista del mandato establecido en la Ley de adoptar medidas adicionales, cabe preguntarse cuáles serán esas medidas.

Al respecto, la propia Ley indica que quien trate los datos adoptará las medidas *"que estime necesarias para brindar mayores garantías en la protección y resguardo de los sistemas de datos personales"*.

Como ya dijimos, dichas medidas de seguridad pueden venir exigidas por otras normas que resulten aplicables al desarrollo de las funciones del ente público[59].

---

[59] Por ejemplo, si se presta atención a la Ley de Archivos del Distrito Federal, publicada en la Gaceta Oficial del Distrito Federal de 8 de octubre de 2008, los entes públicos tienen que adoptar, entre otras, ciertas medidas relativas a la seguridad de los archivos, pudiendo señalarse aquí las siguientes referencias expresas:

Artículo 20. *Serán funciones de la Unidad Coordinadora de Archivos, las siguientes:*

[…]

VIII. Coadyuvar con la instancia responsable de la función dentro del ente público, en la elaboración de un programa de necesidades para la normalización de los recursos materiales que se destinen a los archivos, propiciando la incorporación de mobiliario, equipo técnico, de conservación y seguridad, e instalaciones apropiadas para los archivos, de conformidad con las funciones y servicios que éstos brindan;

Artículo 37. *Los entes públicos, en el marco de su Sistema Institucional de Archivos establecerán las medidas para la administración, uso, control y conservación de los documentos de archivo electrónicos, garantizando los aspectos siguientes:*

[…]

III. Incorporar medidas, normas y especificaciones técnicas nacionales e internacionales, para asegurar la autenticidad, seguridad, integridad y disponibilidad de los documentos de archivo electrónicos y su control archivístico;

Artículo 54. *Para el desempeño de sus funciones, los entes públicos deberán, dentro de lo posible, adecuar las instalaciones de archivo a las recomendaciones de la Asociación Latinoamericana de Archivos para la edificación o adaptación de espacios y mobiliario de archivo.*

Para el resguardo de archivos, los entes públicos deberán contar con:

[…]

Además de lo anterior, es posible también considerar que las medidas de seguridad se aplicarán conforme al principio de proporcionalidad. Es decir, no resulta lógico exigir ni tampoco aplicar medidas de seguridad que resulten desproporcionadas por razones tecnológicas y, por tanto, de coste económico. En consecuencia, las medidas de seguridad adicionales tendentes a garantizar la seguridad de los datos se aplicarán conforme al principio de proporcionalidad, lo que a su vez conlleva atender al principio de neutralidad tecnológica, tan utilizado en las normas de "Nuevas" Tecnologías.

En cualquier caso, el cumplimiento de las medidas de seguridad vendrá dado, en la práctica, por el tratamiento al que se aplican. Esto es, habrá medidas de seguridad que se aplicarán a un tratamiento automatizado y otras a un tratamiento no automatizado de los datos, de manera que la proporcionalidad tiene que ser considerada en todos los contextos posibles y no solamente reducida al ámbito tecnológico. En este sentido, puede haber otras normas que resulten aplicables y que contengan medidas de seguridad a aplicar a ubicaciones o soportes que puedan contener datos personales, tal y como ocurre en el caso de la Ley de Archivos del Distrito Federal, que en sus artículos 20, 37 y 54 contiene disposiciones relativas a las medidas de seguridad aplicables para garantizar los inmuebles y espacios destinados al depósito de documentos, el soporte en que se encuentra la información.

III. Las medidas preventivas y de seguridad que garanticen la protección de los depósitos documentales, tales como:

a. Detectores de humo.

b. Extintores de fuego de gas inocuo;

c. Materiales de archivo retardantes;

d. Salas de desinfección;
e. Salas de desinsectación;
f. Vigilancia; y
g. Plan de emergencia.

En definitiva, partiendo de las medidas de seguridad establecidas en la Ley y en sus Lineamientos, quien trate datos de carácter personal adoptará, en concreto, aquellas medidas que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, teniendo en cuenta, entre otros, los siguientes aspectos:

1. La naturaleza de los datos que sean objeto de tratamiento, lo que determinará, en primer lugar, la aplicación de uno u otro nivel de seguridad y, posteriormente, la necesidad de adoptar medidas adicionales;

2. Otras normas que resulten aplicables al responsable del tratamiento en virtud del desarrollo de sus funciones;

3. El estado de la tecnología, puesto que la seguridad de los datos está unida a la propia evolución de la tecnología e incluso al coste económico que supone su cumplimiento.

4. Los riesgos a que se encuentren sometidos los datos, siendo la finalidad última la ya indicada a efectos de evitar la alteración, pérdida, tratamiento o acceso no autorizado a los datos que se tratan en los sistemas.

Comunicación de las medidas de seguridad al Instituto

Si bien el artículo 13 de la Ley, relativo también a las medidas de seguridad, establece, como ya vimos, que éstas *"deberán constar por escrito y ser comunicadas al Instituto para su registro"*, el artículo 15 viene a aclarar que lo que se comunicará al Instituto es *"el nivel de seguridad aplicable"*[60]. Es decir, el registro del sistema de datos de

[60] Que tal y como ya habíamos señalado al comentar el artículo 13, es lo que indican los Lineamientos al referirse al registro de los sistemas de datos personales ante el Instituto.

carácter personal incluirá el nivel de medidas de seguridad aplicable. Y dicho nivel de medidas de seguridad podrá ser básico, medio o alto conforme a lo dispuesto en el artículo 14 de la Ley.

Tal comunicación seguiría la práctica de otros países, al igual que ocurre por ejemplo en España. Es decir, el órgano de control tendrá conocimiento, vía inscripción del sistema de datos de carácter personal, del nivel de medidas de seguridad aplicable. Sin embargo, cuestión distinta son las medidas de seguridad que se apliquen en la práctica, que quedarán detalladas en el documento de seguridad al que el órgano de control, el Instituto en este caso, podrá acceder en los supuestos previstos en la Ley para vigilar el cumplimiento de ésta.

El documento de seguridad, por tanto, tendrá que estar actualizado en todo momento conforme a los cambios que se produzcan en el sistema de datos personales, lo que incluye tanto el tratamiento de datos personales como las personas que actúan como usuarios del tratamiento.

Por otro lado, como ya dijimos, reiteramos que tanto el responsable como el encargado del tratamiento tienen obligación de adoptar las medidas de seguridad mediante el documento de seguridad.

El Instituto, como órgano al que la Ley encomienda vigilar su cumplimiento, puede solicitar el documento de seguridad o revisar las medidas de seguridad adoptadas por el ente público en los casos previstos en la Ley, que en particular serán aquellos en los que proceda a realizar una visita de inspección.

En definitiva, comunicar al Instituto el nivel de medidas de seguridad que se aplica al sistema de datos personales es lógico puesto que será el que se indique, en su caso, en la publicación del contenido del registro. De esta manera, los interesados podrían ser informados también del nivel de medidas de seguridad aplicable al sistema de datos de carácter personal de que se trate.

Confidencialidad de las medidas de seguridad

La confidencialidad de las medidas de seguridad es parte de la seguridad en sí. Dicha confidencialidad supone que las medidas de seguridad únicamente puedan ser conocidas por quien tiene que cumplirlas, ya que de otra manera se pondría en riesgo la seguridad de los datos.

En la práctica, esto implica que el documento de seguridad sólo deba ser conocido por quien tiene que cumplir con él. Es decir, las medidas de seguridad serán conocidas por los usuarios que tienen que cumplir con ellas, sin que en modo alguno un usuario pueda tener acceso a medidas de seguridad que no tiene que cumplir. Por ejemplo, un usuario que trate datos de carácter personal a los que les sean aplicables medidas de seguridad de nivel básico, tendrá conocimiento únicamente del documento de seguridad aplicable para ese nivel de medidas de seguridad o a la parte correspondiente del documento de seguridad en caso de que éste contuviera varios niveles.

Lo contrario supondría dar acceso a una persona no autorizada a medidas de seguridad que por disposición de la Ley son confidenciales.

Así, el documento de seguridad, o la parte que corresponda, estará disponible únicamente para los usuarios autorizados. Además, una de las medidas de seguridad aplicables a éstos, con la finalidad de garantizar la seguridad de la información, es mantener dichas medidas confidencialmente, lo que viene a sumarse a la obligación de secrecía respecto al tratamiento de datos de carácter personal. Se trata, por tanto, de evitar que una persona no autorizada pueda tener acceso a los datos de carácter personal, garantizando así su seguridad. Al respecto, el documento de seguridad incluirá, al menos, los niveles de seguridad de quienes tendrán acceso a dichas medidas.

Obviamente, la confidencialidad no aplica respecto al Instituto, ya que como órgano de control puede exigir el documento de seguridad en caso de que realice una visita de inspección y la comprobación de que las medidas de seguridad se cumplen en la práctica.

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 previsto 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.

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

El ente público no podrá difundir o ceder los datos personales contenidos en los sistemas de datos desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso por escrito o por un medio de autenticación similar, de las personas a que haga referencia la información. Al efecto, la oficina de información pública contará con los formatos necesarios para recabar dicho consentimiento.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente, respondiendo solidariamente por la inobservancia de las mismas.

Isabel Davara F. de Marcos

COMENTARIO

El Capítulo IV de la Ley está dedicado al desarrollo de los principios de la protección de datos aplicados al tratamiento de datos personales. El artículo 16, primero de este capítulo, se refiere al consentimiento para el tratamiento de los datos.

El eje central de las normativas en protección de datos es el principio del consentimiento, por el que el titular de los datos es el único que tiene derecho a decidir quién, cómo, cuándo y para qué se tratan sus datos, derivado claramente del derecho a la autodeterminación informativa, antes comentado.

Es cierto que hay quienes defienden que el principio fundamental es el de calidad de los datos, argumentando que no tiene ninguna excepción, que siempre debe cumplirse, mientras que el de consentimiento, si bien también esencial en su opinión, sí cuenta con estas excepciones.

En nuestra opinión, lo anterior implica mezclar conceptos. El principio del consentimiento no es una cualidad o adjetivo del tratamiento, sino su eje.

La protección de datos gira en torno al individuo, a la persona, que es a quien se protege, no a los datos, ni al tratamiento de éstos con una finalidad determinada. Es evidente que el objeto de protección de la normativa son los datos sometidos a tratamiento, pero siempre son unos datos unidos a una persona física, en ningún caso disociados de ésta.

Si bien es absolutamente imprescindible definir la finalidad del tratamiento, en tanto sólo se pueden tratar datos con una finalidad explícita, legítima y determinada, lo que de verdad es irrenunciable es la característica subjetiva del derecho que va indisolublemente unido a la persona, cuyo consentimiento, aunque prescindible en algunos casos en pos del equilibrio de derechos fundamentales e intereses en conflicto, constituye la manifestación más relevante de dicha subjetividad.

El consentimiento para la recogida y la cesión de datos

En concreto, este artículo trata el principio del consentimiento tanto en la fase de recogida de los datos como en la fase posterior de transmisión de los datos.

En nuestra opinión el legislador del Distrito Federal acierta en la previsión del consentimiento, puesto que el principio del consentimiento, si bien modulado, debe existir desde el origen.

Decimos modulado de dos maneras: de un lado, porque puede darse en muchas ocasiones de manera tácita, y, de otro, porque pueden darse muchas excepciones.

De no preverse el régimen del consentimiento desde el origen, utilizando, como decíamos, en muchas ocasiones el tácito o

acudiendo a excepciones tasadas, podríamos incurrir en la ilicitud del tratamiento en origen, es decir, que estuviera viciado y contaminara el resto de su vida posterior.

No obstante, es justo decir que esta regulación la encontramos a nivel federal.

El lineamiento 6º en materia de protección de datos personales, bajo el epígrafe de "Licitud", dice que *"la posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios previstos en dichas disposiciones"*.

En nuestra opinión, aunque en el lineamiento 6º se establece la licitud del tratamiento al reiterar que sólo será posible aquél que esté dentro de las atribuciones legales o reglamentarias de la dependencia, debería especificar que no es necesario dicho consentimiento, esto es, que se excepciona. Es decir, que el lineamiento referido debe ser visto como un ejemplo de que lo previsto en la Ley de Protección de Datos Personales para el Distrito Federal es lo correcto, prever el consentimiento desde el origen para el tratamiento lícito de los datos personales.

Es más, al establecer que el tratamiento sólo podrá hacerse dentro de dichas atribuciones, en realidad está supliendo, incluso de una manera muy magistral, la posible ilicitud *ab initio* de dicho tratamiento.

Es decir, los Lineamientos, en este punto, parecen estar diseñados por alguien que ha tenido muy claro dicha deficiencia y la ha salvado con una excepción general al consentimiento, la atribución legal o reglamentaria, pero esto, en nuestro parecer, no tendría por qué haber impedido una referencia más general al consentimiento.

Excepciones al consentimiento

Las excepciones al consentimiento resultan obvias puesto que el tratamiento de datos no puede depender única y exclusivamente de la voluntad del interesado.

Es decir, puede haber situaciones en las que el tratamiento de datos es necesario sin necesidad de consentimiento del interesado. En cualquier caso, dichas situaciones tendrán que estar previstas en una norma con rango legal, tal y como hace la LPDPDF con la finalidad de preservar el derecho a la protección de datos de los titulares.

En concreto, las excepciones a la norma general relativa a la necesidad del consentimiento son las 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 previsto 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.

En relación con las excepciones previstas en la Ley, cabe señalar lo siguiente:

- Se trata de una enumeración amplia de supuestos en los que el consentimiento del interesado queda excepcionado.
- Las excepciones se refieren a cualquier fase del tratamiento, ya que por ejemplo los apartados V y VI se refieren a la transmisión o cesión de datos.
- Entre las excepciones se incluyen algunas que no se refieren al tratamiento de datos personales por entes públicos. Así, por ejemplo, el inciso III se refiere *"a las partes de un convenio de una relación de negocios"* en el que cabe pensar más en el ámbito privado que en el público.

Forma del consentimiento

Por otro lado, la forma del consentimiento, si bien da lugar a una gran seguridad jurídica, puede obstaculizar de manera importante el tratamiento.

Con carácter general cabe distinguir entre consentimiento tácito, expreso y expreso por escrito[61].

---

[61] De las características que conforman el consentimiento se dice que debe ser: libre (que haya sido obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por las leyes, es decir, que no esté viciado.); específico (debe ser "referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento"); informado (el titular conoce con anterioridad al tratamiento de sus datos "la existencia del mismo y las finalidades para las que el mismo se produce"); e inequívoco (no se puede deducir el consentimiento de los meros actos realizados por el afectado – el llamado *consentimiento presunto*-, sino que es preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento). Vid. siguiendo a Castán Tobeñas, Alonso Martínez, C,. "Protección de Datos de Carácter Personal. El consentimiento en entidades financieras", Madrid: Ed. ASNEF, 2002, páginas 56-69.

En cualquiera de los casos señalados, la cuestión se centra en la prueba de la obtención del consentimiento, que recae en quien dice tenerlo.

Es decir, tanto en el consentimiento tácito, principalmente, como en el expreso que no sea escrito, parece que hay que implementar procedimientos estandarizados de obtención de dicho consentimiento a efectos de prueba posterior.

El cesionario

Resultando claro que el cesionario es quien recibe la cesión de los datos, la Ley indica que éste *"quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente"* y a continuación añade que en caso de incumplimiento responderá *"solidariamente por la inobservancia de las mismas"*.

Si bien cedente y cesionario quedan vinculados en virtud de la cesión de datos, puesto que el cedente tendrá que comunicar la rectificación o cancelación de los datos para que el cesionario proceda en el mismo sentido, la referencia a la responsabilidad solidaria no puede entenderse en sentido amplio, sino que tendría que limitarse a aquellos supuestos en los que una determinada obligación tenga que ser cumplida por el cedente y el cesionario conjuntamente. De otra manera, una responsabilidad solidaria supondría hacer que cedente y cesionario tengan que responder por los incumplimientos de uno de ellos aunque la otra parte haya cumplido con sus obligaciones.

En cualquier caso, tal y como prevé la Ley, la cesión de datos por un ente público requiere que éste lo haga con el consentimiento expreso por escrito del interesado. Y a estos efectos añade que serviría un "medio de autenticación similar" de manera que en el entorno electrónico cabe entender que, por ejemplo, marcar una casilla servirá para obtener dicho consentimiento. En este sentido, la Ley prevé que la oficina de información pública "contará con los formatos necesarios para recabar dicho consentimiento" entendiendo que éstos podrán ser tanto en papel como electrónicos.

Artículo 17.- 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.

Issa Luna Pla

COMENTARIO

El artículo 17 de la Ley de Protección de Datos Personales para el Distrito Federal está inscrito dentro del Capítulo IV del Tratamiento de los Datos Personales; con ello el legislador previó tanto la voluntad del titular de los datos como la responsabilidad de quien los detenta. Este precepto se funda en el reconocimiento de la voluntad del sujeto de la información como elemento sustancial para el tratamiento de los sistemas de datos, reflejado igualmente en el "consentimiento" como mecanismo y recurso clave para el ejercicio del derecho de protección de los datos personales.

En los sistemas jurídicos comparados que rigen la protección de los datos personales en posesión de las entidades de gobierno, dotar al sujeto de la información del poder del consentimiento sobre el uso y utilización de sus datos personales implica, a su vez, reconocerle al individuo un derecho de autodeterminación sobre la información referente a su vida privada. Así, en España, Suecia, Reino Unido, Francia, entre otros países, las leyes de protección de los datos personales fundan dicha protección en la voluntad del individuo y el ejercicio libre de sus derechos personales; y en correspondencia con dicha libertad, se crea una obligación y responsabilidad en el tratamiento de los datos personales del lado del detentador de los

sistemas de datos, en este caso, las entidades públicas y organismos del Estado del Distrito Federal.

De esta manera, la tutela que el artículo 17 en comento prevé, se conforma de diversos elementos que, por un lado, se refieren al acto violatorio de uso de los sistemas de datos personales por parte del ente público y cesionario y, por otro lado, determinan la consecuencia jurídica a la conducta contraria a la protección del derecho a los datos personales y a la vida privada de las personas. Veamos cada uno de estos puntos a continuación, en concordancia con la Ley en comento y los Lineamientos para la Protección de Datos Personales en el Distrito Federal publicados en la Gaceta Oficial del Distrito Federal del día 26 de octubre de 2009.

En términos del artículo 17 de la Ley, el impedimento o atentado contra el ejercicio del derecho de las personas tiene un adjetivo condicional que es el de "gravedad", término jurídico indeterminado que cabe analizar. Tanto en la Ley como en sus Lineamientos, no queda definido a detalle a qué se refiere el legislador con que el impedimento o atentado sea *grave*, pues éste calificativo implica que el procedimiento jurídico precautorio y sancionador podrá aplicarse cuando cierto grado de impedimento o atentado suceda. Sin embargo, la Ley y sus Lineamientos, cuando se refieren a la interpretación del artículo 17 de la Ley, aluden indistintamente a que el "tratamiento ilícito" amerita la suspensión o cesión de los sistemas de datos a efectos del acto resolutivo del Instituto facultado.

Es así que para identificar el "tratamiento ilícito", que tampoco se define expresamente en la Ley o sus Lineamientos, debe ser inferido a partir de las obligaciones y responsabilidades del ente público o cesionario previstos en el Capítulo IV del Tratamiento de los Datos Personales de la Ley en comento. Dicho apartado inicia con el artículo 16 que establece que todo tratamiento de los datos personales "requerirá el consentimiento inequívoco, expreso y por escrito del interesado". De

esta forma, un tratamiento ilícito se refiere a aquel manejo de los datos personales carente del consentimiento del sujeto de la información o a espaldas de éste. Pero el tratamiento ilícito también debe determinarse por la no aplicación de los principios sobre el tratamiento de los datos, que a saber son: licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad, que son aludidos en el numeral 18 de los Lineamientos y en el artículo 5 de la Ley de Protección de Datos Personales para el Distrito Federal.

Ahora bien, los Lineamientos desarrollan por su cuenta el procedimiento para la suspensión o cesión de los sistemas de datos personales ante cualquier supuesto de tratamiento ilícito, impedimento o atentado contra el ejercicio del derecho de las personas. El numeral 29 de los Lineamientos versa sobre la materia del tratamiento ilícito de los datos personales y establece el tiempo y la forma en que el Instituto de Acceso a la Información Pública del Distrito Federal, autoridad facultada para los efectos de la suspensión o cesión de los sistemas, emitirá resolución fundada y motivada para los efectos del tratamiento ilícito.

Para el ejercicio de sus facultades de suspensión o cesión de los sistemas, el legislador dotó de diversos instrumentos al Instituto para hacer valer la norma a través de su autoridad. Cabe resaltar que el Instituto está facultado por la Ley y sus Lineamientos para realizar visitas de inspección para evaluar el tratamiento lícito de los sistemas de datos personales.

El primer instrumento trata de emitir un requerimiento de suspensión fundado y motivado en derecho donde el Instituto prevea la terminación del uso o cesión de los datos personales. Esta resolución debe ser cumplida por el ente público, organismo o cesionario en un plazo no mayor a los cinco días hábiles improrrogables y, como parte del cumplimiento de la resolución, el ente rendirá informe al Instituto sobre las medidas que se tomaron para terminar con el uso o cesión de los datos personales.

Al término de este plazo, el Instituto determinará en un nuevo término de 15 días hábiles, de entre los siguientes supuestos mediante resolución de acuerdo con el numeral 29 de los Lineamientos:

I. Emitir recomendaciones en las que requiera al ente público se subsanen 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.

Aún así, el Instituto podrá ordenar el levantamiento de la suspensión solamente en los casos donde su resolución recaiga sobre la hipótesis cualquiera de las fracciones arriba enumeradas. Sin embargo, cuando un requerimiento de suspensión girado por el Instituto a un ente público, ante la detección de un tratamiento ilícito, sea desatendido, la Ley y sus Lineamientos otorgan mayor rigor al órgano garante de la protección de datos personales.

El siguiente instrumento de coercibilidad es la inmovilización de los sistemas de datos personales. En términos de los Lineamientos, en su numeral 3, fracción XII, la inmovilización de los sistemas es una "medida cautelar que consiste en la interrupción temporal en el uso de un sistema de datos personales ordenada por el Instituto en los supuestos de tratamiento ilícito de datos de carácter personal".

Correspondería al mismo Instituto dictar los criterios de tratamiento y administración de dichos datos durante el periodo de inmovilización, en concordancia con los principios jurídicos rectores de la protección de los datos personales fundados en la Ley.

La medida cautelar tiene por objeto proteger un bien jurídico supremo al tratamiento de los datos personales en posesión de los entes públicos o cesionarios, y este bien son los derechos de las personas afectadas, como lo afirma el numeral 30 de los Lineamientos.

Ahora bien, si dicha medida cautelar fuese desatendida por el ente público, el Instituto tiene la facultad de dar vista a la autoridad competente para que deslinde responsabilidades. Puesto que la Ley y los Lineamientos refieren las responsabilidades administrativas de los entes públicos a la Ley Federal de Responsabilidades de los Servidores Públicos; se entiende, por lo tanto, que la autoridad competente a la cual el Instituto de Acceso a la Información Pública del Distrito Federal dará vista del incumplimiento de la inmovilización de sistemas de datos, para los casos del Ejecutivo, es el órgano interno de control, siendo para los efectos del Distrito Federal la Contraloría General del Distrito Federal. Para los casos del Legislativo, el Judicial y los órganos autónomos serán los propios órganos internos los que lleven a cabo dicho procedimiento; y para los partidos políticos corresponde al Instituto Electoral del Distrito Federal determinar la responsabilidad.

Así las cosas, el artículo 17 de la Ley en comento prevé las consecuencias jurídicas de aquellas acciones contrarias a los principios del tratamiento de los datos personales y a aquellas constituidas como tratamiento ilícito, que el Instituto se encuentra facultado para verificar, prevenir y, en su caso, corregir en aras de la protección de los datos personales y los derechos ARCO de las personas.

Artículo 18.- 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 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. El acceso a los datos y documentos relacionados con la salud de las personales queda limitado estrictamente a los fines específicos de cada caso.

Issa Luna Pla

COMENTARIO

Existen valores e intereses públicos o privados que pueden contraponerse al deseo de la persona de mantener sus datos relativos a su estado de salud o genéticos o biométricos en un plano de reserva, por ejemplo. Ante la presencia de un interés público se justificaría la injerencia del Estado, pero tampoco debe admitirse que sea éste el que de manera absoluta determine los ámbitos de la vida íntima que deben quedar resguardados o los que puedan ser invadidos[62].

Se debe distinguir entre pacientes y usuarios de los servicios sanitarios. Así, se entiende por el primero, la persona que requiere asistencia sanitaria y está sometida a cuidados profesionales para el mantenimiento o recuperación de su salud. Mientras que el usuario es simplemente la persona que, sin estar en tratamiento, utiliza los servicios sanitarios de educación y promoción de la salud, de prevención de enfermedades y de información sanitaria.

Se prohíbe que la información introducida en una base de datos sea relacionada con la información de otras instituciones. Debe evitarse el acceso indiscriminado a la base y a la información de datos clínicos,

---

[62] Brena Sesma, Ingrid, *El derecho y la salud. Temas a reflexionar*, México, UNAM, 2004, p. 38.

ya que ésta sólo pueden ser utilizada para asuntos científicos, siempre y cuando no sea posible identificar al enfermo. Si el secreto tuviere riesgo, se requerirá del consentimiento informado del enfermo.[63]

En México, el artículo 9 del Reglamento de la Ley General de Salud señala que la atención médica debe llevarse a efecto de conformidad con los principios científicos y éticos que orientarán la práctica médica. No obstante, hoy en día esos principios no se han establecido. Por otro lado, con la instalación de la Comisión Nacional de Bioética del Consejo de Salubridad —en 1992— se cuenta ahora con una institución cuyo objetivo es estudiar e investigar la temática de los aspectos relativos a la vida, salud, el bienestar y seguridad social. Esta Comisión elaboró un Código Nacional de Bioética. La Comisión Nacional de Derechos Humanos elaboró un Código Ético para el Personal Médico y Hospitalario. La Ley General de Salud, en el artículo 98, señala la obligación de establecer comisiones de ética:

> En las instituciones de salud, bajo la responsabilidad de los directores o titulares respectivos y de conformidad con las disposiciones aplicables, se constituirán: una comisión de investigación; una comisión de ética, en el caso de que se realicen investigaciones en seres humanos, y una comisión de bioseguridad, encargada de regular el uso de radiaciones ionizantes o de técnicas de ingeniería genética. El Consejo de Salubridad General emitirá las disposiciones complementarias sobre áreas o modalidades de la investigación en las que considere que es necesario.

La confidencialidad únicamente se refiere al uso y revelación de los datos una vez recogidos, mientras que la protección de datos o de informaciones comprende el acceso, uso y revelación de éstos[64]. La tutela de los datos o informaciones relativas a la salud individual es, por tanto, más amplia que la confidencialidad, pues no se encuentra

---

[63] Ibidem, p. 57.

[64] Acuña Llamas, Francisco J., "Datos personales sensibles", en Villanueva, Ernesto, *Diccionario de Derecho de la Información,* México, Porrúa-UNAM, 2006, p. 125.

limitada únicamente al uso y revelación de los datos una vez que se han recogido; sino que también comprende la protección jurídica de los que la doctrina denomina información confidencial, en otras palabras, la protección de la cautela para no descubrir ciertos datos o elementos de la esfera íntima que el sujeto no desea compartir.

Los datos o informaciones relativas a la salud son datos de carácter personal que pertenecen a la esfera más íntima del sujeto, su conocimiento nos revela rasgos de la personalidad de éste —algunos doctrinarios los suelen llamar datos personales sensibles—[65]. Por tanto, nos encontramos ante una clase de datos a los que el ordenamiento jurídico debe conceder una especial protección, que viene a reforzar el régimen común de protección que reciben los datos de carácter personal.

Cabe señalar que la relación entre el paciente y/o usuario de los servicios sanitarios y el profesional de la sanidad no se limita al intercambio de datos o informaciones relativos a la salud. La especial relación de confianza entre éstos hace que el usuario o paciente revele informaciones o datos que forman parte de sus convicciones más profundas y que el facultativo conoce en el ejercicio de su profesión. Los propios datos relativos a la salud dejan entrever informaciones que van más allá del mero dato clínico y que revelan informaciones sobre las convicciones del usuario y/o paciente.[66]

En este mismo sentido, los datos que se refieren a la salud individual ordinariamente no revelan por sí mismos informaciones relativas a la ideología, religión o creencias, pero en algunos casos pueden hacerlo, poniendo al descubierto las convicciones del sujeto, y convirtiéndose, de esta forma, en informaciones merecedoras de la protección jurídica más alta. Habría, por lo tanto, que revisar las normas de creación de expedientes clínicos y considerar si dichos datos quedan o no inscritos dentro del expediente y, en consecuencia, determinar su nivel de protección en la misma norma.

---

[65] Tarodo Soria, Salvador, *Libertad de conciencia y derechos del usuario de los servicios sanitarios,* España, Universidad del País Vasco, 2005,, p. 251.

[66] S.T.C. 202/1999, F.J. 2º.

Cabe señalar que los Lineamientos para la Protección de Datos Personales en el Distrito Federal establecen las categorías de datos personales, de las cuales, para efectos del artículo 18 de la Ley de Protección de Datos Personales para el Distrito Federal, nos interesan dos:[67]

> Datos sobre la salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona;
>
> Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos.

Dicho documento coloca el Nivel de Seguridad Alto como aplicable a los sistemas de datos personales que contengan datos relativos a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.

Los datos de salud se han consignado en un documento que en diversas latitudes lleva diferente nombre: expediente clínico, ficha clínica, historial médico o clínico. Sin embargo, la información encontrada en diversos artículos, libros y demás publicaciones en los últimos cinco años es variada y hace evidente la diferencia de opiniones sobre el significado de cada concepto.

---

[67] Publicados en la Gaceta Oficial del Distrito Federal del 26 de octubre del 2009.

El expediente clínico o historia clínica, desde una perspectiva médica, ha sido estudiada de manera pormenorizada por Laín Entralgo[68]. Sin embargo, en este apartado únicamente nos interesaremos por sus aspectos jurídicos. Desde esta perspectiva, ni la Ley General de Salud[69] ni la Ley de los Institutos Nacionales de Salud[70] de nuestro país, definen al expediente clínico. No obstante, esto se ha hecho a través de normas especiales, como la Norma Oficial Mexicana NOM-168-SSA1-1998, que se encuentra fuera del marco póstumo que rige la protección de los datos personales en el Distrito Federal.

La principal justificación de la existencia del expediente clínico está inserta en el contexto de la beneficencia. Si el médico lleva un registro de los datos que conciernen al paciente y anota todo aquello que le pueda ser útil para obtener un diagnóstico correcto, un pronóstico lo más certero posible y un tratamiento adecuado, es porque persigue el bien del paciente. Principio que ha guiado a la medicina desde siempre. Le interesa al médico no olvidar ningún detalle que le permita cumplir adecuadamente con este objetivo y dejar constancia de ello, le facilita volver continuamente a analizarlos, buscando claridad o explicaciones para lo que está observando en el presente.

En México, esta definición la ubicamos en la Norma Oficial Mexicana sobre el Expediente Clínico:

> … al 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, con arreglo a las disposiciones sanitarias.[71]

---

[68] Laín Entralgo, Pedro, *La historia clínica. (Historia y teoría del relato patográfico),* Barcelona, Salvat. 1961.

[69] Ley publicada en el Diario Oficial de la Federación el 7 de febrero de 1984, última reforma publicada en el Diario Oficial de la Federación el 15 de mayo de 2003.

[70] Ley publicada en el Diario Oficial de la Federación el 26 de mayo del 2000.

[71] NOM-168-SSA1-1998, publicada en el Diario Oficial de la Federación el 30 de septiembre de 1999, reformado el 22 de agosto de 2003. Sustituyó a la Norma Técnica 52 de agosto de 1998.

De esta definición podemos extraer las siguientes características del expediente clínico en México:

1. Es un conjunto de documentos ya sean escritos, gráficos e imagenológicos o de cualquier otra índole.

2. Incluye registros, anotaciones y certificaciones correspondientes a su intervención.

Cabe resaltar que el expediente clínico no sólo contiene datos de carácter sanitario. Junto a ellos siempre se encuentran, al menos, datos personales sobre la identidad del usuario o paciente y del centro sanitario. Además, también es frecuente que contenga otros datos personales acerca de las actividades laborales, aficiones, gustos, costumbres; informaciones acerca de su vida familiar; valoraciones subjetivas del médico; datos económicos acerca de los gastos e ingresos producidos durante la prestación sanitaria, etcétera.

Asimismo, los numerales 6 al 10 de la NOM señalan la integración de la información generada del expediente clínico: Consulta externa, Urgencias y Hospitalización, que no siempre ocurren. En este mismo sentido, la NOM establece que en el expediente clínico pueden existir otros documentos del ámbito ambulatorio u hospitalario, elaborados por personal médico, técnico y auxiliar o administrativo. Estos documentos se caracterizan porque su elaboración no corresponde sólo a los médicos, sino que pueden ser elaborados por el personal administrativo o el personal auxiliar.

Cabe señalar que la aplicación de este artículo además deberá seguir la interpretación de las siguientes normas jurídicas relativas a la protección de datos de salud en nuestro país: fracción V del artículo 57 del Reglamento de Servicios Médicos del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado; fracción II del artículo 22 y apartado A del artículo 111 de la Ley del Seguro Social; fracciones V y X del artículo 77 BIS de la Ley General de Salud; fracción II del artículo 10 de la Ley de Asistencia Social; fracciones II y III del artículo 16 BIS 2 de la Ley de Salud del Distrito Federal.

Artículo 19.- 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.

En el caso de que el tratamiento de los sistemas haya sido realizado por una persona distinta al ente público, el instrumento jurídico que dio origen al mismo deberá establecer el plazo de conservación por el usuario, al término del cual los datos deberán ser devueltos en su totalidad al ente público, quien deberá garantizar su tutela o proceder, en su caso, a la supresión.

Issa Luna Pla

COMENTARIO

El artículo 19 de la Ley de Protección de Datos Personales para el Distrito Federal se inserta dentro del Capítulo IV del Tratamiento de los Datos Personales y, en virtud de ello, se inscribe en la línea de los principios rectores de la protección que el propio cuerpo normativo desarrolla. Igualmente, los entes que administran datos personales en cesión por algún ente público que actuó bajo el mandato del acuerdo normativo, se encuentran obligados a cumplir, en solidaridad, las mismas reglas y principios de tratamiento de los sistemas de datos correspondientes.

Así, los Lineamientos para la Protección de Datos Personales en el Distrito Federal, publicados en la Gaceta Oficial del Distrito Federal del día 26 de octubre de 2009, hacen una llamada en el numeral 18 especificando:

> En el tratamiento de los datos personales los entes públicos deberán observar los principios de licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad que establece el artículo 5 de la Ley.

En continuidad de esta alusión, los comentados Lineamientos desarrollan a detalle la interpretación formal y lógica que deben guardar los principios de la Ley para que sean aplicados con particular cuidado en el tratamiento de los datos personales.

Ahora bien, el artículo 19 de la Ley en comento cumple diferentes funciones, todas ellas indispensables para el tratamiento lícito y en la línea de la protección de derecho a los datos personales para el Distrito Federal.

Primero. El mandato del artículo 19 consiste en hacer aplicable la caducidad de los sistemas de datos personales. Esto es, la existencia de bases de datos personales debe corresponder al tiempo de uso y finalidad que de ella se hará. En muchos países, la legislación comparada prevé que no podrán existir bases de datos con tiempos indefinidos, ya que se atentaría contra la voluntad del sujeto de la información que autoriza la utilización de sus propios datos para propósitos específicos y no indeterminados. De este modo, la Ley de Protección de Datos Personales para el Distrito Federal contempla dos mecanismos para determinar la terminación de los sistemas de datos personales, ya sea a través del mandato que creó el sistema de datos —o acuerdo— que establece la fecha de inicio y supresión de los datos, guardando una relación estrecha con la finalidad que originó la base; o bien porque las causas que dieron origen a la creación y uso del sistema de datos se extingan y así lo considere el ente público responsable del sistema.

El primer motivo de terminación de un sistema de datos queda claro, puesto que se trataría de un acto basado en fundamento jurídico directamente. Sin embargo, el legislador deja pendiente para el desarrollo de las normas secundarias la práctica de la segunda opción, es decir, cuando "dejen de ser necesarios para los fines por los cuales fueron recabados".

Para continuar con la interpretación del primer párrafo del artículo 19 de la LPDPDF, los Lineamientos para la Protección de Datos Personales aplicables al Distrito Federal prevén una definición para el principio de la *Finalidad*, esto es:

> 19. Para los efectos de la Ley y de los presentes Lineamientos se entenderá que:
>
> I. Con relación al principio de la licitud se considerará que la finalidad es distinta o incompatible cuando el tratamiento de los datos personales no coincida con los motivos para los cuales fueron recabados.

A esto se agrega el numeral 21 de los mismos Lineamientos, que define concretamente el término de *Finalidad determinada* y lo hace de la siguiente manera:

> 21. Los datos personales en posesión de los entes públicos deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe ser explícita, determinada y legal.

Así pues, la hipótesis normativa marca que procederá la supresión de aquellos sistemas de datos personales cuya finalidad haya terminado y su existencia y manejo dejen de ser necesarios en forma legítima. Concretamente, el ente público que emitió el acuerdo de creación podrá, en todo caso y mediante nuevo acuerdo, ordenar la supresión del sistema, con fundamento en la terminación del fin para el que fue creada.

En el supuesto de que los sistemas de datos persistan o continúen su "vida útil", en incumplimiento del artículo 19 de la Ley y aún después que se dé término a su causa y finalidad, entonces se estaría ante la violación del principio de legalidad de los sistemas. Por ello, los Lineamientos en el numeral 21 desarrollan el término referido como la "finalidad determinada" y vincula, con carácter de exclusividad, el uso de los datos a la finalidad de su creación. Ahora bien, la finalidad de este principio, siguiendo el numeral 21 de los Lineamientos, será "explícita" en cuanto a que esté expresamente delimitada mediante acuerdo publicado en la Gaceta Oficial del Distrito Federal; "determinada" en cuanto a que cumpla con un principio y un fin expresado en fechas concretas; y, "legal" en cuanto las dos condiciones anteriores se den, es decir, que la finalidad sea expresada por acuerdo y contenga fechas de inicio y término en las que su uso es permitido. Ambas condiciones deben guardar una perfecta correlación con las razones de finalidad de creación y uso de los datos personales.

La Ley de Protección de Datos Personales para el Distrito Federal permite la cesión de los sistemas a personas diferentes al ente público que los creó. Esta cesión tiene que ser realizada sin que se pierdan la vigencia de las condiciones y los requisitos que el acuerdo de creación, publicado en la Gaceta Oficial, debe contener. De esta

forma, al tiempo de que se autoriza la cesión de los sistemas, se traspasa igualmente la responsabilidad legal en el tratamiento de los datos personales y, enfáticamente, la finalidad determinada que caracteriza a cada sistema de datos.

Una vez que los sistemas de datos personales llegan al término de su plazo de finalidad, el ente al que fueron cedidos los datos deberá devolver "en su totalidad" los datos al ente público sobre quien pende la responsabilidad de tutelar, modificar o suprimir los datos personales.

Es así que tanto la Ley como sus Lineamientos hacen especial mención a las obligaciones del cesionario, es decir, quien recibe los datos en cesión adquiere las mismas responsabilidades y obligaciones de tutela de los sistemas de datos personales que las del ente que por acuerdo los creó. Inclusive, el numeral 34 de los Lineamientos prevé que los principios de finalidad y duración del tratamiento también quedan subsumidos hacia la persona del cesionario:

> El carácter adecuado de las medidas de seguridad que ofrece el cesionario se evaluará atendiendo las circunstancias que concurran en la transferencia, y en específico se tomará en consideración la naturaleza de los datos personales, la finalidad y la duración del tratamiento.

Lo anterior significa que el cesionario debe tomar en cuenta y como mandato legal con carácter de vinculante, la naturaleza, finalidad y duración del tratamiento de los datos personales.

Finalmente, es importante recalcar que la Ley y los Lineamientos hacen énfasis en que el cesionario deberá devolver todos y cada uno de los datos contenidos en un sistema al ente público de cuyo seno emanó el acuerdo de creación del sistema. Ello implica que el cesionario no podrá hacer un sistema paralelo, ya sea copiando o sustrayendo los datos personales de uno para colocarlos en otro, y resguardar dicho sistema aun cuando su término y finalidad hayan caducado. Tampoco podrá ceder la totalidad del sistema o algunos de sus datos personales a otro particular diluyendo las responsabilidades que tanto la Ley de Protección de Datos Personales para el Distrito Federal como sus Lineamientos prevén.

Artículo 20.- En caso de que los destinatarios de los datos sean instituciones de otras entidades federativas, los entes públicos deberán 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**.**

En el supuesto de que los destinatarios de los datos sean personas o instituciones de otros países, el responsable del sistema de datos personales deberá realizar la cesión de los mismos, conforme a las disposiciones previstas en la legislación federal aplicable, siempre y cuando se garanticen los niveles de seguridad y protección previstos en la presente Ley.

Miguel Carbonell

COMENTARIO

México es un Estado federal, de acuerdo a lo que proclama el artículo 40 de la Constitución Política de los Estados Unidos Mexicanos y a lo que desarrollan otros preceptos de la Carta Magna. El federalismo supone una división de competencias entre los distintos niveles de gobierno, pero también implica la necesidad de cooperación inter-territorial[72].

Muchos actos jurídicos celebrados en una determinada entidad federativa tienen efecto en el territorio de las demás. En la Constitución mexicana están previstos mecanismos de colaboración y reconocimiento de actos jurídicos locales en todo el territorio nacional (por ejemplo, y de manera amplia, en el artículo 121).

Ahora bien, el deber de "lealtad", colaboración, cooperación y reciprocidad que deben observar en sus relaciones recíprocas las entidades federativas, no impide que las leyes de cada una de ellas puedan señalar ciertas formalidades para efecto de proteger los derechos fundamentales de todos, cuando pudieran ponerse en riesgo[73].

---

[72] Un completo estudio sobre el federalismo se encuentra en Serna de la Garza, José María, *El sistema federal mexicano. Un análisis jurídico*, México, IIJ-UNAM, 2008.

[73] En la doctrina constitucional mexicana hay varias confusiones importantes acerca de los deberes

En este contexto considero que debe ser entendido el contenido del artículo 20 de la Ley de Protección de Datos Personales para el Distrito Federal. Su propósito es asegurar que la protección de tales datos no sea puesta en riesgo cuando se entreguen a instituciones de otras entidades federativas. Lo que se pide es que el nivel de protección sea igual o superior al que existe en el Distrito Federal.

El segundo párrafo del artículo en comento se refiere al caso de que algún organismo u autoridad del Distrito Federal tenga que ver con datos cuyos destinatarios sean personas o instituciones de otros países. En principio, aplica lo mismo que ya se ha dicho respecto de la transferencia de datos personales a otras entidades federativas; es decir, se deben asegurar niveles semejantes de seguridad y protección a los previstos en la Ley que estamos comentando.

Sin embargo, hay que añadir un par de elementos que destacan en este párrafo segundo. Por un lado, la Ley introduce una "formalidad" por cuanto a que ordena que se realice una "cesión", la cual debe correr a cargo del responsable del sistema de datos personales (recordemos que el concepto de "cesión de datos personales" está contenido en el artículo 2 de la Ley bajo análisis). Por otra parte, cabe mencionar también que el párrafo segundo remite a la ley federal en la materia para efecto de determinar la forma y procedimientos en que se debe hacer dicha "cesión".

La remisión es importante, dada la ya aludida división de competencias entre la Federación y las entidades federativas que existe en el régimen constitucional mexicano, pero también debido a que dicho régimen establece con claridad que las relaciones exteriores de México son competencia de las autoridades federales (ver al respecto los artículos 76 fracción I, sobre las facultades del Senado de la República, y 89 fracción X, sobre las atribuciones del titular del Poder Ejecutivo Federal). Las relaciones internacionales son conducidas por la Federación, por lo que tiene pleno sentido la remisión aludida.

---

que les incumben a las entidades federativas (y, en general, a los poderes locales) en relación con los derechos fundamentales. Al respecto, Carbonell, Miguel, *Los derechos fundamentales en México*, cit., pp. 115 y siguientes.

Artículo 21.- El titular del ente público designará al responsable de los sistemas de datos personales, mismo que deberá:

I. Cumplir con las políticas y lineamientos así como las normas aplicables para el manejo, tratamiento, seguridad y protección de datos personales;

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;

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;

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;

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;

VI. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido;

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;

IX. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales;

X. Elaborar un plan de capacitación en materia de seguridad de datos personales;

XI. Resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos de las personas;

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;

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;

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; y

XVI. Las demás que se deriven de la presente Ley o demás ordenamientos jurídicos aplicables.

Isabel Davara F. de Marcos

COMENTARIO

Obligaciones del responsable del tratamiento

La Ley dedica un artículo de su Capítulo V del Título II a las obligaciones de los entes públicos.

En concreto, el artículo 21 indica cuáles son las obligaciones que tendrá que cumplir el responsable de los sistemas de datos personales nombrado por el titular del ente público.

Los principios de la protección de datos indican cómo tienen que tratarse los datos por quien tiene acceso a ellos, tanto por el responsable como por el usuario. Una vez establecidos éstos, la Ley incluye también las obligaciones que con respecto al tratamiento de los datos tienen que cumplir los entes públicos, a través de los responsables del tratamiento de los sistemas de datos personales.

Obligaciones del responsable de los sistemas de datos personales

A efectos de analizar las obligaciones del responsable de los sistemas de datos personales, es necesario atender, en primer lugar, a los conceptos que se manejan en este artículo. El artículo se refiere a las obligaciones del responsable de los sistemas de datos personales, indicando que será el ente público quien lo designará.

El artículo 21 tiene que ponerse en relación con los artículos 1 y 2 de la Ley, relativos a su objeto y a las definiciones, respectivamente.

Así, el artículo 1, al referirse al objeto de la Ley, señala que ésta *"tiene por objeto establecer los principios, derechos, obligaciones*

y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los ***entes públicos****."* Por tanto, son los entes públicos los que en última instancia se encuentran sujetos al cumplimiento de la Ley y su normativa de desarrollo, puesto que son quienes están en posesión de los datos personales objeto de tratamiento.

El análisis de este artículo requiere volver a hacer referencia a las figuras del ente público y del responsable de los sistemas de datos personales.

Conforme al artículo 2 de la Ley es posible distinguir entre el:

> *Ente Público: 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;*

Como figura distinta a la del ente público, la Ley introduce la del responsable del sistema de datos personales, definiéndolo también en el artículo 2 como:

> *Responsable del Sistema de Datos Personales: Persona física que decida sobre la protección y tratamiento de datos personales, así como el contenido y finalidad de los mismos;*

Nótese que el artículo que comentamos establece las obligaciones que tendrá que cumplir, con respecto al tratamiento de datos personales, el responsable del sistema de datos personales. Es así que la Ley, conforme a lo dispuesto en su artículo 1, obliga al ente público puesto que es quien está en posesión de los datos personales y, por tanto, quien tiene que cumplir con los *"principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales"*.

Entendemos que hubiera sido necesario establecer claramente que las obligaciones son exigibles en última instancia al ente público, si bien serán cumplidas por los responsables de los sistemas de datos personales. Es decir, si el ente público es quien posee los datos tendrá que responder siempre del tratamiento, aunque será el responsable del sistema de datos quien observará el cumplimiento de estas obligaciones.

En otras palabras, en última instancia la responsabilidad es exigible al responsable, puesto que éste es quien está sujeto al régimen de infracciones previsto en la Ley. No obstante, el responsable podrá exigir por vía interna la responsabilidad que corresponda a cada una de las personas que hayan tenido alguna implicación en la comisión de la infracción de que se trate.

Por su parte, los Lineamientos definen al responsable en la fracción XVI de su apartado 2 de la siguiente manera:

> *Responsable: El 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.*

De manera que resulta claro que el ente público es quien está en posesión del sistema de datos personales, siendo el servidor público un responsable designado por el titular de dicho ente.

Designación del responsable del sistema de datos personales

Internamente, el titular del ente público tendrá un responsable del sistema de datos personales, que es quien tiene que cumplir, en la práctica, con las obligaciones que establece el presente artículo.

Es decir, la Ley se aplica a los entes públicos que, conforme al artículo 1, son quienes están en posesión de los datos personales, y el titular del ente público designará un responsable del sistema de datos personales.

No obstante, entendemos que dicha designación no supone una delegación de la responsabilidad que le corresponda al ente público, como responsable último, 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.

Cabe señalar, por último, que la Ley no dice nada sobre la posibilidad de que el titular del ente público sea designado como responsable del sistema de datos personales y también podría plantearse que haya más de un responsable. De nuevo, insistimos en que este o estos responsables son meramente internos, lo que supone una designación de funciones, correspondiendo en última instancia la responsabilidad al ente público como sujeto de obligaciones.

Clasificación de las obligaciones del responsable del tratamiento

A continuación, procederemos a clasificar las obligaciones del responsable del tratamiento según se refieran al interesado, al Instituto o al ente público:

Referida al	Obligación
Interesado	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; 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;
Instituto	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; 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; 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;
Ente público	I. Cumplir con las políticas y lineamientos así como las normas aplicables para el manejo, tratamiento, seguridad y protección de datos personales; 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; VI. Utilizar los datos personales únicamente cuando éstos guarden relación con la finalidad para la cual se hayan obtenido; 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; IX. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales; X. Elaborar un plan de capacitación en materia de seguridad de datos personales; XI. Resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos de las personas;

Referida al	Obligación
Ente público	XII. Establecer los criterios específicos sobre el manejo, mantenimiento, seguridad y protección del sistema de datos personales[74]; 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; 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;

Y por último, el artículo finaliza con una disposición de carácter general, ya que indica que el responsable del tratamiento también cumplirá con "*[l]as demás que se deriven de la presente Ley o demás ordenamientos jurídicos aplicables.*"

Desde otro punto de vista, las obligaciones establecidas en el artículo 21 pueden clasificarse también atendiendo al objeto de las obligaciones del responsable de los sistemas de datos personales de la siguiente manera:

Materia	Obligación
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;

[74] Nótese que los apartados IX y XI de la Ley se repiten

Materia	Obligación
Medidas de seguridad	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;

Artículo 22. El titular del ente público 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 del mismo.

Issa Luna Pla

COMENTARIO

Como se ha venido analizando, tanto la Ley de Protección de Datos Personales para el Distrito Federal, como los Lineamientos para la Protección de Datos Personales en el Distrito Federal publicados en la Gaceta Oficial del Distrito Federal del día 26 de octubre de 2009, concentran las atribuciones de creación, modificación y supresión de sistemas de datos personales en el titular del ente público, mediante acuerdo publicado en la Gaceta Oficial del Distrito Federal.

Así pues, el artículo 22 de la Ley de Protección de Datos Personales para el Distrito Federal se sirve en determinar, dentro del Capítulo V de las Obligaciones de los Entes Públicos, las competencias formales subjetivas en las que recaen la definición de la finalidad, contenido y uso del tratamiento del sistema de datos personales. Sin embargo, estas responsabilidades no se presentan de forma ilimitada, siempre y cuando se observe que devienen consecutivamente de las obligaciones listadas en el artículo 21 precedente de la Ley en comento.

El contenido normativo del artículo 22 de la Ley debe, entonces, ser interpretado en el marco de los principios del tratamiento de datos personales establecidos en el artículo 5 de la misma Ley, y en el constreñimiento de las obligaciones especificadas en el artículo 21.

En cuanto a los principios del tratamiento de los datos personales, es importante traer a colación fundamentalmente los siguientes, en su relación con el mandato del artículo 22 aquí comentado.

El principio de *legalidad* de los sistemas de datos personales vincula invariablemente la existencia y tratamiento de los datos personales, con la finalidad y uso que de ellos se haga. Este principio, que hace

las veces de base del tratamiento de los datos personales, también es recordado como una de las obligaciones del titular del ente público en el artículo 21, fracción VI, de la Ley en comento.

Igualmente, el principio de legalidad marca una línea normativa que en la aplicación del artículo 22 en comento no se debe perder de vista: que la posesión y el tratamiento de los sistemas de datos personales obedecerá "exclusivamente a las atribuciones legales o reglamentarias de cada ente público". Así es que, aunque la finalidad, contenido y uso son responsabilidad del titular del ente público, por ningún motivo esta decisión podrá apartarse de sus atribuciones legales o reglamentarias, ni tampoco la finalidad de los datos podrá ser adversa a estas atribuciones.

El siguiente principio fundacional de la protección de los datos personales y de los derechos ARCO del sujeto de la información es el *consentimiento*, previsto en el artículo 5 de la Ley comentada. Esto implica que, aunque es decisión del titular de la entidad pública la finalidad, contenido y uso de los datos, dicha facultad jurídica podrá ser ejercida siempre y cuando el titular cuente con el consentimiento expreso y por escrito del sujeto de la información para el uso y tratamiento de sus datos.

Por último, el artículo 22 necesariamente se aplica con base en la interpretación del principio de la *calidad* de los datos personales, y el de la *disponibilidad*. En cuanto al principio de la calidad, en la toma de decisiones sobre la finalidad, contenido y uso de los datos personales, el titular de la entidad pública deberá procurar la actualización de los sistemas de datos, tal y como lo contempla la obligación prevista en el artículo 21 de la Ley en comento en su fracción VIII. El principio de la disponibilidad recuerda al titular de la entidad pública que en su responsabilidad prevista en el artículo 22 aquí comentado, debe garantizar los derechos ARCO del sujeto de la información.

Ahora bien, el ejercicio de la responsabilidad de definir la finalidad, contenido y uso de los sistemas de datos personales que recae sobre el titular de la entidad pública, está condicionado a que, de manera general, cumpla con las siguientes obligaciones previstas en el artículo 21 de la Ley de Protección de Datos Personales para el Distrito Federal:

- Informar al sujeto de la información sobre la recolección de sus datos, que se conformará un sistema, la finalidad y sus usos.
- Adoptar procedimientos de acceso, rectificación, cancelación y oposición de datos personales (derechos ARCO).
- El deber de capacitar a los servidores públicos encargados de atender las solicitudes de información de datos personales.
- El deber de capacitar a los servidores públicos para el correcto tratamiento y la seguridad de los datos personales.
- Establecer los criterios específicos sobre el manejo, tratamiento y seguridad de los sistemas de datos personales.

De estas obligaciones, es posible analizar que la responsabilidad de decisión que coloca en el titular del ente público el presente artículo 22 de la Ley en comento, contempla el ejercicio de la toma de decisiones informada; esto es, que tanto el titular como el resto del personal autorizado para el uso y tratamiento de los datos personales, deben conocer la materia de la Ley y sus Lineamientos, así como organizar e incorporarse a programas de capacitación profesional.

Por su parte, el mandato del artículo 22 viene a ser complementado por las reglas previstas dentro de los Lineamientos de la Ley en comento. En el numeral 35, los Lineamientos prevén el siguiente desarrollo del mandato para la implementación de la responsabilidad sobre la decisión de la finalidad, contenido y uso de los sistemas de datos personales, a saber:

> El titular del ente público tiene la obligación de designar al o los servidores públicos responsables de los sistemas de datos personales, quienes deberán estar adscritos a la unidad administrativa en la que se concrete la competencia material del sistema. Los responsables tienen la atribución de decidir sobre el contenido y finalidad de los sistemas de datos personales.

Si bien el artículo 22 de la Ley es enfático en determinar la responsabilidad del titular de la entidad pública, también es cierto que esta responsabilidad puede ser delegada al personal de la misma Unidad Administrativa "en la que se concrete la competencia material, a cuyo ejercicio sirva instrumentalmente el sistema de datos y esté adscrito el responsable del mismo". De esta misma responsabilidad delegada también se deberá de informar al Instituto de Acceso a la Información Pública del Distrito Federal, tal y como lo manda la Ley. Para tales efectos, según el numeral 35 de los Lineamientos, el titular del ente público también deberá designar "al servidor público que fungirá como enlace entre el ente y el Instituto", esto para reportar del ejercicio de sus obligaciones y responsabilidad en la decisión sobre la finalidad, el contenido y el uso de los sistemas de datos personales.

Para el servidor público designado como enlace entre el ente y el Instituto, los Lineamientos en el numeral 38 desarrollan una serie de obligaciones derivadas de la responsabilidad que la Ley le encomienda, tales como:

I. Coordinar a los responsables de sistemas de datos personales al interior del ente público para el cumplimiento de la Ley, los Lineamientos y demás normativa aplicable;
II. Supervisar que los responsables mantengan actualizada la inscripción de los sistemas bajo su responsabilidad en el Registro electrónico creado por el Instituto;
III. Coordinar las acciones en materia de capacitación; y
IV. Remitir el informe a que hace referencia la fracción III del artículo 21 de la Ley.

En este marco de obligaciones se establece la responsabilidad de decisión sobre la finalidad, el contenido y uso de los datos personales y la delegación de dicha personalidad hacia un servidor público de la misma unidad administrativa que detenta la responsabilidad material, tal como lo establece el artículo 22 aquí comentado.

Artículo 23.- El Instituto de Acceso a la Información Pública del Distrito Federal es el órgano encargado de dirigir y vigilar el cumplimiento de la presente Ley, así como de las normas que de ella deriven; será la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales.

Miguel Carbonell

COMENTARIO

Todas las leyes, en orden a lograr su correcta aplicación, necesitan mecanismos de vigilancia y control, es decir mecanismos de garantía. Las garantías de los derechos pueden tomar distintas formas. Recordemos que, como ya se ha dicho en algunos comentarios previos, la protección de datos personales es un derecho fundamental de acuerdo con el párrafo segundo del artículo 16 constitucional. Algunas son de carácter administrativo, otras son judiciales; unas son de carácter preventivo (actúan antes de que acontezca una violación de derechos) y otras tienen una función restaurativa. No hay un único modelo de garantía para los derechos fundamentales[75]. Cada ordenamiento jurídico debe ir encontrando las propuestas y soluciones que se estimen más adecuadas, pertinentes y efectivas.

Respecto de los mecanismos institucionales para la protección de datos personales, hay distintos modelos. En algunos casos se crean instituciones encargadas exclusivamente de dicha función y, en otros, la tarea se asigna a instituciones ya existentes, que tienen competencias en materias cercanas y que, en esa virtud, suman la protección de datos a otros temas de los que ya venían conociendo.

En México el dilema era relativamente sencillo, desde el punto de vista del diseño institucional. La alternativa consistía en extender las competencias de los órganos de acceso a la información hacia el tema de los datos personales (que en buena medida ya tenían), o bien crear instituciones que atendieran específicamente el tema.

---

[75] Ver sobre el tema las reflexiones de Ferrajoli, Luigi, *Democracia y garantismo*, Madrid,. Trotta, 2008, pp. 60 y siguientes.

A nivel local la alternativa no era difícil de resolver, porque la competencia de las entidades federativas en la materia se limita al tema de los datos personales en posesión de los entes públicos, de tal suerte que se podía dar con pocos problemas una extensión de las competencias de las ya existentes comisiones de acceso a la información pública, que venían trabajando con anterioridad (con resultados sumamente diversos, hay que decirlo) en el ámbito propiamente gubernamental.

El dilema se acentúa en el caso de la Federación, dado que la competencia de sus órganos de garantía se debe extender hasta los datos personales que están en manos de particulares, según la reforma al artículo 73 de la Constitución. En ese caso la experiencia del IFAI, por ejemplo, es más limitada. Y lo mismo puede decirse, quizá incluso con mayor razón, respecto del resto de órganos garantes de los poderes federales (Congreso de la Unión, con sus dos órganos garantes correspondientes a la Cámara de Diputados y al Senado; y Poder Judicial Federal, con sus tres órganos garantes correspondientes a la Suprema Corte de Justicia de la Nación, al Consejo de la Judicatura Federal y al Tribunal Electoral del PJF), así como de los órganos garantes que existen en cada uno de los organismos constitucionalmente autónomos (Banco de México, INEGI, CNDH, IFE).

Dicho lo anterior, podemos decir que la determinación contenida en el artículo 23 de la Ley de Protección de Datos Personales para el Distrito Federal tiene mucho sentido al otorgarle competencias directivas y de vigilancia al Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF).

Las modalidades deónticas del mandato del artículo 23 se expresan a través de la orden al InfoDF de:

a) dirigir y vigilar el cumplimiento de la Ley y de las normas que de ella deriven;

b) garantizar, como autoridad encargada, la protección de los datos personales; y

c) garantizar, como autoridad encargada, el correcto tratamiento de los datos personales.

En la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal está claramente definida la naturaleza y las atribuciones del InfoDF:

> **Articulo 63.** El Instituto de Acceso a la Información Pública del Distrito Federal es un órgano autónomo del Distrito Federal, con personalidad jurídica propia y patrimonio propio, con autonomía presupuestaria, de operación y de decisión en materia de transparencia y acceso a la información pública, encargado de dirigir y vigilar el cumplimiento de la presente Ley y las normas que de ella deriven, así como de velar porque los principios de certeza, legalidad, independencia, imparcialidad y objetividad imperen en todas sus decisiones.

Del artículo 63 que se acaba de transcribir, es muy importante reparar en la naturaleza del InfoDF como órgano autónomo, ya que tal autonomía le da la posibilidad de configurarse como autoridad respecto de los demás poderes, para el único y exclusivo fin de lo que tiene que ver con el derecho de acceso a la información y la protección de datos personales.

El InfoDF es un órgano autónomo por lo que, en esa virtud, no está dentro de la estructura de ninguno de los demás poderes. Podríamos decir, guardadas las salvedades del caso, que se parece a lo que a nivel de la Constitución federal llamamos "órganos constitucionales autónomos".

Los órganos constitucionales autónomos surgen sobre todo a partir de la segunda guerra mundial, aunque fueron ya teorizados por autores como Georg Jellinek y Santi Romano desde finales del siglo XIX[76]. La existencia de dichos órganos supone un enriquecimiento de las teorías clásicas de la división de poderes que postulaban que dentro de un Estado solamente había tres funciones: la legislativa, la ejecutiva y la judicial.

En la actualidad se entiende que dentro de un Estado puede haber funciones distintas a las anteriores, o tareas que deban ser llevadas

---

[76] Carbonell, Miguel, "Órganos constitucionales autónomos" en *Diccionario de derecho constitucional,* 3ª edición, México, Porrúa, UNAM, 2009, tomo II, pp. 1053 y siguientes.

a cabo por órganos diferentes a los tradicionales. La realidad estatal contemporánea, que en los últimos tiempos se ha vuelto compleja y problemática, ha hecho surgir la necesidad de ir perfeccionando las formas de actuación de los órganos públicos y la distribución de funciones entre ellos. En este contexto comienzan a crearse los órganos constitucionales autónomos.

Siguiendo a Manuel García Pelayo, podemos establecer que las características de los órganos constitucionales autónomos son las siguientes:

1. Configuración inmediata por la Constitución; esto significa que es el propio texto constitucional el que prevé su existencia, pero sin limitarse simplemente a mencionarlos, sino determinando su composición, los métodos de designación de sus integrantes, su estatus institucional y sus competencias principales.

2. Una segunda característica de estos órganos es que resultan centrales para la configuración del modelo de Estado y, en este sentido, se vuelven necesarios e indefectibles en la medida de que si desaparecieran se vería afectada la globalidad del sistema constitucional o el buen funcionamiento del modelo de "Estado de Derecho".

3. Una tercera característica es que estos órganos participan en la dirección política del Estado, esto es, inciden en la formación de la voluntad estatal, ya sea en los procesos de toma de decisiones o en la solución de conflictos al interior del Estado de que se trate.

4. Los órganos constitucionales autónomos se ubican fuera de la estructura orgánica de los poderes tradicionales. Esto significa que no se pueden adscribir orgánicamente a ninguno de esos poderes: no forman parte de la administración pública (en ninguna de sus variables), ni del Poder Legislativo, ni tampoco del Judicial. Esta independencia orgánica se

manifiesta no solamente a través de la ausencia de controles burocráticos, sino también con la existencia de una cierta autonomía financiera o garantía económica a favor del órgano constitucional; de otra forma la independencia orgánica podría verse fácilmente vulnerada a través de la asfixia en el suministro de los recursos económicos. La obligación para el legislador de otorgar los fondos necesarios para el desempeño de las funciones de los órganos constitucionales autónomos formaría parte de la "garantía institucional" que se menciona párrafos adelante y que la Constitución les asegura, pues no se trata sólo de tener un ámbito de competencias constitucionalmente determinado, sino también de que ese ámbito cuente con los medios suficientes para poder ser actuado y actuable en la realidad cotidiana del Estado.

5. Otra característica de estos órganos, derivada justamente de su no incorporación orgánica dentro de ninguno de los tres poderes tradicionales señalados en el punto anterior, es que tienen una "paridad de rango" con los demás órganos y poderes, de tal forma que no se encuentran subordinados a ellos. Esto no significa, sin embargo, que las decisiones de los órganos constitucionales autónomos no sean controlables o revisables, p.e., por el Poder Judicial.

Para sintetizar lo anterior, se puede decir que los órganos constitucionales autónomos: *a)* son creados de forma directa por el texto constitucional; *b)* cuentan con una esfera de atribuciones constitucionalmente determinada, lo cual constituye una "garantía institucional" que hace que tal esfera no esté disponible para el legislador ordinario (esto significa que la ley no podrá afectar ese ámbito competencial garantizado por la Constitución e, incluso, no solamente no lo podrá afectar, sino que tendrá que asegurarlo y dotarlo de efectividad a través de la regulación concreta que por vía legislativa se haga de los mandatos constitucionales); *c)* llevan a cabo funciones esenciales dentro de los Estados modernos, y *d)* si bien no se encuentran orgánicamente adscritos o jerárquicamente subordinados a ningún otro órgano o poder, sus resoluciones —a menos que se trate

de órganos límite— son revisables de acuerdo con lo que establezca la Constitución de cada país.

De acuerdo con Trujillo Rincón[77], la noción de órgano constitucional autónomo, que prevalece en la mayor parte de la doctrina, considera como tales a "aquellos órganos a los cuales está confiada la actividad directa e inmediata del Estado, y que, en los límites del derecho objetivo, que los coordina entre sí, pero no los subordina unos a otros, gozan de una completa independencia y paridad recíproca, se encuentran en el vértice de la organización estatal, no tienen superiores y son sustancialmente iguales entre sí, no siéndoles aplicables ni el concepto de autarquía ni el de jerarquía".

Los órganos constitucionales autónomos deben ser distinguidos de los llamados "órganos auxiliares" u "órganos de relevancia constitucional". Estos últimos compartirían algunas, pero no todas, de las características que definen a los órganos constitucionales autónomos. Normalmente, la característica que les falta es la que tiene que ver con la no inclusión en la estructura orgánica de alguno de los poderes tradicionales. En este sentido, serían órganos auxiliares o de relevancia constitucional, por mencionar ejemplos que existen en el ordenamiento jurídico mexicano a nivel federal, la Entidad de Fiscalización Superior de la Federación, dependiente de la Cámara de Diputados (a. 79, C); el Consejo de la Judicatura Federal (a. 100, C) y el Tribunal Electoral (a. 99, C), éstos dos últimos integrados dentro de la estructura orgánica del Poder Judicial de la Federación. En estos tres casos, es la propia Constitución la que los crea y les asegura un ámbito competencial propio y definido, concediéndoles en algunos supuestos incluso facultades de órganos límite; es decir, de órganos que toman decisiones no revisables por ninguna otra instancia, pero manteniéndolos orgánicamente ubicados dentro de uno de los poderes tradicionales. En el derecho constitucional comparado existen muchas variedades de órganos auxiliares o de relevancia constitucional, tales como los tribunales de cuentas o los consejos económicos y sociales.

---

[77] Trujillo Rincón, Ma. Antonia, *Los conflictos entre órganos constitucionales del Estado,* Madrid, Congreso de los Diputados, 1995, pp. 41 y 42.

Algunos autores han propuesto la creación en México de otros órganos constitucionales autónomos o, al menos, órganos separados de los tres poderes tradicionales. Uno de ellos, quizá el más relevante, es la figura del Tribunal Constitucional, que, de acuerdo con el modelo diseñado por Hans Kelsen en la Constitución austriaca de 1920, no se encuadra dentro del Poder Judicial ordinario[78]. Otro podría ser el órgano constitucional autónomo en materia de medios de comunicación, que revisaría todo lo relativo a las concesiones televisivas y radiofónicas, a la correcta competencia dentro del sector de medios, aseguraría el derecho de réplica o rectificación en éstos, etc.

En cualquier caso, lo importante es señalar que la división de poderes es un esquema que sigue teniendo mucha relevancia en la actualidad y que, en esa virtud, debe mantenerse y mejorarse. Una de las formas en que dicho mejoramiento puede ocurrir es enriqueciendo tal división, de manera que el desempeño del Estado, considerado en su conjunto, sea cada vez mejor, más eficiente y legítimo.

Desde luego, al crearse los órganos constitucionales autónomos se deben prever los mismos principios de control y responsabilidad de sus miembros que existen para los demás poderes, de tal forma que la autonomía no sirva como excusa para dejar de cumplir con el ordenamiento jurídico. En este sentido, los órganos constitucionales autónomos deben desarrollar sus funciones con apego a los principios del Estado de Derecho.

Para lograr lo anterior, aunque sea en parte, se deben incluir a los órganos constitucionales autónomos dentro del elenco de sujetos legitimados para intervenir (ya sea de forma activa o pasiva) en las controversias constitucionales previstas en el a. 105 constitucional. Una de las características de un régimen democrático es la posibilidad de solventar las diferencias entre los diversos protagonistas del quehacer estatal de forma pública, a través de los mecanismos y procedimientos establecidos con ese fin por el ordenamiento jurídico.

---

[78] Kelsen, Hans, *La garantía jurisdiccional de la Constitución (La justicia constitucional)*, México, UNAM, 2001 (originalmente publicado en 1929).

En este sentido, resulta un poco disfuncional que, si en el ámbito de las funciones y tareas de los órganos constitucionales autónomos se presenta algún problema o diferencia con respecto a otro órgano del poder público, no se pueda resolver por mecanismos jurídicos—como las controversias constitucionales— y se tenga que acudir a otro tipo de arreglos, de carácter extra institucional.

Finalmente, la creación de los órganos constitucionales autónomos tampoco debe dar lugar a una especie de "fuga de la política", es decir, con el surgimiento de dichos órganos no se deben burlar los mecanismos tradicionales de mediación y de representación política. Los órganos constitucionales autónomos no pueden significar el traslado de facultades asignadas a los poderes públicos tradicionales hacia organismos que funcionen sin los adecuados controles democráticos (p.e., de carácter parlamentario) y de forma absolutamente transparente y diáfana. En este sentido, se tiene que buscar el diseño de un cuidadoso equilibrio entre el funcionamiento autónomo de los órganos constitucionales y su sujeción a los principios de legalidad, transparencia, rendición de cuentas y responsabilidad de sus integrantes, entre otros.

Respecto de los órganos constitucionales autónomos, sus características y alcances, deben tenerse presente en el ámbito de competencias correspondiente al Distrito Federal, al menos, las siguientes tesis jurisprudenciales, aprobadas por el Pleno de la SCJN:

> TESIS JURISPRUDENCIAL Núm. 13/2008 (PLENO) **ÓRGANOS AUTÓNOMOS ESTATALES. PUEDEN ESTABLECERSE EN LOS REGÍMENES LOCALES.** En la Constitución Política de los Estados Unidos Mexicanos no existe precepto que autorice expresamente la creación de órganos constitucionales autónomos; sin embargo, atendiendo a la evolución de la teoría tradicional de la división de poderes en la que se ha dejado de concebir la organización del Estado derivada de los tres poderes tradicionales (Legislativo, Ejecutivo y Judicial) que sin perder su esencia, ahora se considera como una distribución de funciones o competencias para hacer más eficaz el desarrollo de las actividades encomendadas al Estado, es como se ha permitido su existencia en el sistema jurídico mexicano, a través de diversas reformas constitucionales, sin que se advierta que la incorporación de dichos órganos autónomos sea privativa del órgano reformador de la Constitución Política de los Estados

Unidos Mexicanos, dado que conforme al régimen republicano, democrático y federal que establece la Norma Fundamental, los Estados de la República no están obligados a establecer, como órganos de poder, únicamente a los señalados en la Ley Suprema, puesto que en uso de la libertad soberana de que gozan en su régimen interior pueden, según sus necesidades, crear cuantos órganos consideren indispensables para su desarrollo, así como para atribuirles facultades y consignar las limitaciones pertinentes, siempre y cuando no contravengan las estipulaciones del Pacto Federal.

Controversia constitucional 32/2005.- Actor: Municipio de Guadalajara, Estado de Jalisco.- 22 de mayo de 2006. Unanimidad de ocho votos (Ausentes: Sergio Salvador Aguirre Anguiano, José Ramón Cossío Díaz y Olga Sánchez Cordero de García Villegas).- Ponente: Juan N. Silva Meza.- Secretario: Martín Adolfo Santos Pérez.

TESIS JURISPRUDENCIAL Núm. 12/2008 (PLENO) **ÓRGANOS CONSTITUCIONALES AUTÓNOMOS. SUS CARACTERÍSTICAS.** Con motivo de la evolución del concepto de distribución del poder público se han introducido en el sistema jurídico mexicano, a través de diversas reformas constitucionales, órganos autónomos cuya actuación no está sujeta ni atribuida a los depositarios tradicionales del poder público (Poderes Legislativo, Ejecutivo y Judicial), a los que se les han encargado funciones estatales específicas, con el fin de obtener una mayor especialización, agilización, control y transparencia para atender eficazmente las demandas sociales; sin que con ello se altere o destruya la tradicional doctrina de la división de poderes, pues la circunstancia de que los referidos organismos guarden autonomía e independencia de los poderes primarios, no significa que no formen parte del Estado mexicano, ya que su misión principal radica en atender necesidades torales tanto del Estado como de la sociedad en general, conformándose como nuevos organismos que se encuentran a la par de los órganos tradicionales. Ahora bien, aun cuando no existe algún precepto constitucional que regule la existencia de los órganos constitucionales autónomos, éstos deben: a) estar establecidos y configurados directamente en la Constitución; b) mantener con los otros órganos del Estado relaciones de coordinación; c) contar con autonomía e independencia funcional y financiera; y, d) atender funciones coyunturales del Estado que requieran ser eficazmente atendidas en beneficio de la sociedad.

> Controversia constitucional 32/2005.- Actor: Municipio de Guadalajara, Estado de Jalisco.- 22 de mayo de 2006.- Unanimidad de ocho votos (Ausentes: Sergio Salvador Aguirre Anguiano, José Ramón Cossío Díaz y Olga Sánchez Cordero de García Villegas).- Ponente: Juan N. Silva Meza.- Secretario: Martín Adolfo Santos Pérez.

Además de lo señalado, cabe recordar que el artículo 71 de la Ley de Transparencia local señala, entre las atribuciones del InfoDF, varias que son de interés para el tema que estamos analizando. Son las siguientes (se transcriben solamente las fracciones pertinentes):

> **Artículo 71.** El Pleno del Instituto sesionará al menos semanalmente y tendrá las siguientes atribuciones:
>
> III. Opinar sobre la catalogación, resguardo y almacenamiento de todo tipo de datos, registros y archivos de los entes públicos;
>
> IV. Proponer los medios para la creación de un acervo documental en materia de acceso a la información;
>
> X. Otorgar asesoría para la sistematización de la información por parte de los Entes Públicos;
>
> XIX. Establecer y revisar los criterios de custodia de la información reservada y confidencial;
>
> XXIII. Emitir recomendaciones sobre las clasificaciones de información hechas por los Entes Públicos;
>
> XXIV. Implementar mecanismos de observación que permita a la población utilizar la transparencia para vigilar y evaluar el desempeño de los Entes Públicos, de conformidad con las disposiciones jurídicas aplicables;
>
> XXV. Promover la capacitación y actualización de los Entes Públicos responsables de la aplicación de esta Ley;

Artículo 24.- El Instituto tendrá las atribuciones siguientes:

I. Establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que estén en posesión de los entes públicos, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta Ley;

II. Diseñar y aprobar los formatos de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;

III. Establecer sistemas electrónicos para la recepción y trámite de solicitudes de acceso, rectificación, cancelación y oposición de datos personales;

IV. Llevar a cabo el registro de los sistemas de datos personales en posesión de los entes públicos;

V. Elaborar y mantener actualizado el registro del nivel de seguridad aplicable a los sistemas de datos personales, en posesión de los entes públicos, en términos de esta Ley;

VI. Emitir opiniones sobre temas relacionados con la presente Ley, así como formular observaciones y recomendaciones a los entes públicos, derivadas del incumplimiento de los principios que rigen esta Ley;

VII. Hacer del conocimiento del órgano de control interno del ente público que corresponda, las resoluciones que emita relacionadas con la probable violación a las disposiciones materia de la presente Ley;

VIII. Orientar y asesorar a las personas que lo requieran acerca del contenido y alcance de la presente ley;

IX. Elaborar y publicar estudios e investigaciones para difundir el conocimiento de la presente Ley;

X. Solicitar y evaluar los informes presentados por los entes públicos respecto del ejercicio de los derechos previstos en esta Ley. Dicha evaluación se incluirá en el informe que de conformidad con el artículo 74 de la Ley de Transparencia y Acceso a la información pública presenta el Instituto a la Asamblea Legislativa del Distrito Federal y deberá incluir por lo menos:

a) El número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante cada Ente Público, así como su resultado;

b) El tiempo de respuesta a la solicitud;

c) El estado que guardan las denuncias presentadas ante los órganos internos de control y las dificultades observadas en el cumplimiento de esta Ley;

d) El uso de los recursos públicos en la materia;

e) Las acciones desarrolladas;

f) Sus indicadores de gestión; y

g) El impacto de su actuación.

XI. Organizar seminarios, cursos, talleres y demás actividades que promuevan el conocimiento de la presente Ley y los derechos de las personas sobre sus datos personales;

XII. Establecer programas de capacitación en materia de protección de datos personales y promover acciones que faciliten a los entes públicos y a su personal participar de estas actividades, a fin de garantizar el adecuado cumplimiento de los principios que rigen la presente Ley;

XIII. Promover entre las instituciones educativas, públicas y privadas, la inclusión dentro de sus actividades

académicas curriculares y extracurriculares, los temas que ponderen la importancia del derecho a la protección de datos personales;

XIV. Promover la elaboración de guías que expliquen los procedimientos y trámites materia de esta Ley;

XV. Investigar, substanciar y resolver el recurso de revisión en los términos previstos en esta Ley y en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal;

XVI. Evaluar la actuación de los Entes Públicos, mediante la práctica de visitas de inspección periódicas de oficio, a efecto de verificar la observancia de los principios contenidos en esta Ley, las cuales en ningún caso podrán referirse a información de acceso restringido de conformidad con la legislación aplicable;

XVII. Procurar la conciliación de los intereses de los interesados con los de los entes públicos, cuando éstos entren en conflicto con motivo de la aplicación de la presente Ley; y

XVIII. Las demás que establezca esta Ley, y demás ordenamientos aplicables.

Issa Luna Pla

COMENTARIO

El Instituto de Acceso a la Información Pública del Distrito Federal es la institución responsable del control y vigilancia[79], así como de la

[79] Se entiende aquí la función de control en términos de la aplicación de métodos que eviten el uso abusivo del poder y que se acaten los límites jurídicos establecidos por la norma. Ver Huerta, Carla, *Mecanismos constitucionales para el control del poder político,* Tercera edición, Instituto de Investigaciones Jurídicas, UNAM, México, 2010, p. 27.

protección de los datos personales y de la garantía de los derechos ARCO. La Ley de Protección de Datos Personales para el Distrito Federal le otorga dichos poderes al Instituto y, en consecuencia, lo dota de las atribuciones amplias que el artículo 24 establece para el ejercicio de dichos poderes.

Es posible agrupar las atribuciones que la Ley en comento le otorga al Instituto para el desarrollo eficaz de sus funciones en la protección de datos personales en tres grandes rubros: a) atribuciones de regulación; b) atribuciones administrativas; c) atribuciones educativas; d) atribuciones de evaluación y vigilancia; y, e) atribuciones resolutivas. El presente análisis profundiza en cada grupo aludiendo al texto normativo del artículo 24 y a los Lineamientos para la Protección de Datos Personales en el Distrito Federal publicados en la Gaceta Oficial del Distrito Federal del día 26 de octubre de 2009.

El artículo 24 de la Ley en comento robustece la función del Instituto de Acceso a la Información Pública del Distrito Federal dotándolo de poderes regulatorios que desarrollen y marquen las directrices interpretativas de la Ley en el proceso de su implementación cotidiana. Para ello, las fracciones I y IV expresan las facultades de emitir políticas, normas, lineamientos, opiniones, observaciones y recomendaciones de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales.

Como "políticas" debe entenderse el conjunto de decisiones, programas, definición de propósitos, productos o resultados, modelos y procesos que los entes públicos deben observar para la protección de los datos personales. Por normas y lineamientos se entienden los reglamentos, criterios, manuales y guías con carácter vinculante de observancia para los entes públicos. Por opiniones, observaciones y recomendaciones se entienden todas aquellas que, a petición de parte de cierta entidad pública o como producto del desempeño de sus facultades de verificación, el Instituto elabore en el ámbito de sus competencias. Así, las atribuciones reguladoras hacen del Instituto un real órgano garante de la protección de datos personales y verificador del cumplimiento de la Ley en comento.

Las atribuciones administrativas son aquellas que permiten al Instituto ejecutar su mandato de verificación y control entre los entes obligados a la Ley. Así, las fracciones del artículo 24 que desarrollan las atribuciones administrativas son la II, diseñar formatos de solicitudes; III, crear sistemas electrónicos; IV, llevar un registro de los sistemas; y V, elaborar y mantener el registro del nivel de seguridad de los sistemas. Estas atribuciones son fundamentales para el proceso de implementación de la Ley, donde el papel del Instituto es central en la conducción de los procesos de solicitudes de acceso, rectificación, cancelación y oposición de los datos personales, así como de la creación de los sistemas electrónicos y de registro que permitan a los entes públicos administrar la aplicación de la Ley con eficacia en el día a día.

Los sistemas electrónicos que permiten a los usuarios de Internet introducir por la vía remota solicitudes de cualquiera de los derechos ARCO al ente público, son de común utilización en el contexto en que se crea la Ley de Protección de Datos Personales para el Distrito Federal. Con ello, se pone al alcance de cierto público internauta el ejercicio de los derechos ARCO, sin necesidad de acudir a las oficinas burocráticas. Igualmente, la administración del registro de sistemas de datos personales requiere de gestiones que lo mantengan actualizado y seguro ante las amenazas informáticas que en la era de la información es común encontrar.

Ahora bien, las atribuciones educativas son aquellas que dotan al Instituto de una responsabilidad de difusión de la cultura de la protección de los datos personales que, puesto que la Ley lo manda, se suponen trascendentales tanto en los servidores públicos como entre los ciudadanos. Las fracciones VIII, IX, XI, XII, XIII, XIV presentan, a manera de atribución, actividades concretas de la labor de promoción educativa del derecho de protección de datos personales que el Instituto está facultado y obligado a emprender. Se entiende por orientar y asesorar las acciones de resolver consultas ciudadanas y de los entes públicos sobre el alcance de la Ley, ya sea por la vía electrónica, por medio de escrito o por llamadas telefónicas dirigidas a las oficinas del Instituto de Acceso a la Información Pública del Distrito Federal.

Luego vienen atribuciones que requieren de la promoción de actividades académicas importantes, tales como elaborar y publicar estudios e investigaciones, organizar seminarios, cursos y talleres; promover dentro de las instituciones educativas públicas y privadas la inclusión de temas vinculados con la protección de los datos personales dentro de su currículum de estudios; y elaborar guías prácticas que ilustren el proceso del ejercicio de los derechos ARCO ante los entes públicos.

Finalmente, dentro de las atribuciones educativas, en la fracción XII se prevé que el Instituto es responsable de establecer programas de capacitación y material explicativo dirigido a servidores públicos y a su propio personal, con el fin de facilitar el cumplimiento de sus obligaciones en el tratamiento de los datos personales, así como en la garantía del ejercicio de los derechos ARCO de los sujetos de la información. Cabe recalcar que la fracción XII del artículo 24 en comento prevé claramente que las acciones de capacitación del Instituto tendrán también el fin de "garantizar el adecuado cumplimiento de los principios que rigen la presente Ley", a manera de que sean éstos principios los que se comprendan y adopten dentro de la cultura administrativa de los sistemas de datos personales entre el personal del Gobierno del Distrito Federal.

En seguida se analizan las atribuciones de evaluación y vigilancia de la aplicación de la Ley entre los entes públicos que el Instituto es responsable de llevar a cabo. Dichas atribuciones se encuentran enunciadas en las fracciones siguientes: X, sobre la solicitud de informes de gestión de la implementación de la Ley que los entes públicos deberán rendir al Instituto en tiempo y forma; XVI, sobre la función de evaluación e inspección del Instituto para la verificación del cumplimiento e implementación de los principios de la protección y tratamiento de los datos personales. Los informes de las entidades públicas permitirán al Instituto reportar sobre las estadísticas referentes a:

a) El número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante cada Ente Público, así como su resultado;

b) El tiempo de respuesta a la solicitud;

c) El estado que guardan las denuncias presentadas ante los órganos internos de control y las dificultades observadas en el cumplimiento de esta Ley;

d) El uso de los recursos públicos en la materia;

e) Las acciones desarrolladas;

f) Sus indicadores de gestión; y

g) El impacto de su actuación.

Esta atribución pasiva del Instituto le permitiría utilizar estos datos reportados por las entidades y convertirlos en indicadores de gestión sobre el desempeño de la implementación de la Ley de Protección de Datos Personales para el Distrito Federal. Sin embargo, una atribución activa es la de realizar visitas de inspección periódicas de oficio a las oficinas para verificar el cumplimiento de la Ley, lo que le permite corregir y solventar errores de la administración de la Ley, así como identificar problemas que puedan obstaculizar la garantía de los derechos ARCO.

Por último, las atribuciones de resolución del Instituto de Acceso a la Información Pública del Distrito Federal refieren a un modelo de aplicación de la justicia cuasi-jurisdiccional y establecen un procedimiento de verificación, control y conciliación procesal que le permiten identificar violaciones a los derechos ARCO o, en su defecto, la detección del tratamiento ilícito de los datos personales. Las fracciones VII, XV y XVII terminan de hilar los poderes de resolución del Instituto.

Así pues, para los efectos iniciales de la función de resolución, la Ley otorga al Instituto las atribuciones de investigar, substanciar y resolver recursos de revisión, siguiendo el mismo procedimiento que establece la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, que prevé la garantía del derecho de acceso a la información pública.

Para las funciones de investigar y substanciar, los Lineamientos de la Ley en comento en el numeral 40 prevén que el Instituto: "tendrá acceso a los sistemas de datos personales, podrá inspeccionarlos y recabar toda la información necesaria para el cumplimiento de su función de control, podrá solicitar la exhibición o el envío de documentos y datos, así como examinarlos en el lugar en donde se encuentren instalados". Igualmente, el numeral 41 de los Lineamientos desarrollan el procedimiento mediante el cual el Instituto, en los términos del artículo 24, fracción XVI, de la Ley, podrá realizar las visitas de inspección para evaluar la actuación de los entes públicos.

Ahora bien, se entiende por recurso de revisión, en los términos del artículo 76 de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, como el mecanismo de inconformidad que el solicitante puede interponer de manera directa o por medios electrónicos ante el Instituto. Según el artículo 82 de la Ley de Transparencia, en el recurso de revisión el Instituto podrá: desechar el recurso por improcedente o sobreseerlo; confirmar el acto o resolución impugnada por el interesado; revocar o modificar las resoluciones del ente público y ordenarle que permita el acceso a los datos personales, que reclasifique la información o que modifique tales datos.

Finalmente, el Instituto cuenta, por mandato del artículo 24 de la Ley en comento, con la atribución, que más bien se frasea como obligación, de hacer del conocimiento del órgano de control interno del ente público las resoluciones que emita relacionadas con la probable violación a las materias de la Ley, y procurar la conciliación de los intereses de los sujetos de la información con los intereses de los entes públicos cuando entren en conflicto sobre la aplicación de la Ley.

En suma, el artículo 24 de la Ley en comento hace efectivos los poderes de verificación y control del Instituto de Acceso a la Información Pública del Distrito Federal, pero también aquellos de evaluación del cumplimiento de la Ley y de garantía del ejercicio expedito de los derechos ARCO que integran la protección de los datos personales en el Distrito Federal.

Artículo 25.- A efecto de impulsar una cultura de protección de datos personales, se deberá promover el desarrollo de eventos que fomenten la profesionalización de los servidores públicos del Distrito Federal, sobre los sistemas y las medidas de seguridad que precisa la tutela de los datos personales de cada ente público.

Miguel Carbonell

COMENTARIO

La Constitución mexicana ha sido reformada con intensidad en los últimos años. Una parte considerable de tales reformas ha afectado, como no podría ser de otra manera, a la regulación de los derechos fundamentales. Unos han ido ampliando su esfera constitucionalmente protegida; otros se han incorporado progresivamente en nuestra Carta Magna.

Tal es el caso, respecto de los temas que nos ocupan, del derecho de acceso a la información pública (artículo 6 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos) y del derecho a la protección de datos personales (artículo 16 párrafo segundo de la misma Constitución). Se trata, en ambos casos, de derechos completamente nuevos para la cultura jurídica, política e incluso social de México, cuya comprensión en clave normativa no es nada fácil.

La regulación constitucional es relativamente escueta y, como corresponde, está redactada sobre la base de grandes principios. Las leyes que desarrollan los preceptos constitucionales, por su parte, contienen un buen número de conceptos y demás cuestiones técnicas que no son comprensibles siempre en una primera lectura.

Por todo lo anterior, se justifica plenamente el mandato del artículo 25 de la Ley de Protección de Datos Personales para el Distrito Federal, en el sentido de que se promuevan eventos que fomenten la profesionalización de los servidores públicos locales, sobre los

sistemas y las medidas de seguridad que requieren los datos personales que estén en poder de los órganos públicos.

De hecho, quizá sería necesario ir más allá de lo que resulta obligatorio en términos del artículo en comento, para generar una verdadera cultura alrededor de la protección de datos personales. Como es de sobra conocido por quienes se dedican a estudiar estos temas, la completa y eficaz protección de datos personales requiere un trabajo intenso en la generación de una cultura alrededor del tema. Pero esa cultura no puede ni debe ser patrimonio exclusivo de las autoridades que administran tal tipo de datos. Por el contrario, se debe extender más allá de los funcionarios.

Una cultura democrática, sustantiva y robusta de la protección de datos personales debería considerar temas como los siguientes:

1. La separación conceptual y normativa entre lo público y lo privado. Si no entendemos esta distinción primaria será muy difícil comprender el significado y alcance del derecho a la protección de los datos personales[80].

[80] Uno de los signos de las democracias contemporáneas es la separación entre actividades públicas y actividades privadas de los individuos. Si esa separación no existiera se correría el riesgo de caer en alguno de los dos extremos siguientes: o bien se pulverizarían varios de los derechos fundamentales más importantes dentro de la lógica del Estado constitucional (como el derecho a la inviolabilidad del domicilio, la libertad de creencias, la libertad ideológica, la libertad de procreación, etcétera), o bien —en el otro extremo— se diluirían varios de los sistemas de control que actualmente existen para verificar la actuación de las autoridades (las reglas de comportamiento que rigen en el ámbito público son distintas que las que existen en el ámbito privado, y para los funcionarios públicos se crea todo un sistema de mecanismos de verificación que solamente se pueden mantener para el caso en que la distinción entre público y privado sea clara).

2. Las bases constitucionales de los derechos que entran en contacto (y a veces en tensión) con el derecho a la protección de datos personales: derecho de acceso a la información pública, libertad de expresión y libertad de prensa. Además, en los tratados internacionales de derechos humanos se encuentran otros derechos que también confluyen en la temática general de los datos personales, como por ejemplo, el libre desarrollo de la personalidad, el derecho a la vida privada, el derecho al honor, etcétera[81].

3. Las políticas públicas que se deben ir instrumentando para proteger los datos personales: reingeniería institucional, organigramas apropiados, diseño de flujogramas de datos y procesos, determinación de niveles de responsabilidad intra-orgánica, etcétera.

4. El papel de los particulares en el tema de la protección de los datos personales. Si bien es cierto que a nivel local las autoridades no tienen competencia para legislar en materia de datos personales que estén en manos de particulares (tema que está reservado al Congreso de la Unión por mandato del artículo 73, fracción XXIX inciso O), esto no impide que se capacite en el tema y que se difunda el derecho entre los propios particulares, en tanto que son titulares del mismo derecho. Sería absurdo suponer que la capacitación se debe limitar a las autoridades, sin involucrar también de alguna manera a la sociedad civil organizada.

---

[81] Carbonell, Miguel, *Los derechos fundamentales en México*, cit., pp. 367 y siguientes.

Artículo 26.- Todas las personas, previa identificación mediante documento oficial, contarán con los derechos de acceso, rectificación, cancelación y oposición de sus datos personales en posesión de los entes públicos, siendo derechos independientes, de tal forma que no puede entenderse que el ejercicio de alguno de ellos sea requisito previo o impida el ejercicio de otro.

La respuesta a cualquiera de los derechos previstos en la presente ley, deberá ser proporcionada en forma legible e inteligible, pudiendo suministrase, a opción del interesado, por escrito o mediante consulta directa.

Isabel Davara F. de Marcos

COMENTARIO

Derechos en protección de datos

Vistos los principios que rigen el tratamiento de datos, las distintas regulaciones, a nivel nacional e internacional, prevén la existencia de unos derechos de los titulares de dichos datos en los que se concretan los mencionados principios, como instrumento propicio para controlar el tratamiento que haga el responsable del sistema de datos personales.

La Ley dedica a esta materia el Capítulo I, derechos en materia de datos personales, del Título IV, relativo a los derechos y el procedimiento para su ejercicio.

El artículo 26 enumera los citados derechos indicando algunas características generales en relación con su ejercicio.

En el entorno hispanoparlante se ha acuñado con cierto éxito el acrónimo ARCO para referirse a los derechos de Acceso, Rectificación, Cancelación y Oposición, que son los más conocidos y utilizados en la práctica[82].

---

[82] No podemos olvidar, en modo alguno, otros derechos como los de consulta al registro de

No obstante, dicho acrónimo no implica en absoluto su dependencia[83], de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro, como expresamente indica la Ley.

Son derechos personalísimos[84] [85] y de los que siempre tiene que atenderse su ejercicio, pero esto no quiere decir que se conceda lo pedido[86].

---

ficheros o sistemas de datos personales, la impugnación de valoraciones y la indemnización, reconocidos y desarrollados en las normativas de protección de datos de otros países.

[83] Siguiendo con la LOPD en el caso español, la AEPD se ha pronunciado respecto de las características comunes de estos derechos:

> Características generales de los derechos de protección de datos (Memoria 2001, págs. 139 y 140).
>
> *Los derechos de acceso, rectificación, cancelación y oposición de los datos de carácter personal contenidos en ficheros automatizados, se configuran como uno de los ejes fundamentales sobre los que se articula la protección de los datos de ciudadanos(...). Los derechos de acceso, así como los de rectificación, cancelación y oposición de datos son* ***derechos personalísimos*** *y los responsables de los ficheros, resolverán sobre la solicitud en los plazos establecidos por la ley. En el supuesto de que el responsable considere que no procede acceder a lo solicitado por el afectado, se lo comunicará motivadamente en el plazo legalmente establecido. Si no fuere debidamente atendido, el afectado podrá reclamar ante la Agencia de Protección de Datos.*
>
> *La norma Primera de la Instrucción 1/1998, establece los requisitos generales a cumplir tanto por el ciudadano en la solicitud del ejercicio de los derechos como por parte del responsable del fichero con objeto de resolver sobre la solicitud.(...) Obviamente, no es competencia ni voluntad de esta Agencia regular el ejercicio de prácticas comerciales o relaciones negociales entre proveedor y cliente, pero sí entiende que a fin de dar una mejor respuesta a los ciudadanos en el ejercicio de sus derechos, sería conveniente que los responsables de los ficheros establecieran un procedimiento documentado con objeto de su conocimiento y cumplimiento por parte de todas las personas que integran la organización.*

[84] Al respecto, ver supra "son personalísimos".

[85] Es decir, sólo pueden ser ejercitados por su titular o por su representante legal. en caso de minoría de edad o incapacidad, previa la acreditación correspondiente de acuerdo con las previsiones aplicables.

[86] Así por ejemplo, una solicitud de cancelación por haber finalizado la relación parece que no puede negarse en ningún caso, porque no existe ninguna justificación o necesidad para el desarrollo de ninguna relación jurídica obligatoria, por lo que habría que conceder lo pedido, pero

Los derechos de los titulares de los datos deberían ser la concreción de los principios que estructuran el sistema de protección de datos.

Este artículo, como decíamos, menciona los derechos más "populares" o relevantes, al menos cuantitativamente hablando[87]. Pasaremos a analizarlos no sin antes detenernos brevemente en alguna otra cuestión general.

La identidad del titular

El ejercicio de los derechos de protección de datos le pertenece al titular de éstos.

Ya hemos reiterado que lo que se protege es al titular, no a los datos en sí.

Entendemos que la Ley quizá no es el lugar adecuado para desarrollar los requisitos de identificación que se le puedan exigir al demandante, pero al menos debería haber alguna reseña al respecto, tal como "según los medios acreditados en Derecho", o una referencia a un desarrollo reglamentario posterior. Incluso cuando el artículo 4 de la Ley establece las normas de aplicación supletoria a lo no previsto en la Ley, se trata de garantizar que el interesado que va a ejercitar un derecho no tenga que buscar por sí mismo cuáles son éstas, considerando que en ocasiones puede desconocer qué normas son aplicables al respecto.

En este sentido, por ejemplo, atendiendo a la experiencia de otros Estados, el Reglamento de la Ley de Chihuahua[88] en su artículo 67 prevé:

---

si quedaran pendientes obligaciones que cumplir y solicitara cancelar sus datos, habría que atender su solicitud, esto es, contestar, pero no proceder a la cancelación, porque sus datos son necesarios para el mantenimiento y desarrollo de la relación en concreto.

87 Que son los mismos especificados en las reformas a los artículos 6 y 16 Constitucionales.

88 Reglamento de la Ley de Transparencia y Acceso a la Información Pública del Estado de Chihuahua, publicado en el Anexo al Periódico Oficial del 30 de diciembre de 2006.

> ***Artículo 67.-*** *La acción de Hábeas Data o protección de datos personales es aquella que podrán ejercer los titulares de los datos personales, sensibles o información personalísima, y que tiene por objeto acceder, actualizar, rectificar, suprimir o mantener la confidencialidad de dicha información.*
>
> *Los requisitos para el ejercicio de la acción de Hábeas Data o de protección de datos personales, son los siguientes:*
>
> *I.- Nombre de la persona interesada o de su representante legal.*
>
> *La persona interesada deberá identificarse plena e indubitablemente mediante documento suficiente para tal efecto, mientras que quien ostente, en su caso, la representación legal, deberá acreditarla en los términos de la legislación civil (…)*

Aunque la expresión "documento suficiente para tal efecto" puede resultar un poco vaga, al menos es una concreción del extremo que señalábamos.

De nuevo, podría pensarse en un desarrollo posterior (incluso vía Manual de Usuario) o una aplicación de procedimientos similares.

No obstante, el artículo 26 de la LPDPDF establece que el ejercicio de los derechos requiere que el interesado, quien es el titular de los datos, se identifique mediante documento oficial, sin añadir nada más. Otra vez, en virtud del principio de supletoriedad de la Ley, es necesario recurrir en este caso al artículo 41 de la Ley de Procedimiento Administrativo del Distrito Federal.

Para acreditar la identidad del titular o representante legal, se deberá presentar documento oficial en original como: credencial para votar, pasaporte vigente, cartilla del servicio militar, cédula profesional, credencial de afiliación al Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, al Instituto Mexicano del Seguro Social o al Instituto Nacional de Personas Adultas Mayores (INAPAM).

Cuando no se tenga ninguno de estos documentos, se procederá conforme a las normas del derecho común.

Es decir, hay que recordar que los datos son de su titular, quien podrá ejercitar los derechos para instar al responsable a garantizar sus derechos a la protección de datos, avalando que los datos cumplen con los principios de la Ley y los Lineamientos.

Son personalísimos

De ahí que la identidad del titular sea crucial.

En principio, si no se identifica plenamente, no se puede ejercer ninguno de los derechos que conlleva dicha titularidad (acceso, rectificación, cancelación u oposición).

Si bien es cierto que es el titular de los datos el único habilitado para ejercerlos, la realidad impone ciertas situaciones en las que se necesita que el representante legal los ejerza[89].

Así ocurre en el caso de menores de edad u otros incapacitados legalmente, cuya capacidad jurídica tendrá que ser suplida por quien ostente su representación legal. La necesidad de esta capacidad legal resulta clara en tanto que se trata del ejercicio de un derecho que supone obligarse jurídicamente.

En la práctica, se plantean supuestos específicos que tienen que ser tratados de manera analítica. Aunque no es el objetivo de estos comentarios, es posible indicar que en el caso de los menores hay que distinguir entre menores emancipados y no emancipados. De acuerdo al Código Civil para el Distrito Federal, que se aplicaría con carácter supletorio en virtud del artículo 4 de la Ley, no habría duda respecto de los menores emancipados cuando tengan dieciséis (16)

[89] Puede pensarse, por ejemplo, en el supuesto ya desarrollado en otros lugares sobre el ejercicio de los derechos de protección de datos en el caso de personas fallecidas.

años. En el resto de los supuestos, será necesario atender al criterio seguido por el Instituto.

En el ámbito internacional, resulta habitual que los menores que tengan catorce años (14) puedan ejercer sus derechos, puesto que se les reconoce capacidad para otorgar el consentimiento necesario para tratar sus datos.

Otros supuestos específicos son, por ejemplo, el relativo a los fallecidos. Al respecto, de nuevo recurriendo al Código Civil del Distrito Federal por su carácter de aplicación supletoria, resulta claro que, conforme a su artículo 22, la capacidad jurídica de las personas físicas se pierde por la muerte. El fallecimiento supone también la extinción del derecho a la protección de datos. Por lo tanto, en este caso serían los herederos del fallecido quienes lo podrían ejercer.

Acceder, actualizar, rectificar, suprimir o impedir el tratamiento

Además del derecho de acceso se suelen reconocer los derechos de rectificación, cancelación y oposición.

Los términos actualizar y rectificar aluden al derecho de rectificación, que opera cuando el titular de los datos entiende que éstos son inexactos o no adecuados en relación con la finalidad del tratamiento.

También puede operar a instancias del responsable del archivo, cuando conozca de la inexactitud de los datos.

En todo caso, el derecho de rectificación no puede considerarse absoluto. Es decir, no puede entenderse que siempre se tenga que realizar aquello que el titular demande.

Siempre se tendrá que atender el derecho, pero lo pedido puede no coincidir con lo concedido. Es decir, pueden darse ocasiones en que el titular de los datos no pueda exigir la rectificación porque ésta no proceda, justificada y legalmente hablando.

Siempre podrá demandar que se le atienda en su petición, pero atenderle no tiene que significar conceder su petición. Lo mismo podríamos decir del derecho de cancelación.

El derecho de cancelación, técnicamente hablando, no da lugar a la supresión, sino al bloqueo de los datos. Salvo en los supuestos en los que procede de inmediato la supresión de los datos, la cancelación dará lugar al bloqueo de los datos para, una vez transcurridos los plazos establecidos legal o contractualmente, proceder a su supresión.

Aunque puede parecer una diferencia muy sutil, lo cierto es que las consecuencias son muy diferentes.

Cuando se cancela un dato, porque ya no es pertinente para la finalidad para la que fue recabado y tratado, se debe proceder a su bloqueo, no a su supresión. Suprimir implica borrar, hacer desaparecer el dato.

Cancelar implica que ese dato no puede estar accesible para nadie, salvo las autoridades competentes en el ejercicio de sus funciones, mientras duren los plazos de prescripción de las acciones que se puedan derivar del tratamiento del dato en cuestión.

Como decíamos, aunque parezcan distinciones sutiles, lo cierto es que, mientras en la cancelación el dato sigue existiendo, aunque no se deba bajo ninguna circunstancia fuera de las mencionadas acceder al mismo, en la supresión el dato se elimina, y con ello toda acción posterior que se pueda o deba realizar con él. Por tanto, cancelar significa que el dato será bloqueado, de manera que seguirá existiendo, y una vez que transcurran los plazos establecidos, se procederá a su supresión para dejar de existir.

Finalmente, el desarrollo de estos derechos requiere de una concreción regulatoria posterior, donde se establezcan plazos y formas, así como sanciones en caso de incumplimiento.

Por otra parte, el derecho de oposición consiste en que el titular, en los supuestos en que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una ley no disponga lo

contrario, podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos.

Asimismo, en la normativa internacional encontramos otros derechos. Por ejemplo, la Directiva 95/46/CE, ya mencionada, también prevé otro derecho relativo a la posibilidad del titular de los datos de impugnar las valoraciones que de él se hagan como resultado del tratamiento de sus datos de carácter personal. Por último, en otras normativas nacionales se prevén otros derechos concretos, como el derecho de los interesados a recurrir a los Tribunales con objeto de obtener una compensación cuando se hayan vulnerado sus derechos respecto a otros bienes jurídicos protegidos, como el derecho al honor y a la intimidad.

Excepciones al ejercicio de los derechos

En materia de excepciones al ejercicio de los derechos debemos remitirnos al artículo 12, ya analizado. No obstante, creemos conveniente hacer una breve referencia a esta cuestión.

En este sentido, recordemos que la reforma al artículo Decimo Sexto Constitucional[90] ya establece 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*".

Como dijimos, probablemente un reenvío a un desarrollo legal posterior sería deseable en muchos de los términos.

---

[90] Pero la anterior reforma del artículo Sexto Constitucional al respecto señala que: "*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*".

Artículo 27.- El derecho de acceso se ejercerá 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, en términos de lo dispuesto por esta Ley.

Isabel Davara F. de Marcos

COMENTARIO

El artículo 27 se refiere específicamente al derecho de acceso. Reconoce el derecho del interesado a solicitar y obtener información de sus datos que son objeto de tratamiento, el origen de éstos y las cesiones realizadas o que se prevean realizar[91].

Volviendo a proponer un análisis empírico de estos derechos, éste debe hacerse con relación a un ordenamiento práctico en concreto. Precisamente, en nuestro ordenamiento jurídico, al igual que en otros, tenemos que comenzar por decir que son los que plantean más interrogantes y problemas en la práctica.

Como decíamos, el derecho de acceso es personalísimo[92] y, por tanto, sólo puede ser ejercido por el titular ante el responsable del tratamiento o sistema de datos personales, excepto en caso de incapacidad o minoría de edad, pudiendo entonces actuar el representante legal del afectado. En este sentido, tal y como se indicó anteriormente y siguiendo además el criterio establecido por el Pleno del Instituto, el acceso de los menores de edad será posible en aquellos supuestos en los que proceda, tal y como ocurre en el caso de los menores emancipados.

Es importante resaltar que el acceso no implica que el interesado conozca quién trata sus datos dentro del ente público[93]. Si atendemos

---

[91] Nótese que la redacción de dicho artículo es muy similar a la del artículo 15.1 de la LOPD.

[92] En la Resolución R (73) del Comité de Ministros del Consejo de Europa se enuncia claramente este derecho y en especial su carácter personalísimo, a pesar de lo reducido de su texto: *"6. As a general rule, the person concerned should have the right to know the information stored about him, the purpose for which it has been recorded, and particulars of each release of this information. (…) 9. Access to the information stored should be confined to persons who have a valid reason to know it. The operating staff of electronic data banks should be bound by rules of conduct aimed at preventing the misuse of data and, in particular, by rules of professional secrecy."*

[93] En este sentido, en el caso español el Informe Jurídico 167/2005 de la Agencia Española de

al Derecho comparado, cabe señalar que, en este sentido, en el caso español el Informe Jurídico 167/2005 de la Agencia Española de Protección de Datos, sobre la naturaleza y alcance del derecho de acceso, indica que "el derecho concedido al interesado por la Ley únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de organización del responsable del fichero, han podido tener acceso a dicha información."

El acceso se refiere al tratamiento de datos por el responsable, que tiene la obligación de responder por el tratamiento de los datos personales, siendo una cuestión interna quién trate finalmente los datos en el ejercicio de sus correspondientes funciones.

Significado del derecho de acceso

Un aspecto esencial en el análisis del derecho de acceso es el relativo a su propio significado.

Es importante distinguir entre el acceso a datos de carácter personal y el acceso a la información pública o gubernamental, ya que se trata de dos derechos diferentes. Por un lado, el derecho de acceso a los datos personales y por otro lado el derecho de acceso a la información pública gubernamental.

En el caso de la LPDPDF, resulta claro que ésta tutela el acceso a los datos de carácter personal, como aspecto de la privacidad de los interesados. Por tanto, el acceso a la información pública no es objeto de esta Ley.

Es decir, el derecho de acceso faculta al interesado, cuyos datos personales son objeto de tratamiento, a obtener información sobre dicho tratamiento.

Protección de Datos, sobre la naturaleza y alcance del derecho de acceso, indica al respecto que "el derecho concedido al interesado por la Ley únicamente abarcaría el conocimiento de la información sometida a tratamiento, pero no qué personas, dentro del ámbito de organización del responsable del fichero han podido tener acceso a dicha información."

Con carácter general, el derecho de acceso puede ser ejercitado por cualquiera, puesto que cualquier interesado puede querer saber si un ente público trata sus datos de carácter personal. Cuestión distinta es que efectivamente se traten sus datos y que la respuesta al interesado se limite a comunicarle que no se produce el tratamiento de éstos.

Acceso a los datos y acceso a la información pública

Tal y como se apuntaba en el apartado anterior, es necesario distinguir entre el derecho de acceso a los datos personales, que permite al interesado conocer y controlar el tratamiento de sus datos de carácter personal, y el acceso a la información pública o a los documentos, que permite, entre otras cosas, controlar la actividad de la Administración Pública y garantizar su transparencia.

Se trata de una cuestión compleja en la que resulta claro que es necesario atender al ámbito de aplicación de cada una de las normas.

En cuanto a la interpretación jurisprudencial de esta cuestión, consideramos oportuno resaltar a nivel de Derecho comparado una sentencia del Tribunal de Primera Instancia de la Unión Europea[94] que trata sobre esta cuestión y que indica lo siguiente:

> *66 El SEPD subraya la necesidad de mantener un equilibrio óptimo entre la protección de los datos personales, por una parte, y el derecho fundamental del ciudadano europeo de tener acceso a los documentos de las instituciones, por otra parte. Pues bien, el razonamiento de la Comisión no tiene correctamente en cuenta este equilibrio, que se rige explícitamente por el artículo 4, apartado 1, letra b), del Reglamento nº 1049/2001. En efecto, una solicitud de acceso a documentos se basa en principios democráticos y no es necesario mencionar las razones por las que se solicitan los documentos y, por consiguiente, no es pertinente*

[94] Sentencia del Tribunal de Primera Instancia (Sala Tercera), de 8 de noviembre de 2007, «Acceso a los documentos – Reglamento (CE) nº 1049/2001 – Documentos relativos a un procedimiento por incumplimiento – Decisión por la que se deniega el acceso – Protección de las personas físicas respecto del tratamiento de datos personales – Reglamento (CE) nº 45/2001 – Concepto de intimidad» en el asunto T-194/04. Esta sentencia ha sido recurrida ante el Tribunal de Justicia y a la fecha de cierre de este análisis todavía estaba pendiente.

la aplicación del artículo 8 del Reglamento nº 45/2001 en el caso de autos. Asimismo, el SEPD estima que las normas sobre protección de datos no permiten deducir de ellas un derecho general a participar, de forma anónima, en actividades públicas.

67 Según el SEPD, el interés protegido en el artículo 4, apartado 1, letra b), del Reglamento nº 1049/2001 es la intimidad y no la protección de datos personales, que es un concepto mucho más amplio que el de intimidad. Si bien el nombre de un participante, mencionado en el acta de una reunión, entra en el ámbito de los datos personales porque se revela la identidad de esta persona y porque el concepto de protección de datos personales es aplicable a estos datos, pertenezcan o no al ámbito de la intimidad, el SEPD recuerda que, en el marco de las actividades profesionales, la divulgación de un nombre por lo general no tiene relación con la intimidad. Deduce de ello que la Comisión no puede invocar el artículo 4, apartado 1, letra b), del Reglamento nº 1049/2001 para negarse a revelar el nombre de las personas de que se trata.

68 El SEPD concluye que, en todo caso, el artículo 4, apartado 1, letra b), del Reglamento nº 1049/2001 debe interpretarse en el sentido de que el derecho a negarse a la divulgación no es un derecho absoluto, sino que implica que la intimidad sufra un perjuicio grave o considerable, cuestión que debe apreciarse a la luz de las normas y principios de la protección de datos personales. No existe un derecho general de la persona afectada a oponerse a la divulgación. El interesado que se opone a la divulgación debe aportar una razón plausible, que explique por qué la divulgación podría ser perjudicial para él.

69 La Comisión alega que la pretensión de anulación de la Decisión impugnada carece de fundamento. Constata que, en el caso de autos, se trata de la interacción de dos derechos, a saber, el derecho de acceso del público a los documentos y el derecho a la protección de la intimidad y de los datos.

70 Por una parte, el derecho de acceso del público a los documentos conforme al Reglamento nº 1049/2001, en general, carece de restricciones, es automático y no depende del interés particular de una persona que solicita el acceso a un documento. La persona que presenta esta solicitud normalmente no está obligada a justificarla.

71 Por otra parte, los datos personales sólo pueden divulgarse de forma leal y legítima sobre la base de los principios fundamentales que rigen

el derecho a la intimidad y de las disposiciones específicas aplicables en materia de tratamiento de datos personales. La Comisión hace referencia al artículo 8 del CEDH, al artículo 286 CE y a los artículos 7 y 8 de la Carta. Las disposiciones del Reglamento nº 45/2001 establecen que la persona que solicita el acceso a los datos personales debe demostrar que la divulgación de estos datos es necesaria y garantizar a la Comisión que no perjudica a los intereses legítimos de la persona de que se trata.

En definitiva, se trata de distinguir entre dos derechos, y en el supuesto de que el ejercicio de uno pueda tener implicaciones para el otro, se debe analizar caso por caso con la finalidad de garantizar que la información sólo se divulga, de forma legal y legítima, sobre la base de los principios generales que rigen el más conocido derecho a la intimidad, conforme a las disposiciones específicas aplicables en materia de tratamiento de datos personales.

Contenido del derecho de acceso a los datos personales

Centrando, de nuevo, el análisis en el derecho de acceso en protección de datos, a continuación procedemos a analizar algunos aspectos de éste.

Tal y como indica la Ley, mediante el derecho de acceso el interesado podrá obtener información sobre:

1. los datos de carácter personal sometidos a tratamiento,
2. el origen de dichos datos, así como
3. las cesiones:
   a) realizadas o que
   b) se prevén hacer.

El derecho de acceso a los datos personales permite a cualquiera dirigirse al ente público, como responsable del tratamiento, a través del procedimiento establecido para tal efecto, con la finalidad de obtener información sobre el tratamiento de sus datos de carácter personal.

Es así que, incluso, aunque no se trataran los datos de una persona por un determinado ente público, ésta tiene derecho a preguntar al responsable del sistema de datos personales si los está tratando. Por tanto, el derecho de acceso permite al interesado saber si el responsable trata sus datos y, si fuera aplicable, proceder a rectificar, cancelar u oponerse al tratamiento de éstos.

Atención al ejercicio del derecho de acceso

En la práctica, un aspecto importante es cómo se va a atender al ejercicio del derecho de acceso por parte del responsable del tratamiento.

En este sentido, resulta importante recordar lo que establece el artículo 26 de la Ley, el cual indica que:

> *La respuesta a cualquiera de los derechos previstos en la presente ley, deberá ser proporcionada en forma legible e inteligible, pudiendo suministrase, a opción del interesado, por escrito o mediante consulta directa.*

De lo anterior, resulta claro que el responsable del tratamiento tendrá que proporcionar una respuesta al interesado sobre los datos que trate de éste, de forma legible e inteligible. Habrá que atender también a que éste tenga que proporcionarla por escrito o mediante consulta directa. En este sentido, el hecho de dar opción de elegir al interesado, en la práctica puede quedar limitado según la configuración del sistema de tratamiento, puesto que, por ejemplo, permitir el acceso físico al sistema donde se tratan los datos personales puede tener implicaciones desde el punto de vista de las medidas de seguridad.

Por último, reiteramos que entendemos que el ejercicio del derecho de acceso tiene que atenderse siempre, se traten o no datos del interesado por el responsable del tratamiento. Es decir, el responsable del tratamiento tendrá que responder en todo caso, trate o no datos de carácter personal de quien ejercita el derecho de acceso.

Artículo 28.- Procederá el derecho de rectificación de datos del interesado, en los sistemas de datos personales, cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos, siempre y cuando no resulte imposible o exija esfuerzos desproporcionados.

No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos.

Isabel Davara F. de Marcos

COMENTARIO

El artículo 28 trata sobre el derecho de rectificación. El primer párrafo del artículo 28 de la Ley comienza indicando que el derecho de rectificación procederá *"en los sistemas de datos personales, cuando tales datos resulten inexactos o incompletos, inadecuados o excesivos"*.

Por lo tanto, tal y como señala el artículo, procede el derecho de rectificación cuando los datos que sean tratados resulten:

- inexactos;
- incompletos;
- inadecuados, o
- excesivos.

Es decir, el derecho de rectificación procede cuando el tratamiento de datos no se ajuste a la Ley. Por tanto, debe entenderse que los datos tienen que cumplir con el principio de calidad y ser tratados conforme a las previsiones de la norma, ya que en caso contrario sería procedente el derecho de rectificación cuando los datos no estén actualizados y/o no respondan a la realidad.

Unido a lo anterior, los datos serán rectificados cuando resulten ser inexactos o incompletos. La rectificación tiene todo su sentido en estos dos supuestos, dado que los datos no responden a la realidad.

Sería oportuno señalar que la rectificación podrá llevarse a cabo bien por indicación del interesado, atendiendo a la solicitud del ejercicio del derecho, o de oficio, cuando el responsable del tratamiento tenga conocimiento de la inexactitud de los datos.

A diferencia de los casos anteriores, conforme a lo previsto en la Ley, el derecho de rectificación también procederá cuando los datos sean inadecuados o excesivos. No obstante, en estos supuestos debemos entender que procedería la cancelación de los datos por no ser necesarios o adecuados para el tratamiento que se lleva a cabo. Es decir, la rectificación se refiere a la corrección de datos que son inexactos o están incompletos, siendo, por tanto, inadecuados[95].

Por otro lado, el artículo termina diciendo que el derecho de rectificación procederá *"siempre y cuando no resulte imposible o exija esfuerzos desproporcionados"*. No cabe duda de que se trata de conceptos jurídicos indeterminados puesto que no se encuentran desarrollados (lo que, por otro lado, sería bastante difícil) ni en la Ley ni en los Lineamientos.

Es decir, la Ley no define qué ha de entenderse al decir que la rectificación "no resulte imposible" o "exija esfuerzos desproporcionados". Además de lo anterior, tampoco se incluye indicación expresa alguna en la Ley sobre si:

---

[95] Y así parece confirmarlo los Lineamientos al indicar en su apartado 46 que:

> *El derecho de rectificación es la prerrogativa del interesado a que se modifiquen los datos que resulten inexactos o incompletos, con respecto a la finalidad para la cual fueron obtenidos.*

1. El Instituto evaluará los casos en los que el responsable del tratamiento considere que la rectificación resulta imposible o exige esfuerzos desproporcionados, o

2. Será el responsable del tratamiento quien decidirá cuándo la rectificación resulta imposible o exige esfuerzos desproporcionados.

No obstante, resulta claro que dicha evaluación se realizaría al momento de resolver el recurso de revisión, valorando lo expresado por el ente público. Y en caso de que proceda la rectificación, ordenará que ésta se realice.

De cualquier modo, siempre hay que recalcar que, puesto que el objeto de la Ley es garantizar la protección de datos, el tratamiento de los datos por los entes públicos tendría que estructurarse de manera que permita el ejercicio de los derechos, en aras de garantizar la protección debida al titular de los datos. Al respecto, los criterios del Instituto se han encaminado a que el ente público determine si son "desproporcionados o no". El Instituto se ha pronunciado por establecer posibles parámetros, como en el caso de la digitalización de documentos.

Y así lo establece expresamente el artículo 5 de la Ley, cuando entre los principios del tratamiento de los datos de carácter personal resalta el de disponibilidad. Este principio supone que:

> *Los datos deben ser almacenados de modo que permitan el ejercicio de los derechos de acceso, rectificación, cancelación y oposición del interesado.*

En definitiva, la propia Ley señala que no debe haber más excepción al ejercicio de los derechos que las previstas por motivos específicos, sin que pueda entenderse como tal que la rectificación resulta imposible o exija esfuerzos desproporcionados, puesto que el principio de disponibilidad implica que los datos tengan que tratarse en el sistema

de datos, de manera que permitan el derecho de rectificación y el resto de derechos constitucional y legalmente reconocidos a los interesados en materia de protección de datos de carácter personal.

Solicitud y efecto de la rectificación de los datos

Resulta claro que la rectificación podrá ser solicitada por el titular de los datos así como por su representante legal o voluntario en los casos en los que proceda. La solicitud de rectificación será dirigida al responsable del tratamiento, que deberá atenderla y, de resultar procedente, efectuar la rectificación.

En relación con el procedimiento de rectificación, es necesario prestar atención a los Lineamientos a los que nos remitimos expresamente, si bien es posible apuntar aquí que en su solicitud el interesado tendrá que indicar los datos que resulten inexactos o incompletos y adjuntar la documentación justificativa de la rectificación.

Es decir, la rectificación de los datos requiere indicar los datos a rectificar, así como la rectificación que sea necesaria, aportando la documentación que permita al responsable del tratamiento comprobar cuáles son los datos exactos.

Unido a lo anterior, la rectificación seguirá en todo momento el procedimiento establecido para el ejercicio de los derechos, de manera que el interesado tendrá que identificarse ante el responsable del sistema de datos personales, salvo que el derecho se estuviera ejercitando mediante un representante legal, en cuyo caso éste tendrá que aportar la documentación necesaria.

Se trata, por tanto, de garantizar que los datos estén actualizados, cumpliendo así con el principio de calidad.

De otra manera, los datos no responderían con exactitud a la situación actual del interesado, o podrían dar lugar a supuestos de inexactitud de los datos por resultar éstos incompletos.

Excepciones al ejercicio del derecho de rectificación

Si bien la Ley se limita a indicar que la rectificación procede cuando los datos "*resulten inexactos o incompletos, inadecuados o excesivos, siempre y cuando no resulte imposible o exija esfuerzos desproporcionados*", y dejando a un lado lo ya indicado en relación con los conceptos jurídicos indeterminados, cabe señalar que el ejercicio del derecho de rectificación, como el resto, puede quedar sujeto a excepciones.

En este sentido, remitiéndonos nuevamente a los Lineamientos de la Ley, su apartado 50 indica expresamente que:

> *Los derechos de rectificación y cancelación no procederán en los supuestos en que así lo disponga una Ley.*

Por tanto, el ejercicio del derecho de rectificación queda sujeto a que no exista una norma con rango legal que lo excepcione. Y, de nuevo, la propia Ley que lo regula ya puede considerarse como una primera excepción, con cierto carácter general, al ejercicio del derecho, al indicar que éste procederá "*siempre y cuando no resulte imposible o exija esfuerzos desproporcionados.*"

Comunicación de la rectificación efectuada

Es necesario recordar que, si los datos personales que se rectifican hubieran sido cedidos a terceros, el cedente tiene que comunicar la rectificación efectuada a efectos de que el cesionario de la información, si todavía tratara los datos, proceda igualmente a su rectificación.

Insistimos en la necesidad de que el responsable del tratamiento establezca procedimientos internos adecuados que le permitan controlar en qué casos tiene que comunicar, y a quién, la rectificación de los datos.

Además de lo anterior, conforme al artículo 16 de la Ley, cabe recordar que:

> *El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente, respondiendo solidariamente por la inobservancia de las mismas.*

De manera que la no comunicación o la no rectificación de los datos, cuando proceda, podrían determinar la exigencia de responsabilidad tanto para el cedente como para el cesionario de los datos de carácter personal.

Datos personales y procedimiento administrativo o judicial

El segundo párrafo del artículo indica que:

> *No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos.*

Se trata de una previsión que como ya hemos visto también es recogida en otras normas sobre protección de datos internacionales y, en particular, en la española[96].

Al mismo tiempo, la previsión supone que la Ley se aplica también a los archivos administrativos y judiciales —aun cuando puedan tener también tratamientos y excepciones específicas—, de manera que los entes públicos y, en su caso, los órganos judiciales que pudieran estar

---

[96] En relación con el "derecho de rectificación o cancelación" el apartado 1, del artículo 15, del ya derogado Real Decreto 1332/1994 indicaba que:

> *No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo, aquéllos se considerarán exactos siempre que coincidan con éste.*

sujetos al ámbito competencial del Estado, tendrán que cumplir con la normativa sobre protección de datos de carácter personal, con sus especificidades, como ya mencionamos.

Además, en el caso de los archivos en posesión de la Administración Pública del Distrito Federal, Órgano Legislativo, Órgano Judicial y Organismos Públicos Autónomos del Distrito Federal, habrá que tener en consideración otra normativa específica aplicable, tal como la Ley de Archivos del Distrito Federal[97]

En particular, el artículo 61 de la citada Ley establece lo siguiente:

> *Con la finalidad de optimizar los Recursos de Información, garantizar la Transparencia, el Acceso a la Información, la Protección de Datos Personales y la eficacia Administrativa, se conformará la Red de Archivos del Distrito Federal como un conjunto de normas, mecanismos y dispositivos de intercambio y consulta telemática de información entre los entes públicos, de acuerdo con sus funciones y atribuciones.*

[97] Aprobada mediante Decreto por el que se expide ésta y que fue publicado en la Gaceta Oficial del Distrito Federal el 8 de octubre de 2008.

Artículo 29.- El interesado tendrá derecho a solicitar la cancelación de sus datos 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.

La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de los entes públicos, para la atención de las posibles 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.

La supresión de datos no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos.

Isabel Davara F. de Marcos

COMENTARIO

El análisis del derecho de cancelación de los datos requiere comenzar por el concepto mismo de cancelación y sus consecuencias y procedimiento a seguir: la cancelación dará lugar al bloqueo de los datos y posteriormente los datos serán suprimidos.

Bloqueo y cancelación de los datos

El artículo 2 de la LPDPDF define el concepto de bloqueo de los datos de la siguiente manera:

> *La identificación y reserva de datos personales con el fin de impedir su tratamiento.*

Esta definición es idéntica a la que recoge el derogado Reglamento de desarrollo[98] de la Ley de protección de datos española[99]. En el vigente Reglamento[100] ya se define bajo el concepto de cancelación de los datos.

Por su parte, los Lineamientos definen el bloqueo de los datos, en la fracción II de su apartado 3, como:

> *Identificación y conservación de datos personales con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo, legal o contractual, de prescripción de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación del sistema a que corresponda.*

Además, los Lineamientos también definen qué ha de entenderse por cancelación[101], indicando lo siguiente en la fracción III, de su apartado 3:

---

[98] El Real Decreto 1332/1994 definía el bloqueo de datos como "La identificación y reserva de los datos con el fin de impedir su tratamiento" (art. 1.1 R.D. 1332/1994). Este fue derogado por el Real Decreto 1720/2007, de 21 de diciembre, que define el bloqueo de la siguiente manera *"consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades."* Esta definición se incluye dentro del concepto de cancelación.

[99] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el Boletín Oficial del Estado número 298, de 14 de diciembre.

[100] *La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos. (art. 5.1.b).*

[101] En relación con la definición de cancelación de los datos en Derecho comparado es posible atender al Reglamento de desarrollo de la LOPD. En dicha norma, la cancelación es definida de la siguiente manera:

> *Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.* (art. 5.1.b)

La referencia resulta adecuada puesto que la norma reglamentaria que desarrolla la LOPD prevé el bloqueo de los datos como la consecuencia de su cancelación, quedando éstos únicamente a

Eliminación de determinados datos de un sistema de datos personales previo bloqueo de los mismos.

Por lo tanto, los Lineamientos establecen claramente que el bloqueo implica que los datos personales *"no podrán ser objeto de tratamiento"*, y que una vez transcurrido el plazo durante el que fueron bloqueados, éstos deberán ser borrados.

Es decir, los datos serán bloqueados durante el tiempo que establezca la norma o la relación contractual aplicable. Dicho tiempo será el que resulte aplicable para que el responsable del tratamiento atienda las responsabilidades surgidas durante el tratamiento de los datos. Y una vez que han transcurrido los plazos legal o contractualmente establecidos, los datos podrán ser suprimidos.

Durante el plazo en el que los datos estén bloqueados, tal y como indican los Lineamientos, *"no podrán ser objeto de tratamiento"*, lo que en la práctica significa que ni siquiera el responsable del sistema de datos pueda tener acceso a ellos, salvo que sea requerido por una autoridad competente que ordene el acceso a los datos por los motivos que fueran oportunos[102]. De no entenderse así, el acceso a los datos sería contrario a las propias disposiciones de la Ley, ya que ésta indica claramente que los datos "no podrán ser objeto de tratamiento".

Como apuntábamos, la definición del bloqueo resulta altamente importante, si no ya en sí misma, sí en su implicación en la práctica, pues el bloqueo de datos es una de las consecuencias de la cancelación de éstos.

---

disposición de las Administraciones Públicas, Jueces y Tribunales.

[102] En este sentido, véase lo dicho en la nota a pie anterior en cuanto a la normativa española en la materia.

En definitiva, y a modo de breve resumen, el bloqueo implica que los datos no puedan ser tratados durante los plazos establecidos legal o contractualmente, a efectos de responder a las responsabilidades surgidas del tratamiento de los mismos. Y una vez que dichos plazos transcurran se procederá a su cancelación en el sentido de que serán suprimidos.

Ejercicio del derecho de cancelación

El derecho de cancelación está previsto, conforme a lo dispuesto en la Ley, para los siguientes casos:

1. Cuando el tratamiento de los mismos no se ajuste a lo dispuesto en la Ley o en los lineamientos emitidos por el Instituto, o

2. Cuando hubiere ejercido el derecho de oposición y éste haya resultado procedente.

En primer lugar, procederá el ejercicio del derecho de cancelación cuando los datos resulten excesivos o inadecuados, ya que el artículo que comentamos se refiere expresamente a que el tratamiento de los datos *"no se ajuste a lo dispuesto en la Ley o en los Lineamientos"*[103].

En segundo lugar, la Ley prevé que el derecho de cancelación también procederá cuando el interesado haya ejercido el derecho de oposición y éste haya sido considerado procedente. Es decir, como consecuencia del ejercicio del derecho de oposición, si éste resultara procedente, los datos serán excluidos del tratamiento y, por tanto, cancelados.

Es importante recordar que el responsable del tratamiento, en caso de que hubiera cedido los datos a terceros, tiene obligación de comunicar la cancelación de éstos a dichos cesionarios. A su vez, el cesionario o cesionarios procederán a cancelar los datos en caso de que los estuvieran tratando.

---

[103] La referencia a los Lineamientos tiene que entenderse hecha a los Lineamientos de la Ley de Protección de Datos que comentaremos más adelante y a los que nos venimos refiriendo en todo momento.

Excepción al derecho de cancelación

Al igual que los otros derechos en protección de datos, el derecho de cancelación tampoco es un derecho absoluto.

Lo anterior supone que el derecho de cancelación se encuentre sujeto a límites, estableciéndose expresamente los siguientes:

1. Cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o

2. Cuando exista una obligación legal de conservar dichos datos.

La primera de las excepciones previstas se refiere al supuesto en el que la cancelación de los datos del interesado pudiera causar perjuicios a terceros en sus derechos o intereses legítimos. Dicha excepción se entiende en un sentido restringido, ya que tiene que tratarse de terceros que tengan algún derecho o interés legítimo en relación con el tratamiento de datos de carácter personal[104].

En definitiva, el derecho a la protección de datos tampoco es un derecho absoluto y, como cualquier otro derecho, también está sujeto a ciertos límites. Por tanto, el derecho a la protección de datos tiene que ser ponderado frente a otros derechos.

Y la segunda excepción que expresamente prevé la Ley es la previsión legal de conservar unos datos. Es decir, si existe una norma con rango legal que obliga a conservar los datos, éstos no podrán ser borrados o suprimidos e incluso podrían llegar a ser conservados para siempre[105].

---

[104] Es así que incluso se plantean los derechos o intereses legítimos de terceros en relación con un expediente administrativo o documento público que pueda contener datos de carácter personal.

[105] La excepción referida adquiere todo su sentido en el ámbito de las Administraciones Públicas. Piénsese por ejemplo en los datos académicos que serán necesarios para demostrar la titulación obtenida, o no, por una persona, incluso aunque ésta pretendiera suprimirlos. E igual sucede con

¿Qué supone el derecho de cancelación?

La cancelación dará lugar al bloqueo de los datos para, una vez transcurridos los plazos legalmente establecidos que permitirán depurar posibles responsabilidades surgidas del tratamiento de los datos, proceder a su borrado o supresión.

El derecho cancelación supone, en particular, que el interesado pueda solicitar al responsable del tratamiento la supresión de sus datos, lo cual es parte también del conocido como derecho al olvido.

La cancelación puede tener su fundamento en diversas razones, bien sea porque los datos resultan ser inadecuados o excesivos para la finalidad con la que se tratan, bien porque no cumplan con las disposiciones de la Ley y sus Lineamientos. Es decir, si, por ejemplo, los datos se han obtenido sin el consentimiento del interesado, el tratamiento resultaría ilícito y, por tanto, los datos personales tendrían que ser suprimidos.

Si bien la Ley prevé que el interesado pueda dirigirse al responsable del tratamiento para solicitar la rectificación de sus datos, cabe pensar que también el responsable del tratamiento podrá, cuando proceda, decidir la cancelación de los datos por sí mismo, ya que puede conocer que los datos son inadecuados o excesivos. Esto es, la cancelación también podrá, e incluso en algunos casos deberá, producirse de oficio.

Por último, tal y como veremos al comentar los Lineamientos, la cancelación también tiene que ser considerada cuando un sistema de datos personales es suprimido, puesto que dicha supresión puede dar lugar a la cancelación de los datos y, por tanto, a su borrado. Igualmente, la cancelación de los datos puede plantearse en aquellos casos en los que el responsable del tratamiento solicite a un tercero, el usuario, la prestación de servicios, de manera que al final de la relación contractual se le ordene devolver los datos al responsable del tratamiento o borrarlos, en cuyo caso habría que atender de nuevo al bloqueo de los datos.

---

los datos de salud en determinados casos en los que por razones incluso de seguridad pública sea necesario mantenerlos.

Artículo 30.- El interesado tendrá derecho a oponerse al tratamiento de los datos que le conciernan, 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. De actualizarse tal supuesto, el responsable del sistema de datos personales deberá cancelar los datos relativos al interesado.

Isabel Davara F. de Marcos

COMENTARIO

En relación con los derechos reconocidos a los interesados en la LPDPDF, el artículo 30 establece el derecho de oposición.

Significado del derecho de oposición

Para completar el denominado acrónimo de derechos ARCO, la Ley incluye el derecho de oposición, indicando que *"el interesado tendrá derecho a oponerse al tratamiento de datos que le conciernan"*.

Si bien la Ley no ofrece una definición del derecho de oposición, sí lo hacen sus Lineamientos, que indican en su apartado 51 lo siguiente:

> *El derecho de oposición es la prerrogativa del interesado a solicitar que no se lleve a cabo el tratamiento de sus datos personales para un fin determinado o se cese en el mismo, cuando no sea necesario otorgar el consentimiento para el tratamiento en términos de lo dispuesto por el artículo 16 de la Ley, como consecuencia de un motivo legítimo y fundado del interesado y siempre que una Ley no disponga lo contrario.*

Es decir, la oposición implica que el responsable del tratamiento no pueda tratar los datos o si ya se estuvieran tratando se cese en dicho tratamiento[106].

---

[106] En el Derecho comparado, nuevamente podemos recurrir a la Directiva 95/46/CE que en su artículo 7 establece lo siguiente:

En buena medida los Lineamientos clarifican lo dispuesto en la Ley ya que, tal y como veremos en el apartado siguiente, delimitan los requisitos para el ejercicio de este derecho.

Antes de entrar a analizar los requisitos para el ejercicio de los derechos, creemos oportuno citar alguna jurisprudencia internacional en la materia. En concreto, el Tribunal de Primera Instancia[107] de la Unión Europea ha señalado que:

Artículo 14
Derecho de oposición del interesado
Los Estados miembros reconocerán al interesado el derecho a:
a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;
b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.
Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b).

Es decir, la Directiva reconoce el derecho de oposición en una doble vertiente. Así, por un lado, frente al tratamiento en los siguientes casos conforme a lo dispuesto en el artículo 7:

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.

Y por otro lado el interesado puede oponerse al tratamiento de sus datos con fines de prospección comercial.

Por su parte, la LOPD, que transpone al ordenamiento jurídico español, contempla el derecho de oposición conforme a lo dispuesto en la Directiva 95/46/CE. Específicamente, por lo que se refiere a la oposición frente al tratamiento de los datos cuando éste no tiene fines de prospección comercial, la Ley indica lo siguiente en el apartado 4, de su artículo 6:

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

[107] Asunto T-194/04, ya citado.

> 109 En cuanto al derecho de oposición del interesado, el artículo 18 del Reglamento nº 45/2001 dispone que éste tiene derecho a oponerse en cualquier momento, por razones imperiosas y legítimas propias de su situación particular, a que los datos que le conciernen sean objeto de tratamiento, salvo en los casos contemplados, concretamente, en el artículo 5, letra b), de dicho Reglamento. En consecuencia, habida cuenta de que el tratamiento al que se refiere el Reglamento nº 1049/2001 constituye una obligación jurídica en el sentido del artículo 5, letra b), del Reglamento nº 45/2001, el interesado no dispone, en principio, de un derecho de oposición. Sin embargo, puesto que el artículo 4, apartado 1, letra b), del Reglamento nº 1049/2001 prevé una excepción a esta obligación jurídica, debe tenerse en cuenta, sobre esta base, la incidencia de la divulgación de los datos relativos al interesado.

Es decir, resulta claro que el derecho de oposición no procede siempre y que, por tanto, es necesario ponderarlo frente a otros derechos.

Requisitos para su ejercicio

La siguiente tabla compara el artículo 30 de la LPDPDF con los apartados 51 y 52 de sus Lineamientos, referidos al derecho de oposición.

LPDPDF	Lineamientos
El interesado tendrá derecho a oponerse al tratamiento de los datos que le conciernan, 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. De actualizarse tal supuesto, el responsable del sistema de datos personales deberá cancelar los datos relativos al interesado.	51. El derecho de oposición es la prerrogativa del interesado a solicitar **que no se lleve a cabo el tratamiento de sus datos personales *para un fin determinado* o se cese en el mismo**, ***cuando no sea necesario otorgar el consentimiento*** para el tratamiento en términos de lo dispuesto por el artículo 16 de la Ley, como consecuencia de ***un motivo legítimo y fundado del interesado y siempre que una Ley no disponga lo contrario***.

LPDPDF	Lineamientos
	52. En caso de que la oposición sea procedente, ***dará lugar a la cancelación del dato, previo bloqueo***, mientras transcurren los plazos previstos, a efecto de depurar las responsabilidades que correspondan.

A la vista de la tabla anterior, y centrando el análisis específicamente en los requisitos aplicables para el ejercicio del derecho de oposición, cabe señalar que es necesario que se cumpla con los siguientes:

1. *Cuando no sea necesario el consentimiento:* tal y como señala la Ley, el derecho de oposición resultará aplicable en aquellos supuestos en los que los datos se hubiesen recabado sin el consentimiento del interesado. Esta previsión es explicada en los Lineamientos, que indican que el derecho de oposición será aplicable cuando *"no sea necesario otorgar el consentimiento para el tratamiento",* incluyendo una referencia expresa al artículo 16 de la Ley en el que se regula el principio del consentimiento.

Por tanto, el primer requisito para poder aplicar el derecho de oposición es que los datos se traten o se vayan a tratar sin necesidad de obtener el consentimiento del interesado, es decir, en virtud de alguna de las excepciones a la regla general de necesidad de dicho consentimiento.

2. *Existencia de un motivo legítimo y fundado del interesado:* además de lo anterior, la Ley y los Lineamientos añaden el requisito de que el interesado tenga un motivo legítimo y fundado. Se trata de que exista una causa que permita al interesado oponerse al tratamiento de sus datos basado en dicho motivo legítimo.

Por lo tanto, el interesado tendrá que alegar y, en su caso, probar ante el responsable del tratamiento la existencia de un motivo legítimo y fundado para la exclusión del tratamiento de sus datos.

3. *Siempre que una Ley no disponga lo contrario:* por último, la Ley y los Lineamientos indican que el derecho de oposición se aplicará en aquellos casos en los que una Ley no disponga lo contrario.

Es decir, para que pueda aplicarse el derecho de oposición es necesario que la Ley no establezca la necesidad de tratar los datos, aun cuando no fuera necesario el consentimiento del interesado y pese a que existiera un motivo fundado y legítimo. Por tanto, siempre que el consentimiento del interesado no sea necesario, exista un motivo fundado y legítimo para solicitar la exclusión de sus datos del tratamiento, y una Ley no disponga la obligación del tratamiento, será aplicable el derecho de oposición conforme al procedimiento previsto con carácter general en la normativa sobre protección de datos.

Efectos del ejercicio del derecho de oposición

En caso de que proceda el ejercicio del derecho de oposición por el interesado al tratamiento de sus datos de carácter personal, la Ley prevé que éstos serán cancelados.

A lo anterior, los Lineamientos añaden que la cancelación dará lugar al bloqueo de los datos y que una vez que hayan transcurrido los plazos legalmente establecidos para responder de las responsabilidades en las que se pudieran haber incurrido, los datos serán cancelados.

Por tanto, el derecho de oposición tiene, conforme a la LPDPDF y sus Lineamientos, los mismos efectos que el derecho de cancelación de los datos. Además, es necesario recordar las excepciones al ejercicio de los derechos previstas en el artículo 12 de la Ley.

Artículo 31.- Si los datos rectificados o cancelados hubieran sido transmitidos previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan transmitido, en el caso de que se mantenga el tratamiento por este último, quién deberá también proceder a la rectificación o cancelación de los mismos.

Isabel Davara F. de Marcos

COMENTARIO

Este artículo establece que el responsable del tratamiento debe notificar la rectificación o cancelación de los datos a aquellos terceros a los que haya comunicado los datos para que, a su vez, procedan en el mismo sentido.

Se trata de un derecho del interesado y de una obligación para el cedente y el cesionario de los datos, puesto que ambos tendrán que tener un control sobre los datos que tratan, siendo capaces de identificar en todo momento cuáles son los datos que tienen que rectificar y, en su caso, cancelar.

Es decir, se busca garantizar que los datos estén actualizados y que dicha actualización se notifique también a quien le fueron comunicados, facilitando así que el interesado no tenga que dirigirse a todos y cada uno de los cesionarios de sus datos, puesto que, además, es el responsable del tratamiento quien los conoce.

Como decimos, el artículo impone una obligación tanto para el cedente de los datos como para el cesionario de éstos.

El cedente tiene que comunicar la rectificación o cancelación que haya llevado a cabo a aquellos terceros a los que haya cedido los datos. Es importante tener en consideración que sólo se comunicará a los cesionarios, de manera que nada de lo dicho en este artículo es aplicable al usuario, puesto que éste sólo trata datos por cuenta del responsable del tratamiento o sistema de datos personales.

La notificación implica que el cedente tenga que llevar un control de a quién comunica los datos, lo cual le permitirá responder al

ejercicio del derecho de acceso, en virtud de que éste también tiene que indicar a quién comunicó los datos. A su vez, el cesionario tiene que rectificar o cancelar los datos.

Obligación del responsable del tratamiento (cedente)

En primer lugar, el cedente será el ente público que cede los datos a un tercero, por los motivos que fuera y siempre que la cesión cumpla con los principios y requisitos de la Ley.

El artículo impone al responsable del tratamiento la obligación de notificar la rectificación o cancelación de los datos a quienes les hayan sido transmitidos. Se trata de una obligación lógica, puesto que es el responsable del tratamiento ante quien el interesado ejercitará sus derechos de rectificación y cancelación, según corresponda. Por tanto, es éste quien tiene que cumplir con la obligación de notificar la rectificación o cancelación, con la finalidad de garantizar que los datos estén actualizados en todo momento, incluso cuando hayan sido objeto de cesión.

Esta obligación muestra la importancia de la cesión de datos y cómo es necesario que el cedente atienda en todo momento a quien le está cediendo los datos, ya que, tal y como expresa la Ley, entre cedente y cesionario se establece un vínculo jurídico que llegará a suponer incluso la exigencia de responsabilidad solidaria.

Además de lo anterior, la notificación de la rectificación y/o cancelación de los datos, según corresponda, implica que el cedente tenga que establecer un procedimiento para comunicarlas. Sobra decir que es necesario que controle a quien le está cediendo los datos para posteriormente notificarle toda rectificación o cancelación de éstos.

Y también es importante notar que el hecho de que el cedente tenga la obligación de notificar la rectificación o cancelación de los datos supone que, a su vez, pueda ser cesionario de los datos. Por lo tanto,

el responsable del tratamiento sería parte de una cadena de cesiones de datos y, por tanto, tendría que establecer un procedimiento que le permita gestionar fácil y rápidamente cualesquiera notificaciones respecto de los datos de los que es responsable.

Obligación del cesionario

El cesionario, por el mero hecho de la cesión, se convierte también en responsable del tratamiento. El cesionario puede ser tanto un ente público como una empresa.

Como consecuencia de la notificación efectuada por el cedente, el cesionario, si aún estuviera tratando los datos, es decir, si no los hubiera cancelado o excluido del tratamiento por las razones que fuera, tendrá que proceder a rectificar o cancelarlos, según corresponda.

A la vista del último supuesto indicado en el apartado anterior, consideramos que aunque no tuviera ya los datos en su sistema o sistemas de información, el cesionario, si a su vez hubiera cedido los datos a terceros, tiene la obligación de comunicar las rectificaciones o cancelaciones de las que sea notificado. De otra manera, se rompería la cadena de notificaciones incumpliéndose el objetivo de la Ley, que es el de garantizar que los datos se encuentran en todo momento actualizados y cumplen con el principio de calidad.

Además, recordemos que la notificación sólo tiene que producirse en aquellos casos en los que se hubieran comunicado los datos. Es decir, si hubieran sido sometidos previamente a un procedimiento de disociación, la obligación quedará eximida puesto que no habrá ya datos que rectificar o cancelar.

Y, de nuevo, recordemos que la cancelación dará lugar al bloqueo de los datos durante los plazos legalmente establecidos para responder de cualquier responsabilidad surgida del tratamiento. Una vez extinguidos dichos plazos, los datos serán suprimidos.

Rectificación y/o cancelación de los datos

Un aspecto importante en el análisis de este artículo es el hecho de que el cesionario tendrá que proceder a rectificar o cancelar, según el caso, los datos que le sean indicados por el responsable del tratamiento que se los cedió.

Esto supone que el cesionario tenga que atender a los datos que está tratando, ya que podría llegar a darse el hecho de que haya obtenido más datos que los inicialmente cedidos o, incluso, que haya rectificado dichos datos al dirigirse al interesado. Y también, tal y como prevé el propio artículo, que hubiera cancelado ya los datos por los motivos que fuese.

Es decir, si el cesionario ya hubiera rectificado los datos tendrá que atender a las rectificaciones efectuadas, de manera que en dicho caso la rectificación de los datos no sería ya necesaria.

Supuestos específicos

a) Personas fallecidas

Una cuestión que podría plantearse y que no es tratada por la LPDPDF es la relativa a los datos de las personas fallecidas. Sería posible pensar y altamente probable que el cedente hubiera comunicado datos de una persona que posteriormente fallece. En dicho caso se plantearía si se aplica la normativa sobre protección de datos[108].

---

[108] Podemos acudir nuevamente a otros ordenamientos donde la cuestión ha sido ya tratada. En concreto, la Agencia Española de Protección de Datos, en su informe jurídico 0278/2009, trató está cuestión indicando al respecto lo siguiente:

> *[…] si el derecho fundamental a la protección de datos ha de ser considerado como el derecho del individuo a decidir sobre la posibilidad de que un tercero pueda conocer y tratar la información que le es propia, lo que se traduce en la prestación de su consentimiento al tratamiento, en el deber de ser informado y en el ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición, es evidente que dicho derecho desaparece por la muerte de las personas, por lo que los tratamientos de datos de personas fallecidas no podrían considerarse comprendidos dentro del ámbito de*

Es así que, con carácter general, cabe señalar que extinguida la personalidad jurídica no resulta aplicable la protección de datos, puesto que ya no hay interesado o titular de los datos.

b) Supuestos de concurrencia de competencias

Teniendo en consideración que la LPDPDF sólo se aplica a los entes públicos de su ámbito territorial, es decir, donde el Instituto de Acceso a la Información Pública del Distrito Federal ejerce sus competencias en cuanto a vigilar y hacer cumplir la Ley, es posible pensar también en algún supuesto de transferencia de competencias entre el Gobierno Federal y el Estatal.

Este tipo de situaciones se ha producido ya en otros ordenamientos jurídicos, con un reparto político no igual pero sí muy similar y, por tanto, extrapolable.

Siguiendo la experiencia acumulada por la Agencia Española de Protección de Datos en la interpretación de la normativa sobre protección de datos, es posible atender a otro de sus informes jurídicos[109].

En concreto, el informe se refiere a la aplicación de la normativa sobre protección de datos, atendiendo específicamente a quién ejerce competencias sobre el tratamiento de datos y distinguiendo entre el responsable y el usuario, donde se indica lo siguiente:

---

aplicación de la Ley Orgánica 15/1999.

Por tanto, tal y como a continuación concluye el citado informe:

las normas de protección de datos no son aplicables a los fallecidos que han dejado de ser titulares de este derecho como consecuencia del fallecimiento.

[109] Informe Jurídico 442/2006 sobre ficheros gestionados por el Servicio Público de Empleo Estatal, competencias transferidas y ejercicio de derechos de los afectados.

> *[La consultante] se encargaría, de conformidad con lo dispuesto en la Ley 56/2003, y en particular su artículo 13 g), así como con los Reales Decretos de transferencia, del mantenimiento y gestión de una base de datos centralizada, respecto de la que actuaría como encargado del tratamiento de las Comunidades competentes y "propietarias" de la información, que serían responsable del fichero.*

La referencia resulta relevante puesto que en el caso de entes públicos del Distrito Federal podría ocurrir que el responsable del tratamiento externalice parte o todo el tratamiento de datos y éste sea llevado a cabo por otro ente público del Estado o, en su caso, por una entidad o dependencia de la Administración Pública Federal, los cuales serían considerados como usuarios y no como cesionarios a los efectos del artículo que venimos comentando.

La distinción entre cedente, cesionario y usuario es importante a efectos de cumplir con las obligaciones establecidas por este artículo, puesto que tal y como indica el informe:

> *Ello implica que en la respuesta a las solicitudes de ejercicio de los derechos la consultante debería, en relación con las bases de datos de las que sea encargada del tratamiento, contar con la decisión de los órganos competentes de las Comunidades Autónomas, "propietarias" de las bases de datos, sin poder sin más atender a dichas solicitudes, en particular las vinculadas a los derechos de rectificación, cancelación y oposición.*
>
> *De este modo, sería posible la centralización en la consultante del ejercicio de los derechos, siempre y cuando así se acordase con los órganos autonómicos competentes, emitiéndose el correspondiente acuerdo, bien bilateral.*

Artículo 32.- La recepción y trámite de las solicitudes de acceso, rectificación, cancelación u oposición de datos personales que se formule a los entes públicos se sujetarán al procedimiento establecido en el presente capítulo.

Sin perjuicio de lo que dispongan otras leyes, sólo el interesado o su representante legal, previa acreditación de su identidad, podrán solicitar al ente público, a través de la oficina de información pública competente, que le permita el acceso, rectificación, cancelación o haga efectivo su derecho de oposición, respecto de los datos personales que le conciernan y que obren en un sistema de datos personales en posesión del ente público.

La oficina de información pública del ente público deberá notificar al solicitante en el domicilio o medio electrónico señalado para tales efectos, en un plazo máximo de quince días hábiles contados desde la presentación de la solicitud, la determinación adoptada en relación con su solicitud, a efecto que, de resultar procedente, se haga efectiva la misma dentro de los diez días hábiles siguientes a la fecha de la citada notificación.

El plazo de quince días, referido en el párrafo anterior, podrá ser ampliado una única vez, por un periodo igual, siempre y cuando así lo justifiquen las circunstancias del caso.

Si al ser presentada la solicitud no es precisa o no contiene todos los datos requeridos, en ese momento el Ente Público, en caso de ser solicitud verbal, deberá ayudar al solicitante a subsanar las deficiencias. Si los detalles proporcionados por el solicitante no bastan para localizar los datos personales o son erróneos, la oficina de información pública del ente público podrá prevenir, por una sola vez y, dentro de los cinco días hábiles siguientes a la presentación de la solicitud, para que aclare o complete su solicitud, apercibido de que de no desahogar la prevención se tendrá por no presentada la solicitud. Este requerimiento interrumpe los plazos establecidos en los dos párrafos anteriores.

En el supuesto que los datos personales a que se refiere la solicitud obren en los sistemas de datos personales del ente público y éste considere improcedente la solicitud de acceso, rectificación, cancelación u oposición, se deberá emitir una resolución fundada y motivada al respecto. Dicha respuesta deberá estar firmada por el titular de la oficina de información pública y por el responsable del sistema de datos personales del ente público.

Cuando los datos personales respecto de los cuales se ejerciten los derechos de acceso, rectificación, cancelación u oposición, no sean localizados en los sistemas de datos del ente público, se hará del conocimiento del interesado a través de acta circunstanciada, en la que se indiquen los sistemas de datos personales en los que se realizó la búsqueda. Dicha acta deberá estar firmada por un representante del órgano de control interno, el titular de la oficina de información pública y el responsable del sistema de datos personales del ente público.

Miguel Carbonell

COMENTARIO

El artículo 32 de la Ley de Protección de Datos Personales para el Distrito Federal detalla las líneas generales del procedimiento que se deben seguir para recibir y tramitar las solicitudes de acceso, rectificación, cancelación u oposición de datos personales, promovidas ante los órganos públicos obligados por la citada Ley.

Vamos a intentar describir, a grandes rasgos, la forma en que se va estructurando dicho procedimiento, a través de un sistema de reglas que ordenen lo dispuesto por el artículo 32 que estamos analizando:

1. Por lo que respecta a la legitimación para solicitar el acceso, la rectificación, la cancelación o ejercer la oposición en materia de datos personales, el artículo 32 señala que es una legitimación "cerrada", en tanto que la tiene solamente el "interesado" (es decir, como regla general, el titular de los datos personales) o su representante legal.

2. El área competente para recibir las solicitudes en cuestión es la oficina de información pública del ente u organismos bajo cuya posesión estén los datos personales.

3. El plazo para notificar al interesado el resultado de su solicitud es de 15 días hábiles, los cuales comienzan a contarse desde la presentación de la solicitud.

4. Si el interesado está conforme con la determinación de la autoridad, la misma se deberá hacer efectiva dentro de los siguientes 10 días, contados a partir de que se haya notificado la resolución.

5. El plazo original de 15 días hábiles puede ser ampliado, por una única vez, cuando existan circunstancias que así lo ameriten. La carga de la prueba sobre la existencia de dichas circunstancias y sobre su efecto en el plazo señalado para emitir la resolución está a cargo de la autoridad siempre.

6. La autoridad que reciba una solicitud relacionada con datos personales tiene el deber de suplir las deficiencias o carencias que pudiera contener dicha solicitud, a efectos de ubicar de la mejor forma posible la información que se le está pidiendo. Si mediante dicha suplencia no es posible contar con los

detalles necesarios para saber lo que se está pidiendo o bien para encontrar la información, la autoridad podrá prevenir al solicitante, a efecto de que supla las carencias de su solicitud en un plazo de 5 días hábiles a más tardar. De no hacerlo así la solicitud se tendrá por no interpuesta. Cuando se emite la prevención dejan de correr los plazos ordinarios para resolver la solicitud.

7. Puede darse el caso de que la solicitud presentada se considere improcedente, en cuyo caso el titular de la oficina de información pública del órgano en cuestión deberá expresarlo así mediante resolución fundada y motivada. En este supuesto el órgano tiene en su poder y ha identificado los datos que se solicitan, pero se encuentra normativamente imposibilitado para entregárselos al solicitante. La resolución señalada deberá estar firmada por el titular de la oficina de información pública y por el responsable del sistema de datos personales del ente público.

8. El último supuesto contemplado por el artículo 32 se produce cuando los datos no son localizados en las bases de datos del órgano ante el que se presenta la solicitud. En ese caso la inexistencia se deberá hacer del conocimiento del solicitante mediante un acta circunstanciada. El acta debe ser firmada por un representante del órgano interno de control, por el titular de la oficina de información pública y por el responsable del sistema de datos personales del ente en cuestión. Se deberán señalar las bases de datos que fueron examinadas para determinar la inexistencia.

Artículo 33.- La solicitud de acceso, rectificación, cancelación u oposición de datos personales, se deberá presentar ante la oficina de información pública del ente público que el interesado considere que está procesando información de su persona. El procedimiento de acceso, rectificación, cancelación u oposición de datos personales, iniciará con la presentación de una solicitud en cualquiera de las siguientes modalidades:

I. Por escrito material, será la presentada personalmente por el interesado o su representante legal, en la oficina de información pública, o bien, a través de correo ordinario, correo certificado o servicio de mensajería;

II. En forma verbal, será la que realiza el interesado o su representante legal directamente en la oficina de información pública, de manera oral y directa, la cual deberá ser capturada por el responsable de la oficina en el formato respectivo;

III. Por correo electrónico, será la que realiza el interesado a través de una dirección electrónica y sea enviada a la dirección de correo electrónico asignada a la oficina de información pública del ente público;

IV. Por el sistema electrónico que el Instituto establezca para tal efecto, y

V. Por vía telefónica, en términos de los lineamientos que expida el Instituto.

Issa Luna Pla

COMENTARIO

El artículo 33 de la Ley de Protección de Datos Personales para el Distrito Federal establece los medios por los cuales el titular de los datos personales puede presentar la solicitud, así como la unidad administrativa ante la cual se ejercitarán los derechos ARCO.

El primer elemento que comprende el artículo citado es que las personas que deseen ejercitar su derecho fundamental deberán presentar su escrito ante la oficina de información pública, la cual es una figura heredada de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, y que es definida por la Ley de la materia de datos personales como:

> … La unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los entes públicos, a cuya tutela estará el trámite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida el Instituto…[110]

Es decir, es una unidad que cuenta con un cierto nivel de especialización en el tema y sirve de vínculo entre el ente público y el titular de los datos personales; además de que bajo su tutela se encuentra el desahogo del ejercicio de cualquiera de los Derechos ARCO.

Ahora bien, otro de los elementos que conforman el artículo en comento deriva de una presunción por parte del titular de los datos personales de que el ente público ante el cual dirige su "escrito" se encuentra procesando sus datos; lo que significa que, la simple creencia por parte de una persona de que el ente público cuenta con un sistema de datos personales en donde, posiblemente, se encuentra su información, lo habilita para presentar un "escrito" por el que se ejercita cualquiera de sus derechos ARCO.

Otro de los requisitos "formales" para la procedencia del ejercicio de los derechos ARCO es la forma o modalidad en la que se puede presentar la solicitud; ésta pueden ser:

---

[110] Artículo 2 de la Ley.

- Por escrito material
- En forma verbal
- Por correo electrónico
- Por INFOMEX[111]
- Por teléfono

El primer componente señalado implica todo aquel medio en el que estén representadas ideas o palabras, que sea legible o comprensible por distinta persona al que lo haya redactado, es decir, toda carta, documento o cualquier papel manuscrito, mecanografiado o impreso. Es necesario apuntar que, a pesar de se trata de un escrito libre, es necesario que reúna algunos requisitos de forma, los cuales se encuentran plasmados en el artículo 34 de la Ley en comento, que señala que todo escrito por el que se promueva el ejercicio de uno de los derechos ARCO, deberá contener:

I. Nombre del ente público a quien se dirija;
II. Nombre completo del interesado, en su caso, el de su representante legal;
III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;
IV. Cualquier otro elemento que facilite su localización;
V. El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones, y

---

[111] Los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal lo define, en el segundo párrafo del lineamiento uno, como "…el sistema electrónico mediante el cual las personas podrán presentar sus solicitudes de acceso a la información pública y de acceso, rectificación, cancelación y oposición de datos personales y es el sistema único para el registro y captura de todas las solicitudes recibidas por los entes públicos a través de los medios señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y la Ley de Protección de Datos Personales para el Distrito Federal, así como para la recepción de los recursos de revisión interpuestos a través del propio sistema…"

VI. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas

Ahora bien, el escrito en comento debe ser presentado de manera personal en la oficina de información pública del ente público ante el cual se ejercita el derecho; sin embargo, existe la posibilidad de que la presentación se realice por medio de un representante legal, es decir, la Ley de Protección de Datos Personales para el Distrito Federal abre la posibilidad de que el titular de los datos personales ejercite los derechos ARCO por medio de un mecanismo de sustitución de su voluntad, lo que implica que un tercero suple la imposibilidad jurídica de actuación de éste, por lo que el representante es el único con la posibilidad de actuar en su nombre. Es necesario resaltar que en este artículo en comento, a diferencia de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal, se encuentra implícito que quien promueve a nombre propio o por medio de un representante legal, debe tener un interés legítimo, esto es, que debe ser el propietario de los datos personales, en virtud de que esta misma Ley y la Ley de Transparencia imposibilitan obtener un resultado del ejercicio de los derechos ARCO si se tratase de una persona distinta.

Como se señaló en el párrafo anterior, el escrito debe ser presentado ante la oficina de información pública; sin embargo, la última parte de la fracción I del artículo en comento, establece la posibilidad de que dicho escrito sea remitido por medio del sistema o servicio postal, entendiéndose como tal, la recogida, admisión, clasificación, tratamiento, curso, transporte, distribución y entrega al remitente; los tipos de servicios que puede optar el titular de los datos personales o su representante legal son el correo ordinario, certificado (es necesario resaltar que este tipo de envío debe ser con acuse de recibido, a fin de que pueda tener una validez jurídica) o por servicio de mensajería especializada.

El segundo elemento, implica la posibilidad de que el titular de los datos personales formule su solicitud de manera verbal, obligando

a la persona que se encuentre al frente de la oficina de información pública a transcribir dicha solicitud verbal en un formato específico, esto en los términos del numeral 3, fracción XXVII, de los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal. Es necesario apuntar que es una obligación de ese servidor público registrar la solicitud verbal en el módulo manual del INFOMEX y, en el supuesto de que el titular o su representante legal permanezcan en las instalaciones de esa unidad administrativa, se le debe otorgar una copia del acuse que genera el sistema electrónico señalado o, en su defecto, deberá remitirlo al domicilio o medio señalado para recibir notificaciones, en un plazo no mayor a los tres días hábiles.[112] Este mismo procedimiento deberá observar el ente público, si el escrito fuere presentado por medio del correo electrónico, y deberá entenderse, salvo prueba en contrario, que dicho medio electrónico será ante el cual se deberán realizar las notificaciones que se generen por motivo del procedimiento que se derive del ejercicio de los derechos ARCO.

Otro de los elementos que se ha apuntado, es el relativo a la posibilidad de presentar el escrito por medio del "… sistema electrónico que el Instituto [Instituto de Acceso a la Información Pública del Distrito Federal] establezca para tal efecto…"[113]. Dicho sistema es el denominado comúnmente como INFOMEX-DF, el cual es la herramienta tecnológica por el que el titular de los datos personales o su represente legal podrá presentar su solicitud de acceso, rectificación, cancelación u oposición de datos personales.

El último elemento clave, implica que la solicitud del ejercicio de cualquiera de los derechos ARCO sea presentada por vía telefónica, es decir, por conducto de las operadoras del TEL-INFODF, lo cual involucra de manera implícita una solicitud verbal y que debe

---

[112] Lineamiento 19, fracción II de los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal.

[113] Fracción IV del artículo 33 de la Ley de Protección de Datos Personales para el Distrito Federal.

observarse, en términos generales, lo señalado en párrafos anteriores. Sin embargo, tiene algunas peculiaridades específicas que lo diferencian de los primeros pasos del procedimiento de una solicitud verbal; en términos de los Lineamientos que regirán la operación del Centro de Atención Telefónica del Instituto de Acceso a la Información Pública, estas diferencias serían a groso modo:

- La solicitud no es presentada directamente ante la oficina de información pública.
- El operador[114] se encuentra obligado a proporcionar *no sólo el folio del acuse que es generado por el INFOMEX*, sino que también tiene que proporcionar el *número de atención telefónica*.
- El acuse generado por el INFOMEX puede ser recogido directamente en las instalaciones del Instituto de Acceso a la Información Pública del Distrito Federal, o bien, y a solicitud expresa del titular o su representante legal, ser remitido por correo electrónico.

[114] El operador, es defino por el lineamiento 2, fracción I, de los Lineamientos que regirán la operación del Centro de Atención Telefónica del Instituto de Acceso a la Información Pública, como: Persona capacitada para registrar las solicitudes, orientar y responder las consultas telefónicas que se formulen al Centro de Atención Telefónica.

Artículo 34.- La solicitud de acceso, rectificación, cancelación u oposición de los datos personales deberá contener, cuando menos, los requisitos siguientes:

I. Nombre del ente público a quien se dirija;

II. Nombre completo del interesado, en su caso, el de su representante legal;

III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;

IV. Cualquier otro elemento que facilite su localización;

V. El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones, y

VI. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas.

En el caso de solicitudes de acceso a datos personales, el interesado, o en su caso, su representante legal deberá acreditar su identidad y personalidad al momento de la entrega de la información. Asimismo, deberá acreditarse la identidad antes de que el ente público proceda a la rectificación o cancelación.

En el caso de solicitudes de rectificación de datos personales, el interesado deberá indicar el dato que es erróneo y la corrección que debe realizarse y acompañar la documentación probatoria que sustente su petición, salvo que la misma dependa exclusivamente del consentimiento del interesado y ésta sea procedente.

En el caso de solicitudes de cancelación de datos personales, el interesado deberá señalar las razones por las cuales considera que

el tratamiento de los datos no se ajusta a lo dispuesto en la Ley, o en su caso, acreditar la procedencia del ejercicio de su derecho de oposición.

Los medios por los cuales el solicitante podrá recibir notificaciones y acuerdos de trámite serán: correo electrónico, notificación personal en su domicilio o en la propia oficina de información pública que corresponda. En el caso de que el solicitante no señale domicilio o algún medio de los autorizados por esta ley para oír y recibir notificaciones, la prevención se notificará por lista que se fije en los estrados de la Oficina de Información Pública del Ente Público que corresponda.

El único medio por el cual el interesado podrá recibir la información referente a los datos personales será la oficina de información pública, y sin mayor formalidad que la de acreditar su identidad y cubrir los costos de conformidad con la presente Ley y el Código Financiero del Distrito Federal.

El Instituto y los entes públicos contarán con la infraestructura y los medios tecnológicos necesarios para garantizar el efectivo acceso a la información de las personas con discapacidad.

Miguel Carbonell

COMENTARIO

El artículo 34 de la Ley en comento se refiere a las formalidades que deberán observar las solicitudes de acceso, rectificación, cancelación u oposición de datos personales.

Las seis fracciones del párrafo primero del artículo 34 se refieren a los requisitos comunes para los actos jurídicos señalados, mientras que el párrafo segundo regula requisitos formales diferenciados según el acto de que se trate. El párrafo tercero trata lo relativo a la manera en que se podrá recibir la información por parte de los interesados y el párrafo cuarto aborda el tema de la tecnología apropiada para las personas con discapacidad. Veamos con algún detalle todos estos aspectos.

El primer requisito se refiere al nombre del ente público al que se dirige la solicitud. Este requisito es desde luego razonable en la medida en que intenta ofrecer certeza a las autoridades correspondientes, respecto de la voluntad del peticionario para dirigirse a ella y no a otra diferente.

El segundo requisito se refiere al nombre del peticionario o del representante legal (se requiere representante legal, por ejemplo, en el caso de los menores de edad o de las personas sujetas a tutela o curatela). En esto, el régimen jurídico de los datos personales ofrece una diferencia sustancial respecto de las reglas constitucionalmente establecidas para el derecho de acceso a la información pública gubernamental. Mientras por el lado del derecho de acceso ningún órgano puede exigir que se identifique el peticionario (y tampoco que acredite algún tipo de interés jurídico para solicitar información pública)[115], por el de datos personales opera precisamente la regla contraria: no se pueden dar a conocer a nadie, salvo al propio titular o bien a un órgano público en los casos establecidos expresamente por la ley. De ahí que la legislación deba prever un sistema de legitimación activa riguroso, que permita a la autoridad, en cuya posesión estén los datos, protegerlos adecuadamente. Ese es el propósito, razonable y pertinente, del segundo requisito establecido por el párrafo primero del artículo 34.

---

[115] Cabe recordar que la fracción III del párrafo segundo del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos establece con claridad que cuando se solicite cualquier información pública no se tendrá que acreditar interés alguno o justificar su utilización. Debemos entender la exigencia de dicha fracción en un sentido amplio; es decir, para que la autoridad esté obligada a contestar basta con que le llegue la solicitud. No podrá exigir ningún otro requisito para dar respuesta a una petición informativa. Es importante señalar que la ausencia del requisito de acreditar la personalidad jurídica o el interés para pedir la información es congruente con el carácter de derecho fundamental, y por tanto universal, que tiene el derecho a la información.

La no exigencia de algún requisito, más que el de ser persona y solicitar la información, permite alejarse de fenómenos inhibitorios, los cuales podrían darse en el caso de solicitudes de información sobre temas delicados como por ejemplo los relacionados con la seguridad pública o con presuntos actos de corrupción. Si en estos casos le pedimos al solicitante que proporcione copia de su identificación oficial y un domicilio para recibir notificaciones, lo más seguro es que le generaremos un cierto temor en el ejercicio de su derecho fundamental a la información. Con ello se producirían efectos indeseables que minarían en la práctica la supervisión ciudadana del quehacer gubernamental, lo cual también es uno de los propósitos de la transparencia.

Por supuesto, el razonamiento en el caso de los datos personales es completamente distinto.

El tercer requisito se refiere a la descripción clara y precisa de los datos personales sobre los que se ejerza la solicitud. Esto se justifica en virtud de dos circunstancias: por un lado, le permite a la autoridad dirigir su búsqueda de forma más exacta, con lo cual se evitan pérdidas de tiempo y se gana en eficacia institucional; por otra parte, dirige a la autoridad hacia lo realmente pedido, evitando de esa forma que los funcionarios busquen en bases de datos que no sean pertinentes para determinada solicitud, con lo cual se fortalece la mayor reserva posible de los datos, que corren menos riesgos en la medida en que no sean cotidianamente manipulados por funcionarios.

La fracción cuarta prevé un requisito adicional, que resulta complementario en buena medida del anterior. Se refiere a la necesidad de que el peticionario aporte cualesquiera elementos que permitan facilitar la localización de los datos sobre los que se ejerce determinada solicitud. Al tratarse de un requisito ciertamente amplio (pues los "elementos" citados por la Ley pueden ser de muy variado tipo), su cumplimiento deberá ser casi siempre presumido por parte de la autoridad, ya que de otra manera se puede crear una barrera importante para el ejercicio del derecho de protección de datos personales, si la autoridad se niega a darle curso a una solicitud argumentando que no se cumple con lo señalado en la fracción IV.

De cualquier forma, la interpretación correcta es que se trata de un requisito indicativo, pero no limitativo. Se debe cumplir en la mayor medida posible, sin que la autoridad pueda construir sobre su base una barrera para el legítimo ejercicio del derecho de protección de datos personales.

El quinto requisito se refiere al domicilio del solicitante, el cual puede ser físico, en cuyo caso deberá encontrarse dentro del Distrito Federal, o bien electrónico, que le servirá al solicitante para recibir notificaciones. El señalar una dirección electrónica para recibir notificaciones, como es lógico, no supone que se pueda dejar de cumplir con la acreditación de la personalidad del solicitante, que es el primer requisito a observar por parte de toda solicitud.

Finalmente, la fracción VI del artículo 34 establece que se puede, si así lo estima el solicitante (dado que es un requisito de cumplimiento voluntario), señalar la modalidad en la que se prefiere que se otorgue el acceso a los datos personales. Además, esta fracción señala las tres posibles modalidades en que dicho acceso se puede realizar: la consulta directa, las copias simples o las copias certificadas.

En los párrafos siguientes (dos al cuatro) se indican algunos requisitos específicos de cada una de las modalidades que puede tomar una solicitud relativa a los datos personales: acceso, rectificación, cancelación u oposición.

Respecto de las solicitudes de acceso a datos personales, del párrafo segundo del artículo 34, se desprende que el interesado o su representante legal deberá acreditar su personalidad tanto al momento de presentar la solicitud como al momento de la entrega. Lo mismo sucede con las solicitudes de cancelación o rectificación.

Ahora bien, respecto de las solicitudes de rectificación, el párrafo tercero del referido artículo añade el requisito de que el solicitante indique el dato que considera erróneo y el sentido en que debe darse la corrección; en su caso, debe acompañar la documentación probatoria que sustente su petición, a menos que baste con su simple consentimiento.

Sobre las solicitudes de cancelación de datos personales, este artículo, en su párrafo cuarto, añade el requisito de que el interesado señale las razones por las que estima que el tratamiento de un cierto dato personal (o de un conjunto de ellos) no se ajusta a lo que señala la Ley. También puede dirigir dichas razones a oponerse al tratamiento dado por el órgano poseedor del dato en cuestión.

El párrafo quinto trata de los medios por los cuales se pueden recibir notificaciones, reiterando (aunque con un alcance más amplio) lo que ya señalaba la fracción V del mismo precepto legal. De acuerdo con este párrafo, los medios para recibir notificaciones y acuerdos

de trámite son el correo electrónico, la notificación personal en domicilio o bien a través de la oficina de información pública correspondiente.

El párrafo sexto del artículo en comento señala que solamente a través de la oficina de información pública del órgano correspondiente se podrá recibir información relativa a datos personales. Esta disposición es importante porque contribuye a ofrecer seguridad jurídica respecto, entre otras cuestiones, a la autoridad responsable de recibir y procesar las solicitudes, y a la autoridad encargada de la entrega de la información a los peticionarios.

Esta disposición contribuye positivamente en la determinación de las responsabilidades por manejos indebidos de ciertos datos personales, sin que tales responsabilidades se puedan diluir al interior de un determinado órgano público. Al haber una oficina legalmente señalada como responsable, se centralizan las funciones y tareas en beneficio de los solicitantes, y se fortalece el sistema de exigencia de responsabilidades y rendición de cuentas. Por otra parte, se facilita la tarea de capacitación, al permitir enfocarla hacia algunos funcionarios.

El mismo párrafo señala que para efecto de recibir información se deberá acreditar la personalidad (tema en el que no sobran las reiteraciones, y al que ya se había referido el párrafo segundo de este artículo) y cubrir los costos de acuerdo con lo señalado por el Código Financiero. La Ley aborda el tema de los costos en el artículo 37, sobre el que se hace un análisis unas páginas más adelante.

El último párrafo del artículo 34 dispone que tanto el InfoDF como los entes públicos obligados por la Ley deben contar con la infraestructura y los medios tecnológicos necesarios para garantizar el efectivo acceso a la información de las personas con discapacidad. Este mandato es importante porque contribuye a hacer efectivo el "acceso a la información" en la modalidad de la protección de los

datos personales (ambos conceptos correctamente vinculados en la fracción II del párrafo segundo del artículo 6 constitucional)[116].

Ahora bien, en virtud de que el concepto de "persona con discapacidad" abarca un amplio espectro de posibilidades, la obligación legislativa señalada por el artículo 34 se tendrá que plasmar en una serie de medidas de política pública igualmente diversa. Por ejemplo, se requerirá el auxilio de rampas para permitir el acceso de personas con discapacidad motriz; el auxilio de documentos en braille para personas con discapacidad visual; el auxilio de intérpretes de lenguaje de señas para personas con discapacidad auditiva y así por el estilo. Aunque dichas medidas pueden ser costosas y quizá puedan no ser de carácter permanente, se justifican para asegurar una accesibilidad universal que permita ejercer en la práctica, con la mayor eficacia posible, el derecho a la protección de datos personales. Si no se permite dicho ejercicio universal, se estaría violando el derecho a no ser discriminado por motivos de discapacidad, cuestión que está expresamente prevista en el párrafo tercero del artículo 1 constitucional[117].

---

[116] Uno de los principios generalmente reconocidos respecto del derecho de acceso a la información pública es el de la accesibilidad, que implica el deber de las autoridades para tomar todas las medidas oportunas y pertinentes a fin de asegurar que cualquier persona pueda tener acceso efectivo y sencillo a la información pública.

[117] El tema se ha estudiado en Carbonell, Miguel, *Los derechos fundamentales en México*, 3ª edición, México, Porrúa, UNAM, CNDH, 2009, pp. 183 y siguientes.

Artículo 35.- Presentada la solicitud de acceso, rectificación, cancelación u oposición de datos personales, la oficina de información pública del ente público, observará el siguiente procedimiento:

I. Procederá a la recepción y registro de la solicitud y devolverá al interesado, una copia de la solicitud registrada, que servirá de acuse de recibo, en la que deberá aparecer sello institucional, la hora y la fecha del registro;

II. Registrada la solicitud, se verificará si cumple con los requisitos establecidos por el artículo anterior, de no ser así se prevendrá al interesado, tal y como lo señala el artículo 32 de la presente Ley. De cumplir con los requisitos se turnará a la unidad administrativa que corresponda para que proceda a la localización de la información solicitada, a fin de emitir la respuesta que corresponda;

III. La unidad administrativa informará a la oficina de información pública de la existencia de la información solicitada. En caso de inexistencia, se procederá de conformidad con lo previsto por el artículo 32 para que la oficina de información pública a su vez realice una nueva búsqueda en otra área o unidad administrativa.

En la respuesta, la oficina de información pública, señalará el costo que por concepto de reproducción deberá pagar el solicitante en los términos del Código Financiero del Distrito Federal;

IV. La oficina de información pública, notificará en el domicilio o a través del medio señalado para tal efecto, la existencia de una respuesta para que el interesado o su representante legal pasen a recogerla a la oficina de información pública;

V. En cualquier caso, la entrega en soporte impreso o el acceso electrónico directo a la información solicitada se realizará de forma personal al interesado o a su representante legal; y

VI. Previa exhibición del original del documento con el que acreditó su identidad el interesado o su representante legal, se hará entrega de la información requerida.

En caso de que el ente público determine que es procedente la rectificación o cancelación de los datos personales, deberá notificar al interesado la procedencia de su petición, para que, dentro de los 10 días hábiles siguientes, el interesado o su representante legal acrediten fehacientemente su identidad ante la oficina de información pública y se proceda a la rectificación o cancelación de los datos personales.

Issa Luna Pla

COMENTARIO

El artículo 35 de la Ley de Protección de Datos Personales para el Distrito Federal establece el procedimiento que deben observar las oficinas de información pública al recibir una solicitud de acceso, rectificación, cancelación u oposición de datos personales (ARCO). La fracción primera del procedimiento se encuentra conformada por dos momentos procesales: el primero de ellos establece la obligación de la oficina de información pública de recibir y registrar el "escrito" por el que se ejercite alguno de los derechos ARCO. En el caso de que las solicitudes sean presentadas en las instalaciones de esa unidad administrativa, el servidor público deberá proceder a capturar la solicitud (física o verbal) en el módulo manual[118] de

[118] En términos del 3, fracción XIX, de los Lineamientos para la gestión de la solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal, el módulo manual es "…un componente del sistema que permite a la Oficina de Información Pública del ente público el registro y la captura de las solicitudes recibidas por escrito material, correo electrónico o de manera verbal, y que inscribe dentro del sistema las diversas respuestas y notificaciones que se le pueden emitir al solicitante…"

INFOMEX, dentro del mismo día que la hubiere recibido[119], salvo que se hubiere presentado después de las 15:00 hrs. El segundo momento procesal referido, consiste en la obligación del ente público de entregar una copia de la solicitud registrada como acuse de recibo. Para que esta copia tenga validez y sirva como prueba de la presentación de la solicitud, deberá contar con el sello del ente público, la fecha y hora en que fue recibida y, en caso de que tuviera anexos, deberá asentarse el o los anexos. Es necesario destacar que la entrega del acuse tiene como finalidad generar certeza jurídica al solicitante en los términos de la Tesis VI,2o.C.507.C, que señala:

> Registro No. 174562
>
> Localización:
>
> Novena Época
>
> Instancia: Tribunales Colegiados de Circuito
>
> Fuente: Semanario Judicial de la Federación y su Gaceta XXIV, Agosto de 2006 Página: 2135
>
> Tesis: VI.2o.C.507 C
>
> Tesis Aislada
>
> Materia(s): Civil
>
> ACUSE DE RECIBO. SI NO EXISTE CONGRUENCIA ENTRE LA RAZÓN QUE SE ASIENTA EN EL ORIGINAL DEL ESCRITO PRESENTADO ANTE UN ÓRGANO JURISDICCIONAL CON LA CONSIGNADA EN LA COPIA QUE DE ESE DOCUMENTO SE DEVUELVE AL INTERESADO, DEBE OTORGARSE CREDIBILIDAD A LA QUE CONSTA EN EL DOCUMENTO CON QUE ALGUNA DE LAS PARTES JUSTIFICA QUE SU INSTANCIA ESTUVO ACOMPAÑADA DE UN DETERMINADO NÚMERO DE COPIAS.

---

[119] Lineamiento 19, fracción I, de los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal.

> La razón que el oficial mayor de un órgano jurisdiccional asienta en el original de un escrito o promoción de un particular, que se entrega al secretario respectivo para que a su vez dé cuenta al titular con lo solicitado, debe ser congruente con la constancia o razón que dicho funcionario consigne en la copia que del mismo devuelve o entrega al interesado como acuse de recibo, a efecto de que no exista duda al respecto; por tanto, en caso de incongruencia entre una y otra razones, debe otorgarse credibilidad a la que consta en el documento con que alguna de las partes justifica que su instancia estuvo acompañada de un determinado número de copias pues, de lo contrario, se colocaría en estado de indefensión al promovente, ya que se llegaría al extremo de exigirle prueba distinta del documento que a él se le entregó como justificante de la forma y términos en que actuó para probar su veracidad.
>
> SEGUNDO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL SEXTO CIRCUITO.
>
> Amparo en revisión 141/2006. Raquel Hernández Rodríguez. 31 de mayo de 2006. Unanimidad de votos. Ponente: Ma. Elisa Tejada Hernández. Secretario: Crispín Sánchez Zepeda.

Ahora bien, es necesario recordar que no sólo es posible presentar una solicitud de acceso de los derechos ARCO de manera presencial, ya que existe otro mecanismo tal como el INFOMEX-DF. Bajo esta última herramienta tecnológica, el titular de los datos personales o su representante legal, pueden registrar su solicitud y al término de llenar los requisitos ahí exigidos, el sistema arrojará un acuse de recibido, con todas las características señaladas anteriormente.

Es importante resaltar que, en términos del numeral 39, fracción II, de los Lineamientos para la gestión de solicitudes de información pública y de datos personales a través del sistema INFOMEX del Distrito Federal, en el supuesto de que la solicitud hubiere sido registrada en el módulo manual de ese sistema electrónico, y que el titular de los datos personales o su representante legal se hubiere retirado de las instalaciones de la oficina de información pública, se le deberá

remitir al domicilio o medio señalado para recibir notificaciones el acuse que genere el INFOMEX.

La fracción II del artículo en comento se encuentra conformada por varios componentes: el primero de ellos establece que, una vez ingresada la solicitud, el servidor público deberá verificar que se reúnan todos los requisitos de procedencia señalados en el artículo 34 de la Ley de Protección de Datos Personales para el Distrito Federal, que a saber son:

Artículo 34…

I. Nombre del ente público a quien se dirija;

II. Nombre completo del interesado, en su caso, el de su representante legal;

III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;

IV. Cualquier otro elemento que facilite su localización;

V. El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones, y

VI. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas

…

El siguiente componente que conforma la fracción en comento establece el supuesto de que no se reuniera alguno de estos requisitos y señala que se deberá prevenir al particular para que en un término de cinco días hábiles subsane la dolencia detectada, so pena, de no realizarse esa precisión, de que la solicitud se tendrá por no presentada.

Como último componente, se señala que en el caso de que la solicitud reúna todos los formalismos demandados por el artículo 34, se deberá turnar "… a la unidad administrativa que corresponda para que proceda a la localización de la información solicitada…"; el turno en comento se deberá realizar por medio del INFOMEX-DF. Es necesario precisar que quién debería recibir la solicitud para su trámite interno, es el responsable del o los sistemas de datos personales, y presupone este hecho que el servidor público que se encuentra al frente de la oficina de información pública cuenta con el conocimiento suficiente de cada uno de los sistemas que fueron registrados ante el Instituto de Acceso a la Información Pública del Distrito Federal. Lo anterior, con el fin de agilizar el trámite de desahogo de la solicitud; una vez que la unidad administrativa haya terminado la gestión interna de desahogo de la solicitud de alguno de los derechos ARCO, deberá notificar a la oficina, por el mismo medio (es decir, el INFOMEX-DF), el resultado obtenido.

La fracción III contempla dos hipótesis centrales: la primera de ellas radica en que la unidad administrativa haya localizado la información objeto de la solicitud en trámite, y la segunda hipótesis que se plantea es que no se haya localizado esa información. En ambos casos, como se precisó en el párrafo anterior, deberá notificar a la oficina de información pública el resultado obtenido. Bajo la primera hipótesis, el servidor público encargado de la oficina señalada deberá notificar[120] al titular de los datos personales o a su representante legal el resultado obtenido y, en su caso, comunicarle en ese mismo acto el costo "… que por concepto de reproducción deberá pagar […] en los términos

[120] Fracción IV, artículo 35 de la Ley de Protección de Datos Personales para el Distrito Federal.

del Código Financiero del Distrito Federa"[121], y deberá solicitarle que acuda ante ésta (la OIP) con el propósito de que acredite su personalidad. Bajo el supuesto de la última hipótesis, el funcionario encargado de la citada oficina, al recibir la notificación de la unidad administrativa, deberá turnarla a otra oficina. Es necesario resaltar que el procedimiento descrito hasta este momento deberá llevarse dentro del plazo de los quince días hábiles, fijado por el artículo 32 de la Ley en comento.

Es importante subrayar que en el caso de que la búsqueda de los datos personales hubiere arrojado un resultado negativo, es decir, que no se encontrase la información dentro de los sistemas de datos personales, se deberá levantar un acta circunstanciada en la que se indique el o los sistemas de datos personales en los que se haya realizado la búsqueda, y deberá estar firmada por el responsable de los sistemas de datos personales en donde se realizó la búsqueda, el servidor público encargado de la oficina de información pública y el representante del órgano interno de control. Lo anterior, en términos del último párrafo del artículo 32 de la Ley de Protección de Datos Personales para el Distrito Federal.

Las dos últimas fracciones del artículo en comento se encuentran íntimamente relacionadas, ya que establecen los mecanismos de entrega de la información requerida o del resultado obtenido de la búsqueda de la información, esto previa identificación que realice el titular de los datos personales o su representante legal. En el supuesto de que se presentase el representante legal, el servidor público que se encuentre al frente de la oficina de información pública deberá verificar que el documento con que se acredite el representante cuente con todas las atribuciones necesarias para la representación; en caso contrario, se le deberá negar el acceso. La acreditación en comento deberá realizarse dentro de los diez días hábiles siguientes al que se haya notificado el resultado obtenido.

---

[121] Segundo párrafo de la fracción III, del artículo 35 de la Ley de Protección de Datos Personales para el Distrito Federal.

Artículo 36.- En caso de que no proceda la solicitud, la oficina de información pública deberá 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, pudiendo recaer dichas funciones en la misma persona.

Issa Luna Pla

COMENTARIO

En el supuesto de que el ente público determine que es improcedente el ejercicio de alguno de los derechos ARCO, se debe notificar al titular de los datos personales o su representante legal tal hecho. El oficio por el que se notifique tal situación debe reunir varios requisitos de forma y de fondo para que éste tenga validez.

Bajo tal supuesto, el artículo 36 de la Ley de Protección de Datos Personales para el Distrito Federal señala que debe reunir todos los extremos del principio de legalidad contemplado en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, entendiendo por tal:

> …FUNDAMENTACION Y MOTIVACION, CONCEPTO DE.
>
> La garantía de legalidad consagrada en el artículo 16 de nuestra carta magna, establece que todo acto de autoridad precisa encontrarse debidamente fundado y motivado, entendiéndose por lo primero la obligación de la autoridad que lo emite, para citar los preceptos legales, sustantivos y adjetivos, en que se apoye la determinación adoptada; y por lo segundo, que exprese una serie de razonamientos lógico-jurídicos sobre el por qué considero que el caso concreto se ajusta a la hipótesis normativa.
>
> CUARTO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.
>
> AMPARO EN REVISION 220/93. ENRIQUE CRISOSTOMO ROSADO Y OTRO. 7 DE JULIO DE 1993. UNANIMIDAD DE VOTOS. PONENTE: ALFONSO MANUEL PATIÑO VALLEJO. SECRETARIO: FRANCISCO FONG HERNANDEZ.
>
> SEMANARIO JUDICIAL DE LA FEDERACION, OCTAVA EPOCA, TOMO XIV, NOVIEMBRE DE 1994, P. 450.

El elemento "fundado" contemplado en el artículo en comento, y que deviene del principio citado, implica que en el escrito por el cual se notifica la negativa del ejercicio de alguno de los derechos ARCO debe señalarse, en un primer término, el o los preceptos legales que facultan a ese ente público a emitir el oficio en comento, esto es la norma que le otorga competencia para la emisión del acto; y, en un segundo término, deberán establecerse los cuerpos legales y preceptos que esté aplicando para su negativa; es decir, los artículos que son aplicables al caso concreto, mediante la cita del o los preceptos legales que imposibiliten al ente público obsequiar una respuesta favorable a la solicitud del titular de los datos personales[122].

El siguiente elemento que conforma el principio de legalidad es la "motivación", la cual implica todos y cada uno de los argumentos, circunstancias especiales o razones que debe verter el ente público para determinar la improcedencia. Es necesario hacer hincapié en que dicha argumentación debe guardar una estrecha relación con el fundamento empleado.

Ahora bien, es importante señalar que la Ley de Protección de Datos Personales para el Distrito Federal no establece de manera directa las limitantes al derecho fundamental que regula (a diferencia de la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal). No obstante lo anterior, el artículo 12 de la Ley de Protección de Datos Personales señala ciertas causales por las que se podría negar el ejercicio de los derechos ARCO. Dicho artículo establece:

> "Artículo 12.- Los responsables de los sistemas de datos personales con fines policiales, para la prevención de conductas delictivas o en

---

[122] El Poder Judicial de la Federación, ha señalado al respecto que:

> … la garantía de fundamentación consagrada en el artículo 16 constitucional lleva implícita la idea de exactitud y precisión en la citación de los cuerpos legales, preceptos, incisos, subincisos y fracciones de los mismos que se están aplicando al particular en el caso concreto, y no es posible abrigar en la garantía individual comentada, ninguna clase de ambigüedad, o imprecisión, puesto que el objetivo de la misma primordialmente se constituye por una exacta individualización del acto autoritario, de acuerdo a la conducta realizada por el particular, la aplicación de las leyes a la misma y desde luego, la exacta citación de los preceptos competenciales, que permiten a las autoridades la emisión del acto de poder… (*Séptima Época; Instancia: Tribunal Colegiado de Circuito; Fuente: Semanario Judicial de la Federación; Tomo: 175-180 Sexta Parte; Página: 98*)

> materia tributaria, podrán negar el acceso, rectificación, oposición y cancelación de datos personales en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando, así como cuando los mismos obstaculicen la actuación de la autoridad durante el cumplimiento de sus atribuciones"

Del artículo citado podemos determinar que las limitantes son:

- Defensa del Estado
- Seguridad Pública
- Protección de derechos y libertades de terceros
- Investigaciones
- Obstaculización de las actividades de las autoridades

Sin embargo, estas causales no las pueden invocar todos los entes públicos, sino que sólo aquellos que se encuentren relacionados con la materia tributaria y seguridad pública en el Distrito Federal.

Aquí cabría preguntarnos qué pasaría si se solicitara un derecho ARCO sobre datos contenidos en un sistema de datos personales que no estuviera relacionado con los fines policiales, la prevención de conductas delictivas o en materia tributaria y que, de concederse, pudiera ocasionar un riesgo a intereses públicos o privados.

Sobre este particular, se considera que haciendo una interpretación sistemática de la Ley y acudiendo a lo que establece la reciente reforma al artículo 16 de la Constitución Federal, dicha solicitud podría ser declarada improcedente.

El segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, añadido con la reforma en comento, establece 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.

Esta reforma constitucional otorgó la categoría de derecho fundamental al derecho a la protección de datos personales. Pero, como todo derecho, éste no es absoluto y en el mismo párrafo se delimitan causales de excepción, las cuales coinciden en gran medida con las señaladas en el artículo 12 de la Ley de Protección de Datos Personales para el Distrito Federal.

Válidamente, de los preceptos anteriormente citados, podemos determinar que uno de los límites al derecho de protección de datos personales, en consecuencia de los ARCO y sobre el cual debe versar en gran medida el esfuerzo de los entes públicos para negar el ejercicio de estos derechos, es el derecho de terceros, es decir, la protección de los datos personales de otras personas, de su esfera íntima o privada, el patrimonio de terceros, etc.

No podemos soslayar que, bajo esta hipótesis, el ente público debe comprobar dentro de su motivación y fundamentación los elementos que lleven a concluir que al conceder la solicitud de cualquiera de los derechos ARCO al interesado se pondría en riesgo la defensa del Estado, la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de alguna investigación en curso, así como que, de concederse la solicitud, se obstaculice la actuación de la autoridad tributaria o de seguridad pública durante el cumplimiento de sus atribuciones.

En consecuencia, en determinados supuestos es posible declarar la improcedencia de los derechos de acceso, rectificación y cancelación u oposición reconocidos en la Ley de Protección de Datos Personales para el Distrito Federal.

En concreto, es posible denegarlos en los siguientes casos:

- En función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando en materia de seguridad pública.
- En los sistemas de datos personales en materia tributaria cuando el ejercicio de estos derechos obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el interesado este siendo objeto de actuaciones inspectoras.

En el caso del derecho de cancelación, la Ley en comento establece que no procederá cuando pueda causar perjuicios a derechos o intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos (artículo 29).

Finalmente, debemos hacer mención de los requisitos formales en caso de que se declare improcedente una solicitud ARCO. En este sentido, la determinación, además de observar los requisitos de motivación y fundamentación, debe estar firmada por el titular de la oficina de información pública, instancia ante la que se presenta la solicitud, y por el responsable del sistema de datos personales correspondiente, ya que es a éste a quien compete resolver sobre el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos de las personas. El responsable también tiene la obligación de adoptar los procedimientos adecuados para dar trámite a las solicitudes ARCO.

Cabe señalar que en esta respuesta, firmada por el responsable de la oficina de información pública y por el responsable del sistema de datos personales (figura que puede recaer en la misma persona), se deberá notificar al solicitante su derecho a interponer un recurso de revisión ante el Instituto de Acceso a la Información Pública del Distrito Federal.

Artículo 37.- El trámite de solicitud de acceso, rectificación, cancelación u oposición de datos de carácter personal es gratuito. No obstante, el interesado deberá cubrir los costos de reproducción de los datos solicitados, en términos de lo previsto por el Código Financiero del Distrito Federal.

Los costos de reproducción de la información solicitada se cobrarán al solicitante de manera previa a su entrega y se calculará atendiendo a:

I. El costo de los materiales utilizados en la reproducción de la información;

II. El costo de envío; y

III. La certificación de documentos cuando proceda.

Los Entes Públicos deberán esforzarse por reducir al máximo, los costos de entrega de información.

Miguel Carbonell

COMENTARIO

La fracción III del párrafo segundo del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos establece con claridad el principio de gratuidad en el acceso a la información, y también respecto a las solicitudes de acceso y rectificación de datos personales.

En congruencia con dicha disposición, el artículo 37 de la Ley que estamos comentando señala que los trámites relativos a datos personales (acceso, rectificación, cancelación u oposición) son gratuitos.

La anterior afirmación se debe considerar en su literalidad; es decir, lo gratuito son los trámites realizados ante las autoridades correspondientes o las solicitudes relativas a los datos personales. Ahora bien, esto no significa que no se puedan generar costos para el peticionario respecto de cuestiones distintas a los trámites derivados de una solicitud.

Por ejemplo, la Ley en el artículo 37 se refiere a los costos relativos a los materiales utilizados para reproducir la información, al envío, en su caso, de la información solicitada y a la certificación que se tuviera que hacer si así lo solicita el interesado.

En todo caso, lo relativo a los costos de reproducción será determinado por el Código Financiero del Distrito Federal en cuanto a su monto.

Sin embargo, dicho Código no puede fijar de manera arbitraria o absolutamente libre el monto de los costos de reproducción, envío y certificación. Por el contrario, los costos no pueden superar un cierto umbral de razonabilidad, porque de lo contrario los volvería inconstitucionales, al inhibir de forma indebida el ejercicio de un derecho fundamental. En este sentido, tiene plena justificación el último párrafo del artículo 37, que ordena a los entes públicos obligados por la Ley que tomen todas las medidas apropiadas y pertinentes para reducir al máximo los costos de entrega de la información.

Ahora bien, en virtud de que ese último párrafo es una norma en buena medida programática (ya que señala un objetivo que se debe lograr o alcanzar, pero no incluye un listado de las medidas que se deben observar para alcanzarlo), el intérprete puede legítimamente preguntarse qué deben hacer los entes obligados a fin de dar cumplimiento a lo ordenado por la Ley. Es decir, de qué manera pueden proceder los funcionarios para reducir al máximo los costos de entrega de la información.

En este punto la tarea principal debe ser sobre todo pedagógica hacia los usuarios, dado que los costos están predeterminados por el Código Financiero del Distrito Federal. Es decir, se les debería explicar a los peticionarios de datos personales (bajo cualquiera de las modalidades que señala la Ley) que hay ciertas formas de entregar la información que abaten costos. Y lo mismo sucede con los gastos de envío.

Respecto de la determinación de los costos, con independencia de lo que establece el citado Código Financiero, hay que considerar que los

elementos señalados en la fracción I y II del artículo 37 que estamos analizando son de carácter objetivo. O sea, se puede determinar con cierta objetividad el costo de una fotocopia, de un CD o de un diskette. Igualmente, se puede saber lo que cuesta un envío postal o un determinado servicio de mensajería. Se trata de información que es pública y cuya verificación no es difícil de hacer. La duda surge respecto del cálculo de lo señalado por la fracción III del artículo en comento.

En otras palabras: ¿cómo se debe calcular el costo de la certificación de documentos? La primera respuesta, en efecto, la encontramos en el Código Financiero. Pero supongamos por un momento que un peticionario no está de acuerdo con ese costo y lo impugna a través de un amparo. ¿Cómo tendría que construir su argumentación jurídica la autoridad jurisdiccional correspondiente, a fin de verificar que el costo estuviera apegado a los principios constitucionales que rigen en materia de acceso a la información pública y protección de datos personales?

Hace un tiempo fue cuestionado, a través del juicio de amparo, el costo de copias certificadas que había determinado la Comisión Nacional de los Derechos Humanos. El particular promovente de la acción de amparo obtuvo la protección de la justicia federal, a fin de que no se le cargara un costo que estaba por arriba de lo razonable.

No es fácil dar respuestas certeras y precisas a esas cuestiones, pero tiene sentido al menos plantearlas, dado que atañen por igual al legislador (al señalar los costos en el Código Financiero) y a los particulares (que tienen desde luego el derecho de estimar que algún costo desproporcionado inhibe el ejercicio de uno de sus derechos fundamentales y, en esa medida, pueden defenderse por los medios que establece el ordenamiento constitucional mexicano).

Lo que debe quedar claro, en todo caso, es que el costo de reproducción, envío y certificación debe ser el menor posible, pues es la única manera de evitar sesgos discriminatorios por razones económicas en el ejercicio de los derechos fundamentales involucrados (acceso a la información pública y protección de datos personales).

Artículo 38.- Podrá interponer recurso de revisión ante el Instituto, el interesado que se considere agraviado por la resolución definitiva, que recaiga a su solicitud de acceso, rectificación, cancelación u oposición o ante la omisión de la respuesta. Para este efecto, las oficinas de información pública al dar respuesta a las solicitudes, orientarán al particular sobre su derecho de interponer el recurso de revisión y el modo y plazo para hacerlo.

Lo anterior, sin perjuicio del derecho que les asiste a los interesados de interponer queja ante los órganos de control interno de los entes obligados.

Miguel Carbonell

COMENTARIO

La Ley de transparencia del Distrito Federal regula el recurso de revisión en sus artículos 76 a 92.

La Ley de datos personales que estamos analizando señala que será precisamente ese recurso el que se deberá interponer, en caso de inconformidad con la respuesta que se obtenga por parte de la autoridad a una solicitud de acceso, rectificación, cancelación u oposición de datos personales. También procede el recurso por omisión en el deber de respuesta.

El artículo 78 de la Ley de Transparencia establece el plazo para la interposición del recurso: 15 días hábiles, contados a partir de que surta efectos la notificación de la resolución de la autoridad. En el supuesto de que el recurso se interponga por omisión de respuesta, el plazo empieza a contarse desde que vence el periodo que señala la Ley para que la autoridad haya formulado su respuesta.

El propio artículo 78 de la Ley de Transparencia señala los requisitos que debe contener el recurso de revisión. El texto conducente del señalado precepto es el siguiente:

> El recurso de revisión podrá interponerse por escrito libre, o a través de los formatos que al efecto proporcione el Instituto o por medios electrónicos, cumpliendo con los siguientes requisitos:

I. Estar dirigido al Instituto de Acceso a la Información Pública del Distrito Federal;

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;

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 notificación correspondiente. Cuando se trate de solicitudes que no se resolvieron en tiempo, anexar copia de la iniciación del trámite.

Hay que señalar que el artículo 38 de la Ley de datos personales ordena a las oficinas de información pública orientar a los particulares respecto de su derecho a interponer el recurso de revisión, en caso de que estén insatisfechos con la respuesta recaída a una solicitud de datos personales. En esa información deben precisar al interesado el modo y plazo en que pueden interponer el recurso en cuestión. Lo mejor para hacer realidad este mandato legal es simplemente agregarlo en forma de formato para todas las resoluciones que se dicten en la materia.

Desde luego, la interposición del recurso de revisión no exime de la eventual responsabilidad de los funcionarios que tienen a su cargo el trámite de las solicitudes y la custodia de los datos personales.

Por eso es que se considera acertada la disposición del segundo y último párrafo del artículo 38, según el cual los interesados pueden interponer queja ante los órganos de control interno de los entes obligados.

Abordaremos con detalle el trámite del recurso de revisión al comentar el artículo 40 de la Ley de datos personales, pues es el artículo que contiene una remisión específica sobre el tema.

Antes de terminar este comentario, conviene señalar que el derecho a interponer un recurso en contra de las decisiones de cualquier autoridad forma parte de lo que se conoce en la teoría jurídica contemporánea como el debido proceso legal (es decir, lo que se denomina "due process of law" en el ámbito anglo-sajón)[123]. Por medio de ese recurso se busca que la decisión de la autoridad sea revisada por un órgano imparcial y autónomo, que verifique su apego a las normas jurídicas que rigen el acto en cuestión.

---

[123] Orth, John V. *Due process of law. A brief history*. Lawrence, University of Kansas Press, 2003; García Ramírez, Sergio, "El debido proceso. Concepto general y regulación en la Convención Americana de Derechos Humanos", *Boletín mexicano de derecho comparado*, número 117, México, 2006.

Artículo 39.- El Instituto tendrá acceso a la información contenida en los sistemas de datos personales que resulte indispensable para resolver el recurso. Dicha información deberá ser mantenida con carácter confidencial y no estará disponible en el expediente.

Las resoluciones que emita el Instituto serán definitivas, inatacables y obligatorias para los entes públicos y los particulares.

En contra de las resoluciones del Instituto el particular podrá interponer juicio de amparo.

La autoridad judicial competente tendrá acceso a los sistemas de datos personales cuando resulte indispensable para resolver el asunto y hubiera sido ofrecida en juicio. Dicha información deberá ser mantenida con ese carácter y no estará disponible en el expediente.

Miguel Carbonell

COMENTARIO

El artículo 39 contiene distintas disposiciones de la mayor importancia, no solamente en relación con el trámite del recurso de revisión, sino respecto de la concepción global del derecho a la protección de datos personales. Veamos.

Por un lado se señala que el InfoDF tiene acceso a la información contenida en las bases de datos personales. Es decir, el InfoDF cuenta con las mismas facultades de acceso que los funcionarios encargados de resguardar los datos personales, lo cual es del todo congruente con el carácter de autoridad en la materia que tiene el Instituto, pero además resulta indispensable para que ejerza de forma completa y apropiada su tarea de supervisión respecto de los entes públicos obligados.

Pero quizá sea el párrafo segundo del artículo que estamos comentando el más importante, en el sentido de que define perfectamente el papel del InfoDF respecto de la tutela del derecho fundamental a la protección de datos personales. En efecto, el segundo párrafo del artículo 39 establece el carácter definitivo, inatacable y obligatorio de las resoluciones del Instituto. Estas tres características operan tanto frente a las autoridades, como frente a los particulares (con el importante matiz del párrafo tercero que enseguida comentaremos).

¿Qué consecuencias se desprenden de lo que dispone el párrafo segundo? Su carácter de definitivo se refiere a que las resoluciones del Instituto no pueden ser revisadas o revocadas por el propio órgano, ni forman parte de un procedimiento más amplio: son el final del procedimiento que inicia con una solicitud presentada por un particular o con el ejercicio de alguna facultad que le conceda la Ley al propio Instituto. Su carácter de inatacables significa que contra ellas no cabe interponer ningún recurso ordinario previsto por ninguna norma de rango legal; la decisión del Instituto está blindada frente a cualquier impugnación de carácter ordinario (salvo la procedencia, en su caso, del recurso constitucional de amparo, distinto de los recursos ordinarios). Su carácter de obligatorias supone que no se pueden dejar de cumplir y que su acatamiento no está condicionado a ningún otro acto de convalidación ni nada por el estilo: se deben cumplir por el mero hecho de haberse emitido. No son recomendaciones o sugerencias: las determinaciones del Instituto son órdenes y obligan de forma completa.

El tercer párrafo del artículo en comento señala la ya apuntada procedencia de ese recurso de carácter extraordinario que en el sistema jurídico mexicano es el juicio de amparo, regulado a nivel constitucional en los artículos 103 y 107 de la Carta Magna. Ahora bien, el mismo párrafo señala que el amparo lo puede interponer el particular, indicando, como es obvio, al Instituto como autoridad responsable y a la determinación que se quiere impugnar como acto reclamado.

Lo anterior significa que el ente público a cargo de los datos personales no puede recurrir al amparo para combatir la determinación del InfoDF. La determinación legislativa del párrafo tercero es correcta en virtud de tres consideraciones al menos:

a) Como se ha venido repitiendo a lo largo de varios comentarios, 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. Eso hace

que sea correcto que la legitimación para interponerlo la tengan los particulares y no las autoridades.

b) La Ley de Amparo en su artículo 9 limita el acceso al juicio de amparo para las que llama (de forma no muy apropiada, quizá) "personas morales oficiales", de tal suerte que su legitimación activa para promover un amparo se limita a aquellos casos en que "el acto o la ley que se reclame afecte los intereses patrimoniales de aquéllas". Para afectaciones a entes públicos que no sean de carácter patrimonial proceden otros medios de defensa, pero no el amparo. En algunos casos, de acuerdo a lo que señala el artículo 105, fracción I, de la Constitución Política de los Estados Unidos Mexicanos, pudiera llegar a plantearse una controversia constitucional ante la Suprema Corte de Justicia de la Nación.

c) El ejercicio de los derechos fundamentales debe estar sujeto a las menores formalidades y cargas procesales que sean posibles, sobre todo para los titulares de tales derechos. De otro modo se estaría generando una barrera que sin lugar a dudas generaría un efecto inhibitorio indeseable. Por eso es que se justifica que las leyes de transparencia y acceso a la información pública gubernamental, así como las leyes de protección de datos personales, simplifiquen al máximo los procedimientos y los hagan tan breves como sea posible.

En ese tenor, es explicable que el recurso de revisión sea la última instancia "administrativa", sin que la autoridad pueda llevar el tema ante un tribunal contencioso-administrativo, pues de esa manera se haría muy prolongado el procedimiento y se obligaría al particular a incurrir en una serie de gastos (contratar a un abogado, para empezar) que harían sumamente gravosos los procedimientos para ejercer sus derechos fundamentales de acceso a la información pública y de protección de datos personales. Tomando en cuenta que, como ya se apuntaba, el titular de los derechos en juego son los particulares y no las autoridades, parece razonable que la Ley determine el carácter definitivo de las decisiones del Instituto en materia de datos personales.

Artículo 40.- El recurso de revisión será tramitado de conformidad con los términos, plazos y requisitos señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Igualmente, el recurrente podrá interponer el recurso de revocación, que será sustanciado en los términos que establezca la propia Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y el Reglamento Interior del Instituto.

Miguel Carbonell

COMENTARIO

El artículo 40 de la Ley en comento contiene dos párrafos. En el primero se refiere al régimen jurídico al que se deberá someter la tramitación ante el InfoDF del recurso de revisión, en particular respecto de los términos, plazos y requisitos. Para tales efectos, la Ley de datos personales incluye un reenvío, en el párrafo mencionado, a la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal. Nos referiremos enseguida al contenido de esta Ley, en la parte que ahora nos interesa.

En el segundo párrafo, el artículo 40 se refiere al recurso de revocación, para cuya substanciación remite a la Ley local de Transparencia, pero también al Reglamento Interior del InfoDF.

En cuanto a de la remisión del primer párrafo, cabe recordar lo que ya se dijo respecto del plazo para la interposición del recurso de revisión. El artículo 78 de la Ley de Transparencia señala como plazo común y general el de 15 días hábiles, contados a partir de la fecha en que surta efecto la notificación del acto que se va a impugnar. En caso de que el recurso se promueva reclamando una falta de respuesta por parte del ente obligado, el plazo señalado comenzará a contarse desde el momento en que haya transcurrido el tiempo que señala la Ley para que se emita la respuesta.

Con relación a las formalidades a observar en la interposición del recurso, el mismo artículo 78 determina lo siguiente:

El recurso de revisión podrá interponerse por escrito libre, o a través de los formatos que al efecto proporcione el Instituto o por medios electrónicos, cumpliendo con los siguientes requisitos:

I. Estar dirigido al Instituto de Acceso a la Información Pública del Distrito Federal;

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;

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 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 procedente hacer del conocimiento del Instituto.

Por su parte, el recurso de revocación al que se refiere el artículo 40 que estamos comentando, está regulado por el artículo 89 de la Ley de Transparencia del Distrito Federal.

Se trata de un recurso que se interpone contra las resoluciones no definitivas que pueda tomar el InfoDF en el trámite de un recurso de

revisión. El plazo para su interposición es de 3 días hábiles, contados a partir de que surta efectos la notificación del acto o resolución que se pretende combatir. La Ley es acuciosa, en el artículo 89, al señalar las formalidades del recurso (algunas quizá innecesarias). El mismo precepto señala que una vez que se interpone el recurso de revocación, dejan de correr los plazos establecidos legalmente para resolver el recurso de revisión; ahora bien, esto no causa ningún tipo de lesión en la celeridad con que se debe tramitar la revisión, en virtud de lo breves que son los plazos establecidos por el artículo 89 para resolver el recurso de revocación.

El Reglamento Interior del InfoDF, al que alude el párrafo segundo del artículo 40 que estamos analizando, fue publicado en la Gaceta Oficial del Distrito Federal el 26 de diciembre de 2008.

El artículo 21, fracción II, del citado Reglamento señala que es competencia de la Dirección Jurídica y Desarrollo Normativo la de

> II. Substanciar los recursos de revisión, de revocación y de recusación en los términos previstos en la Ley de Transparencia y la Ley de Datos Personales, el presente Reglamento y demás normatividad aplicable, así como elaborar los proyectos de resolución que correspondan.

El recurso de revocación, lo mismo que el de revisión, son resueltos por el Pleno, según lo indica el artículo 12, fracción XXIV, del propio Reglamento (el cual viene a reiterar simplemente el mandato legal contenido en el artículo 71, fracción II, de la Ley de Transparencia, por lo que respecta al recurso de revisión).

Artículo 41.- Constituyen infracciones a la presente Ley:

I. La omisión o irregularidad en la atención de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

II. Impedir, obstaculizar o negar el ejercicio de derechos a que se refiere la presente Ley;

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;

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;

X. Obtener datos personales de manera engañosa o fraudulenta;

XI. Transmitir datos personales, fuera de los casos permitidos, particularmente cuando la transmisión haya tenido por objeto obtener un lucro indebido;

XII. Impedir u obstaculizar la inspección ordenada por el Instituto o su instrucción de bloqueo de sistemas de datos personales, y

XIII. Destruir, alterar, ceder datos personales, archivos o sistemas de datos personales sin autorización;

XIV. Incumplir con la inmovilización de sistemas de datos personales ordenada por el Instituto, y

XV. El incumplimiento de cualquiera de las disposiciones contenidas en esta Ley.

Las infracciones a que se refiere este artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada en términos de la Ley de Federal de Responsabilidades de los Servidores Públicos, siendo independientes de las de orden civil o penal que procedan, así como los procedimientos para el resarcimiento del daño ocasionado por el ente público.

Miguel Carbonell

COMENTARIO

La fracción VII del párrafo segundo del artículo 6 de la Constitución Política de los Estados Unidos Mexicanos señala que deben existir sanciones para quienes violen las leyes de acceso a la información y transparencia. En rigor, lo que contiene dicha fracción es un mandato al legislador, a fin de que prevea: a) las conductas que están obligados a realizar los aplicadores prácticos de todo el régimen jurídico en materia de transparencia y acceso a la información pública; y b) las sanciones que corresponde aplicar a quienes no observen dichas conductas. El artículo 41 de la Ley que estamos analizando trata precisamente de ambos asuntos, si bien en el segundo incorpora una remisión a otro ordenamiento, como lo veremos enseguida.

Para poder cumplir con lo que ordena la Constitución General de la República, el legislador cuenta con un margen legítimo de apreciación y de configuración. Dentro de ese espacio el legislador

debe elegir si las leyes en materia tanto de transparencia como de protección de datos personales tienen que incluir un capítulo en el que se detallen las sanciones aplicables, o si tal previsión es objeto de un reenvío legislativo a otras normas legales (por ejemplo a las leyes de responsabilidades de los funcionarios públicos, como es el caso del artículo que nos ocupa).

Desde el punto de vista de la técnica legislativa, lo más correcto es contar con una regulación lo más comprensiva posible dentro de un único cuerpo legislativo, evitando en consecuencia las remisiones a otras fuentes del derecho. En vista de lo dicho, resulta del todo adecuado que las propias leyes de transparencia y de protección de datos personales pudieran establecer el catálogo completo de conductas y el correspondiente catálogo de sanciones. Pero no es una opción que resulte obligatoria para el legislador. Es bueno y pertinente que lo haga, pero si deja de hacerlo no viola por ello la Constitución. Lo importante es que, como se dijo, se describan las conductas a sancionar y haya un catálogo de sanciones para cada una de esas conductas. Si está o no en la misma ley es algo opcional para el autor de la norma.

El régimen de sanciones que ordena la fracción VII del artículo 6 constitucional (y las normas de rango legislativa que de ella derivan) forma parte de lo que los teóricos del derecho administrativo llaman "derecho administrativo sancionador".

Entre los expertos en el tema parece haber un cierto consenso acerca del hecho de que los principios del derecho penal son aplicables, en términos generales, al derecho administrativo sancionador. Además, así parece haberlo entendido la jurisprudencia de nuestros tribunales federales; al respecto pueden citarse, entre otras, las siguientes tesis jurisprudenciales:

> RESPONSABILIDADES DE LOS SERVIDORES PÚBLICOS. LAS SANCIONES ADMINISTRATIVAS PREVISTAS EN LA LEY FEDERAL RELATIVA TAMBIÉN SE RIGEN POR EL PRINCIPIO CONSTITUCIONAL DE EXACTA APLICACIÓN DE LA LEY QUE IMPERA EN LAS DE CARÁCTER PENAL, AUN CUANDO SEAN DE DIVERSA NATURALEZA. La marcada diferencia entre la naturaleza

de las sanciones administrativas y las penales, precisada en la exposición de motivos del decreto de reformas y adiciones al título cuarto de la Constitución Federal, publicado en el Diario Oficial de la Federación el veintiocho de diciembre de mil novecientos ochenta y dos, en los artículos que comprende dicho título y en la propia Ley Federal de Responsabilidades de los Servidores Públicos, con base en la cual se dispone que los procedimientos relativos se desarrollarán en forma autónoma e independiente, no significa que en el ámbito sancionador administrativo dejen de imperar los principios constitucionales que rigen en materia penal, como es el relativo a la exacta aplicación de la ley (nullum crimen, sine lege y nulla poena, sine lege), que constituye un derecho fundamental para todo gobernado en los juicios del orden criminal, garantizado por el artículo 14 de la Constitución Federal, sino que tal principio alcanza a los del orden administrativo, en cuanto a que no se podrá aplicar a los servidores públicos una sanción de esa naturaleza que previamente no esté prevista en la ley relativa. En consecuencia, la garantía de exacta aplicación de la ley debe considerarse, no sólo al analizar la legalidad de una resolución administrativa que afecte la esfera jurídica del servidor público, sino también al resolver sobre la constitucionalidad de la mencionada ley reglamentaria, aspecto que generalmente se aborda al estudiar la violación a los principios de legalidad y seguridad jurídica previstos en los artículos 14 y 16 constitucionales con los que aquél guarda íntima relación. Amparo en revisión 2164/99. Fernando Ignacio Martínez González. 29 de junio de 2001. Unanimidad de cuatro votos. Ausente: Mariano Azuela Güitrón. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: Aída García Franco.

DERECHO ADMINISTRATIVO SANCIONADOR ELECTORAL. LE SON APLICABLES LOS PRINCIPIOS DEL IUS PUNIENDI DESARROLLADOS POR EL DERECHO PENAL. Los principios contenidos y desarrollados por el derecho penal, le son aplicables mutatis mutandis, al derecho administrativo sancionador. Se arriba a lo anterior, si se considera que tanto el derecho administrativo sancionador, como el derecho penal son manifestaciones del ius puniendi estatal; de las cuales, el derecho penal es la más antigua y desarrollada, a tal grado, que casi absorbe al género, por lo cual constituye obligada referencia o prototipo a las otras especies. Para lo anterior, se toma en cuenta que la facultad de reprimir conductas consideradas ilícitas, que vulneran el orden jurídico, es connatural a la organización del Estado, al cual el Constituyente originario le encomendó la realización de todas las actividades necesarias para lograr el bienestar común, con las limitaciones correspondientes, entre las cuales destacan, primordialmente, el respeto irrestricto a los derechos humanos y las normas fundamentales con las que se

construye el estado de derecho. Ahora, de acuerdo a los valores que se protegen, la variedad de las conductas y los entes que pueden llegar a cometer la conducta sancionada, ha establecido dos regímenes distintos, en los que se pretende englobar la mayoría de las conductas ilícitas, y que son: el derecho penal y el derecho administrativo sancionador. La división del derecho punitivo del Estado en una potestad sancionadora jurisdiccional y otra administrativa, tienen su razón de ser en la naturaleza de los ilícitos que se pretenden sancionar y reprimir, pues el derecho penal tutela aquellos bienes jurídicos que el legislador ha considerado como de mayor trascendencia e importancia por constituir una agresión directa contra los valores de mayor envergadura del individuo y del Estado que son fundamentales para su existencia; en tanto que con la tipificación y sanción de las infracciones administrativas se propende generalmente a la tutela de intereses generados en el ámbito social, y tienen por finalidad hacer posible que la autoridad administrativa lleve a cabo su función, aunque coinciden, fundamentalmente, en que ambos tienen por finalidad alcanzar y preservar el bien común y la paz social. Ahora, el poder punitivo del Estado, ya sea en el campo del derecho penal o en el del derecho administrativo sancionador, tiene como finalidad inmediata y directa la prevención de la comisión de los ilícitos, ya sea especial, referida al autor individual; o general, dirigida a toda la comunidad, esto es, reprimir el injusto (considerado éste en sentido amplio) para disuadir y evitar su proliferación y comisión futura. Por esto, es válido sostener que los principios desarrollados por el derecho penal, en cuanto a ese objetivo preventivo, son aplicables al derecho administrativo sancionador, como manifestación del ius puniendi. Esto no significa que se deba aplicar al derecho administrativo sancionador la norma positiva penal, sino que se deben extraer los principios desarrollados por el derecho penal y adecuarlos en lo que sean útiles y pertinentes a la imposición de sanciones administrativas, en lo que no se opongan a las particularidades de éstas, lo que significa que no siempre y no todos los principios penales son aplicables, sin más, a los ilícitos administrativos, sino que debe tomarse en cuenta la naturaleza de las sanciones administrativas y el debido cumplimiento de los fines de una actividad de la administración, en razón de que no existe uniformidad normativa, sino más bien una unidad sistémica, entendida como que todas las normas punitivas se encuentran integradas en un solo sistema, pero que dentro de él caben toda clase de peculiaridades, por lo que la singularidad de cada materia permite la correlativa peculiaridad de su regulación normativa; si bien la unidad del sistema garantiza una homogeneización mínima. Sala Superior, tesis S3EL 045/2002. Recurso de apelación. SUP-RAP-022/2001.-Partido del Trabajo.-25 de octubre de 2001.-Mayoría de cuatro votos.-Ponente: Leonel

Castillo González.-Disidentes: Alfonsina Berta Navarro Hidalgo, Eloy Fuentes Cerda y José Fernando Ojesto Martínez Porcayo.-Secretario: José Manuel Quistián Espericueta

Ahora bien, ¿cuáles son los principios que el legislador está obligado a tomar en cuenta al diseñar el sistema de sanciones que menciona la fracción VII del párrafo segundo del artículo 6 de la Constitución mexicana vigente? Al menos debe tomar en cuenta los principios señalados, de forma expresa o implícita, en el párrafo tercero del artículo 14 constitucional, es decir, los principios de: a) reserva de ley; b) taxatividad; c) proporcionalidad; y d) prohibición de analogía. La explicación exhaustiva de cada uno de esos cuatro principios nos llevaría muchas páginas, pero vale la pena, al menos, apuntar sus características más relevantes[124], dado que su conocimiento es necesario para los aplicadores de las sanciones previstas en normas como el artículo 41 que estamos intentando analizar.

El principio de legalidad en materia penal, que tiene como una de sus consecuencias a la reserva de ley, surge en el ámbito del pensamiento iluminístico-liberal, cuando se piensa que para salvaguardar adecuadamente la libertad de los ciudadanos se tenía que reservar a los órganos legislativos el poder para emanar disposiciones penales. Aunque ya existía en algunos textos normativos anteriores, no es sino hasta el siglo XVIII cuando se universaliza y comienza a concebirse como un verdadero derecho individual.

En general, la reserva de ley puede entenderse como la remisión que hace normalmente la Constitución y de forma excepcional la ley, para que sea justamente una ley y no otra norma jurídica la que regule una determinada materia. En otras palabras, se está frente a una reserva de ley cuando, por voluntad del constituyente o por decisión del legislador, tiene que ser una ley en sentido formal la que regule un sector concreto del ordenamiento jurídico.

---

[124] Un análisis más detenido se encuentra en Carbonell, Miguel, *Los derechos fundamentales en México*, 3ª edición, México, Porrúa, UNAM, CNDH, 2009, pp. 665 y siguientes.

La reserva de ley, siempre que se trate de un Estado que cuente con una Constitución rígida, presenta dos aspectos: por una parte prohíbe la intervención, en las materias reservadas, de fuentes subordinadas a la ley o sub legislativas; por otra, prohíbe en ciertos casos al legislador reenviar la disciplina de esas materias a otras fuentes distintas a la ley.

En la actualidad la reserva de ley cumple una doble función: por un lado una función de carácter liberal o garantista, y por otro, una función democrática.

a) La función liberal o garantista consiste en que a través de la reserva se tutelan los derechos de los ciudadanos contra las intromisiones del poder ejecutivo. Los ciudadanos solamente pueden ver restringida su libertad por virtud de una "ley", no por actos del ejecutivo que no tengan sustento legal. Por eso se ha dicho por muchos teóricos que todo lo referido a los derechos fundamentales se encuentra sujeto a reserva de ley.

b) La función democrática tiene que ver con que, en virtud de la reserva, se reconduce la regulación de ciertas materias al dominio del poder legislativo, el cual es representativo de las mayorías —como el poder ejecutivo— pero también de las minorías políticas de un Estado. En palabras de Manuel Aragón, "Entendida la democracia como democracia pluralista, el Parlamento como órgano de representación de todo el pueblo y el gobierno sólo como órgano de representación de la mayoría, la reserva a la ley de determinadas materias no significa sólo la reserva al órgano más (directamente) democrático, sino también al órgano que por contener la representación de la pluralidad de opciones políticas permite que todas ellas (y no sólo la opción mayoritaria) participen en la elaboración de la norma".

A la luz de lo anterior, cabe apuntar que ciertas variantes de lo que se conoce como "normas penales en blanco" podrían ser violatorias del principio de reserva de ley, tal como lo reconoce la siguiente tesis jurisprudencial:

> NORMAS PENALES EN BLANCO. SON INCONSTITUCIONALES CUANDO REMITEN A OTRAS QUE NO TIENEN EL CARÁCTER DE LEYES EN SENTIDO FORMAL Y MATERIAL. Los denominados "tipos penales en blanco" son supuestos hipotéticos en los que la conducta delictiva se precisa en términos abstractos y requiere de un complemento para integrarse plenamente. Ahora bien, ordinariamente la disposición complementaria está comprendida dentro de las normas contenidas en el mismo ordenamiento legal o en sus leyes conexas, pero que han sido dictadas por el Congreso de la Unión, con apoyo en las facultades expresamente conferidas en la Constitución Política de los Estados Unidos Mexicanos. En consecuencia, las "normas penales en blanco" no son inconstitucionales cuando remiten a otras que tienen el carácter de leyes en sentido formal y material, sino sólo cuando reenvían a otras normas que no tienen este carácter -como el caso de los reglamentos-, pues ello equivale a delegar a un poder distinto al legislativo la potestad de intervenir decisivamente en la determinación del ámbito penal, cuando es facultad exclusiva e indelegable del Congreso de la Unión legislar en materia de delitos y faltas federales.

Las penas en el Estado constitucional de derecho (y, por extensión, todo el derecho administrativo sancionador según lo que ya se ha explicado) no solamente deben estar sujetas al principio de reserva de ley, sino que además deben estar acompañadas de la exigencia de taxatividad, la cual se despliega con mayor amplitud en el campo de la determinación de las conductas sancionables penalmente, que son precisamente el objeto de regulación del artículo 41 bajo estudio.

El artículo 14 párrafo tercero de la Constitución señala que para que se pueda aplicar una sanción penal debe existir una ley "exactamente" aplicable a la conducta de que se trate. A partir de esa disposición podemos extraer un elemento "cualitativo" de la ley penal que vendría exigido por la Constitución; en efecto, para que una ley sea "exactamente" aplicable a una cierta conducta debe tener ciertas "cualidades" lingüísticas, pues es seguro que no toda descripción lingüística tendría la posibilidad de ser aplicada con exactitud a la conducta humana. Así por ejemplo, consideremos un enunciado normativo que dijera lo siguiente: "Se impondrán de cinco a siete años de prisión a la persona que se comporte de manera dañina respecto a otras personas o que altere el bienestar general de la sociedad"; con

esa descripción, ¿cómo podría el juez realizar una "exacta" aplicación si los supuestos normativos están claramente indeterminados, son vagos y polisémicos? Por lo tanto, lo que nos está diciendo el párrafo tercero del artículo 14 es que las normas penales deben contar con ciertos elementos que nos permitan identificar claramente su campo de aplicación. A este deber de precisión y claridad de las normas se le conoce como el principio de "taxatividad" en materia penal (recordando siempre que este y otros principios son aplicables a la materia de sanciones administrativas).

La taxatividad de la ley penal consiste en que los textos que contengan normas sancionadoras describan claramente las conductas que están regulando y las sanciones penales que se pueden aplicar a quien las realicen. La taxatividad es una especie del genérico principio de legalidad en materia penal y tiene por objeto preservar la certeza jurídica (que a su vez es una especie de la seguridad jurídica) y la imparcialidad en la aplicación de la ley penal. Luigi Ferrajoli en su libro clásico *Derecho y razón. Teoría del garantismo penal* describe el principio de taxatividad penal (que también se puede llamar "principio de estricta legalidad") con las siguientes palabras:

> Este principio... puede ser caracterizado ahora como una *regla semántica metalegal de formación de la lengua legal* que prescribe al legislador penal: a) que los términos usados por la ley para designar las figuras de delito sean dotados de extensión determinada, por donde sea posible su uso como predicados "verdaderos de los" hechos empíricos por ellos denotados; b) que con tal fin sea connotada su intensión con palabras no vagas ni valorativas, sino lo más claras y precisas posible; c) que, en fin, sean excluidas de la lengua legal las antinomias semánticas o cuando menos que sean predispuestas normas para su solución. De ahí se sigue, conforme a esta regla, que las figuras abstractas de delito deben ser *connotadas* por la ley mediante *propiedades o características esenciales* idóneas para determinar su *campo de denotación* (o de aplicación) de manera *exhaustiva*, de forma que los hechos concretos que entran allí sean denotados por ellas en proposiciones verdaderas, y de manera exclusiva,

de modo que tales hechos no sean denotados también en proposiciones contradictorias por otras figuras de delito connotadas por normas concurrentes.

Las propiedades o características esenciales que debe contener una ley para cumplir con el principio de taxatividad penal son parecidas, en parte, a las que derivan del principio de reserva de ley, aunque van más allá: dichas características se pueden resumir en el concepto de elementos constitutivos del delito, es decir, en la acción (que debe ser exterior y empíricamente visible), en su efecto o resultado (que debe consistir en un daño tangible) y en la culpabilidad (que debe permitir la adscripción causal de la acción a la persona que la lleva a cabo).

De acuerdo con lo anterior, violarían el principio de taxatividad penal todas las disposiciones legislativas que sancionaran penal o administrativamente una conducta vagamente descrita o aquellas que dispusieran de consecuencias jurídicas también indeterminadas.

Habiendo hecho un repaso somero de los principios de reserva de ley y de taxatividad ya contamos con un panorama acerca de los vínculos que la Constitución impone al legislador en materia penal y en materia de derecho administrativo sancionador. Pero hace falta subrayar un aspecto adicional: el principio de proporcionalidad[125].

Recordemos, de forma sumaria, que el principio de proporcionalidad exige que cualquier determinación de una autoridad que restrinja los derechos fundamentales es aceptable en caso de que no vulnere el contenido esencial del derecho de que se trate, siempre que sea proporcional. Para que se verifique la proporcionalidad es necesario que se observen los sub principios de idoneidad, necesidad y proporcionalidad en sentido estricto; es decir, existirá proporcionalidad cuando: a) la regulación o limitación de un derecho fundamental sea

[125] La bibliografía sobre el tema es cada vez más extensa. Una compilación de autores relevantes puede verse en Carbonell, Miguel (coordinador), *El principio de proporcionalidad y la protección de los derechos fundamentales*, México, CNDH, CEDH de Aguascalientes, 2008.

adecuada para la obtención de un fin constitucionalmente legítimo; b) la medida adoptada sea la más benigna posible respecto del derecho en cuestión, de entre todas las que revistan la misma idoneidad para alcanzar el fin propuesto; y c) las ventajas que se obtengan con la restricción deben compensar los posibles sacrificios del derecho para su titular y para la sociedad en general.

¿Cómo se aplica lo anterior a las leyes que contengan sanciones en materia administrativa? La reflexión sobre este tema debe partir del hecho de que cualquier ley que disponga la aplicación de sanciones —penales o administrativas— supone de alguna u otra forma una intervención en los derechos fundamentales, concretamente sobre el derecho de libertad, según el cual toda persona puede hacer lo que no esté prohibido por el ordenamiento jurídico. La proporcionalidad supone un límite a la "cantidad" de prohibiciones que el legislador puede establecer así como a la cantidad de "penalización" que se puede determinar para una conducta penalmente regulada. Es decir, la proporcionalidad se relaciona con el monto de la sanción que el legislador decide imponer para la realización de X o Y conducta.

Luigi Ferrajoli explica el principio de proporcionalidad con las siguientes palabras:

> El hecho de que entre pena y delito no exista ninguna relación natural no excluye que la primera deba ser *adecuada* al segundo en alguna medida. Al contrario, precisamente el carácter convencional y legal del nexo retributivo que liga la sanción al ilícito penal exige que la elección de la calidad y la cantidad de una se realice por el legislador y por el juez *en relación* con la naturaleza y la gravedad del otro. El *principio de proporcionalidad* expresado en la antigua máxima *poena debet commensurari delicto* es en suma un corolario de los principios de legalidad y de retributividad, que tiene en éstos su fundamento lógico y axiológico.

El párrafo tercero del artículo 14 constitucional establece que no podrán imponerse, en los juicios del orden penal, penas por simple analogía o por mayoría de razón. Se trata de un mandato constitucional que sirve para reforzar el significado de los principios

de reserva de ley y de taxatividad en materia sancionadora. Es decir, lo que nos indica el artículo 14 es que el juzgador no puede acudir a métodos hermenéuticos, como la analogía y la mayoría de razón, para imponer una sanción penal o administrativa y, en consecuencia, debe atenerse a lo que pueda resolver utilizando otros métodos interpretativos en los que se observe la reserva de ley (en el sentido de mandato constitucional por el que se excluyen del ámbito penal fuentes normativas distintas a la ley) y la taxatividad (en el sentido de que las disposiciones que sirvan de base para imponer una sanción penal o administrativa deban ser claras, concretas y específicamente aplicables a la conducta que se pretende sancionar).

Sobre la prohibición de la analogía Luigi Ferrajoli señala que es un corolario del principio de (estricta) legalidad. Este autor indica que "En la medida en que sea posible afirmar de las figuras de calificación penal definidas por las leyes, gracias a su conformidad con el principio de legalidad, que son verdaderas o falsas respecto a los hechos que se examinan, es obvio que no hay sitio para el razonamiento analógico. A la inversa, el uso por parte de la ley, con contraposición con el principio de estricta legalidad, de fórmulas elásticas o carentes de denotación determinada permite la que se ha llamado 'analogía anticipada'".

La última observación de esta cita de Ferrajoli es muy importante porque señala que la prohibición de analogía, siendo coherente con el mandato de taxatividad de la ley penal, debería ser oponible también al legislador.

El propio Ferrajoli nos recuerda que la prohibición de analogía se aplica solamente para la analogía *in malam partem*, es decir, la que es desfavorable para el procesado. En sentido contrario, la analogía puede perfectamente admitirse en la interpretación de las excusas absolutorias o en cualquier aspecto que beneficie al acusado.

Riccardo Guastini nos explica que, desde el punto de vista jurídico, la aplicación analógica es "la aplicación de una norma a un supuesto de hecho *no previsto* por ella, pero *semejante* al previsto por la misma"[126].

---

[126] Guastini, Riccardo, *Estudios sobre la interpretación jurídica*, 6ª edición, México, Porrúa, UNAM, 2004.

Lo que está prohibiendo el mandato constitucional es justamente la aplicación por el juez de normas que no están *expresamente previstas* en la ley como constitutivas de delito y que, por tanto, no son sancionables desde el punto de vista penal. Podríamos decir que la *semejanza* no puede ser tenida en cuenta en materia penal o de sanciones administrativas, sino que por la importancia de los bienes jurídicos que están en juego se requiere prácticamente la identidad entre la conducta a sancionar y la descripción típica contenida en la ley.

Es en este contexto analítico en el que debe ser interpretado y aplicado el artículo 41 de la Ley local del DF en materia de protección de datos personales.

Las 15 fracciones del artículo 41 van describiendo conductas que generan responsabilidad por violación de la Ley. Algunas descripciones son más precisas y otras menos, pero en todo caso caen dentro de reglas razonables de generalidad lingüística. No tiene sentido describir a detalle cada una de ellas.

Lo importante, antes de terminar este comentario, es destacar el contenido de la remisión que se menciona en el último párrafo del artículo 41. Lo que nos indica ese párrafo es que las conductas descritas por las 15 fracciones del propio artículo 41 se van a sancionar de acuerdo a lo que establezca la legislación en materia de responsabilidades de los funcionarios públicos. Pero, además, agrega que las responsabilidades (naturalmente administrativas) que se puedan imponer por esa vía, serán independientes de las de orden penal o civil que resulten aplicables, y serán también independientes de los procedimientos que pudieran llegar a instaurarse para reclamar el resarcimiento causado por una mala aplicación de la ley.

Es interesante destacar, como se pone de manifiesto en el artículo 42 de la Ley en comento, que el reenvío a la legislación de responsabilidades es también una opción importante respecto del órgano que debe imponer las sanciones. Regresaremos de inmediato a ese tema, en el comentario siguiente.

Artículo 42.- El Instituto denunciará ante las autoridades competentes cualquier conducta prevista en el artículo anterior y aportará las pruebas que considere pertinentes. Los órganos de control y fiscalización internos de los entes públicos entregarán semestralmente al Instituto, un informe estadístico de los procedimientos administrativos iniciados con motivo del incumplimiento de la presente Ley y sus resultados. Esta información será incorporada al informe anual del Instituto.

Dicha resolución se comunicará al Ente Público y al responsable del sistema de datos personales y, en su caso, a los interesados de los datos personales que resultaren afectados.

Lo anterior sin perjuicio de las responsabilidades penales o civiles que pudieran derivarse.

Miguel Carbonell

COMENTARIO

En los años recientes se ha producido un intenso debate público, articulado, sobre todo, a través de intervenciones académicas y por parte de los integrantes de los órganos garantes en materia de acceso a la información pública, sobre el alcance de las competencias que deberían tener en materia sancionadora tales órganos. No es un tema fácil, pero supone el contexto de interpretación necesario para comprender a cabalidad el alcance del artículo 42 de la Ley de Protección de Datos Personales para el Distrito Federal.

Hay quienes opinan que es indispensable que los órganos garantes puedan sancionar directamente a los infractores de las leyes de transparencia y a las de protección de datos personales, pues si la competencia de tales órganos se limita a dar vista a los encargados de fiscalizar internamente a los sujetos obligados (por ejemplo a las contralorías), su autoridad y su autonomía pudieran llegar a desdibujarse, pues se convertirían —según ese punto de vista— en una especie de órganos "recomendadores", sin elementos suficientes para obligar de manera tajante a las demás autoridades.

Para otros, el otorgamiento de facultades sancionadoras directas a los órganos garantes los pone en una situación delicada, al menos desde dos puntos de vista: a) desde una óptica política porque la imposición de sanciones genera evidentes tensiones con otros órganos públicos, mucho más consolidados que aquéllos (y muchas veces dispuestos a tomar represalias de todo tipo contra los órganos garantes, tales como restricciones presupuestales, persecuciones penales e intentos de remoción); b) desde una perspectiva jurídica, ya que la imposición de sanciones tiene como requisito la instrucción de procedimientos que no siempre son sencillos, para lo cual se requiere personal especializado, infraestructura, presupuesto, etcétera.

La solución por la que optó el legislador local del Distrito Federal en materia de protección de datos personales es dejarle la facultad sancionadora a los órganos internos de control.

El InfoDF puede, desde luego, participar en los procesos de exigencia de responsabilidades, por medio de la presentación de denuncias y a través de la aportación de pruebas.

Como una medida de control, la Ley en el artículo 42 obliga a los órganos fiscalizadores a entregar un informe semestral al InfoDF, en el que se precisen los procedimientos administrativos iniciados para verificar el cumplimiento de la Ley y los resultados obtenidos. De tal información el InfoDF dará cuenta en la presentación de su informe anual.Estas obligaciones de informar sobre los procedimientos instaurados son importantes porque evitan 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.

Vale la pena reparar en el significado imperativo que utiliza el párrafo primero del artículo 42: el InfoDF "denunciará" y "aportará las pruebas que considere pertinentes", dice el citado precepto. Es decir, el Instituto no puede dejar ni de presentar denuncias ni de aportar

pruebas. Lo que puede hacer es aportar las pruebas que considere que son pertinentes, desechando las que no reúnan esa característica. Pero su involucramiento en los procedimientos de exigencia de responsabilidad no son optativos: debe hacerlo por mandato de la Ley.

El párrafo segundo del artículo en comento, que no es un modelo de congruencia legislativa ni de buena redacción, señala que la resolución que se dicte (suponemos que en los procesos de responsabilidad de funcionarios que pudieran llegar a instaurarse por violaciones a la Ley), serán comunicados al ente público en cuestión, al responsable del sistema de datos personales y, en su caso, a los titulares de los datos que pudieran haber sido afectados por una conducta ilícita.

El último párrafo del artículo 42 desvincula las posibles responsabilidades administrativas derivadas de las conductas prohibidas que enuncia el artículo 41 de la Ley que estamos analizando, de las responsabilidades penales y civiles que pudieran derivarse de las conductas sancionadas. Si bien es cierto que no puede sancionarse a una persona dos veces por un mismo hecho (de acuerdo al conocido principio *Ne bis in idem*, recogido expresamente en el ordenamiento constitucional mexicano), lo que sí puede hacerse es imponerle a una persona distintos tipos de sanciones por la misma conducta, sin afectar por ello sus derechos fundamentales. De esta manera un funcionario público puede eventualmente ser sujeto de responsabilidades administrativas, pero también enfrentar procedimientos civiles o penales que darán lugar, en su caso, a las respectivas sanciones, diferentes en buena medida a las primeras.

ANÁLISIS DE LOS LINEAMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL DISTRITO FEDERAL

ANÁLISIS DE LOS LINEAMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES EN EL DISTRITO FEDERAL [127]

Dra. Isabel Davara F. de Marcos[128]

Los Lineamientos para la Protección de Datos Personales en el Distrito Federal[129] fueron aprobados mediante Acuerdo 547/SO/14-10/2009 del Instituto de Acceso a la Información Pública del Distrito Federal.

El fundamento jurídico para la aprobación de dichos Lineamientos se encuentra en los artículos 23 y 24, fracción I, de la LPDPDF[130].

Puesto que ya hemos comentado los artículos 2, 5, 9, 13, 14, 15, 16, 21 y 26 a 31 de la Ley, a continuación comentaremos en general los Lineamientos, prestando especial atención a los apartados específicos correspondientes a los comentados en la Ley. Así, analizaremos más en profundidad los siguientes numerales:

- 3, relativo a las definiciones.
- 12 a 14, dedicados al principio de información.
- 15 a 17, relativos a las medidas de seguridad.

---

127 Publicados en la Gaceta Oficial del Distrito Federal el 26 de octubre de 2009.

128 Quiero agradecer desde el inicio la inestimable colaboración del Mtro. Miguel Recio Gayo, sin cuya ayuda estos comentarios no hubieran sido posibles.

129 En lo sucesivo, citados también como los Lineamientos PDPDF o los Lineamientos.

130 Que indican, respectivamente, lo siguiente:

> **Artículo 23.-** El Instituto de Acceso a la Información Pública del Distrito Federal es el órgano encargado de dirigir y vigilar el cumplimiento de la presente Ley, así como de las normas que de ella deriven; será la autoridad encargada de garantizar la protección y el correcto tratamiento de datos personales.
>
> **Artículo 24.-** El Instituto tendrá las atribuciones siguientes:
>
> I. Establecer, en el ámbito de su competencia, políticas y lineamientos de observancia general para el manejo, tratamiento, seguridad y protección de los datos personales que estén en posesión de los entes públicos, así como expedir aquellas normas que resulten necesarias para el cumplimiento de esta Ley;

- 18 a 34, sobre los principios aplicables al tratamiento de los datos.
- 35 a 39, relativos a las obligaciones de los entes públicos.
- 42 a 52, sobre los derechos de acceso, rectificación, cancelación y oposición, así como el procedimiento para su ejercicio.

Sin embargo, como decíamos, comentaremos en general todos los Lineamientos; en particular entendemos que especialmente es necesario tener en consideración otros apartados, dado que desarrollan cuestiones específicas como, por ejemplo, el numeral 4, relativo a los tipos de sistemas de datos personales y que, por lo tanto, aclara el concepto de sistema de datos personales. Igualmente, el numeral 5 de los Lineamientos, relativo a las categorías de datos personales, desarrolla el concepto de datos personales establecido en el artículo 2 de la LPDPDF y el numeral 3 de los Lineamientos.

Por lo tanto, a la vista de los artículos de la LPDPDF analizados anteriormente y los numerales de los Lineamientos a analizar en profundidad, es posible presentar la siguiente tabla comparativa que permite ver a nivel conceptual lo que regula la Ley y lo que desarrollan los Lineamientos:

LPDPDF	Art(s).	Lineamientos	Numerales
Definiciones	2	Definiciones	3
Principios de la protección de datos	5	Principios de la protección de datos	18 a 34
Información en la recogida	9	Información en la recogida	12 a 14
Medidas de seguridad	13 a 15	Medidas de seguridad	15 a 17
Consentimiento	16		
Obligaciones del responsable del tratamiento	21	Obligaciones de los entes públicos	35 a 39
Derechos en protección de datos	26 a 31	Derechos en protección de datos y procedimiento	42 a 52

1. Definiciones

Remitiéndonos en primer lugar a la Ley, su artículo 2 define los siguientes términos:

1. Bloqueo de datos personales
2. Cesión de datos personales
3. Datos personales
4. Ente Público
5. Instituto
6. Interesado
7. Oficina de Información Pública
8. Procedimiento de disociación
9. Responsable del Sistema de Datos Personales
10. Sistema de Datos Personales
11. Tratamiento de Datos Personales
12. Usuario

Por su parte, el numeral 3 de los Lineamientos incluye las siguientes definiciones:

1. Autentificación
2. Bloqueo
3. Cancelación
4. Cesionario
5. Documentos
6. Documento de seguridad
7. Encargado

8. Enlace
9. Fuente de acceso público
10. Incidencia
11. INFOMEX
12. Inmovilización
13. Lineamientos
14. Ley
15. Registro Electrónico de Sistemas de Datos Personales
16. Responsable
17. Responsable de seguridad
18. Sistema de datos personales
19. Soporte físico
20. Soporte electrónico
21. Supresión
22. Suspensión

En definitiva, podemos ver que la Ley y los Lineamientos incluyen definiciones que se complementan y que son las siguientes: bloqueo de datos personales; sistema de datos personales y responsable del sistema de datos personales. Además, los Lineamientos proporcionan algunas definiciones que no están en la Ley y que resultan necesarias para una mejor comprensión de las implicaciones que tiene la normativa sobre protección de datos en la práctica. Por ejemplo, los Lineamientos introducen las definiciones de encargado y de supresión, que resultan relevantes.

A continuación, pasamos a profundizar en el análisis de algunas de ellas, especialmente las no tratadas en la Ley. Por tanto, se han seleccionado las de sistema de datos personales y fuente de acceso público, debido a la repercusión que tienen en cuanto al tratamiento de los datos personales.

Datos personales

Si bien la definición ya ha sido analizada al comentar el artículo 2 de la Ley, creemos conveniente hacer una referencia al hecho de que los Lineamientos dedican su numeral 5 a las categorías de datos personales.

Dada la relevancia de este concepto, consideramos oportuno detenernos brevemente en las previsiones de los Lineamientos en particular.

Para ello, en primer lugar incluiremos una comparativa entre la Ley y los Lineamientos:

DCP	Ley PDPDF	Lineamientos
Definición	Datos personales: La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos (art. 2)	
Categorías de datos		Los datos personales contenidos en los sistemas se clasificarán, de manera enunciativa, más no limitativa, de acuerdo a las siguientes categorías:

DCP	Ley PDPDF	Lineamientos
Categorías de datos		I. Datos identificativos: El nombre, domicilio, teléfono particular, teléfono celular, firma, clave del Registro Federal de Contribuyentes (RFC), Clave Única de Registro de Población (CURP), Matrícula del Servicio Militar Nacional, número de pasaporte, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, demás análogos; II. Datos electrónicos: Las direcciones electrónicas, tales como, el correo electrónico no oficial, dirección IP (Protocolo de Internet), dirección MAC (dirección Media Access Control o dirección de control de acceso al medio), así como el nombre del usuario, contraseñas, firma electrónica; o cualquier otra información empleada por la persona, para su identificación en Internet u otra red de comunicaciones electrónicas; III. Datos laborales: Documentos de reclutamiento y selección, nombramiento, incidencia, capacitación, actividades extracurriculares, referencias laborales, referencias personales, solicitud de empleo, hoja de servicio, demás análogos; IV. Datos patrimoniales: Los correspondientes a bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, fianzas, servicios contratados, referencias personales, demás análogos; V. Datos sobre procedimientos administrativos y/o jurisdiccionales: La información relativa a una persona que se encuentre sujeta a un procedimiento administrativo seguido en forma de juicio o jurisdiccional en materia laboral, civil, penal, fiscal, administrativa o de cualquier otra rama del Derecho;

DCP	Ley PDPDF	Lineamientos
Categorías de datos		VI. Datos académicos: Trayectoria educativa, calificaciones, títulos, cédula profesional, certificados y reconocimientos, demás análogos; VII. Datos de tránsito y movimientos migratorios: Información relativa al tránsito de las personas dentro y fuera del país, así como información migratoria; VIII. Datos sobre la salud: El expediente clínico de cualquier atención médica, referencias o descripción de sintomatologías, detección de enfermedades, incapacidades médicas, discapacidades, intervenciones quirúrgicas, vacunas, consumo de estupefacientes, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, así como el estado físico o mental de la persona; IX. Datos biométricos: huellas dactilares, ADN, geometría de la mano, características de iris y retina, demás análogos; X. Datos especialmente protegidos (sensibles): origen étnico o racial, características morales o emocionales, ideología y opiniones políticas, creencias, convicciones religiosas, filosóficas y preferencia sexual; y XI. Datos personales de naturaleza pública: aquellos que por mandato legal sean accesibles al público.

A continuación, pasamos a valorar sucintamente el concepto de datos de carácter personal —una de las definiciones sobre las que gira la normativa— y su aplicación sustancial, a la vista de la regulación hecha tanto por la Ley como por sus Lineamientos, para, en forma posterior, expresar algunas conclusiones al respecto.

En cuanto al concepto de dato de carácter personal, cabe señalar que:

- Es información referida a una persona física identificada o identificable. Es así que los datos tienen que ponerse en relación con la persona a la que se refieren, ya que de otra manera resultan ser neutros.
- Al tratarse solamente de personas físicas, quedan excluidas las personas morales, públicas o privadas, sin perjuicio de otras protecciones que les sean conferidas, en su caso, por el ordenamiento jurídico.
- Los datos personales, conforme a los Lineamientos, pueden clasificarse atendiendo a diferentes criterios, si bien podemos distinguir básicamente entre datos sensibles y los que no lo son. En particular, esta distinción cobra relevancia en cuanto a las obligaciones que debe cumplir quien los trate, puesto que, por ejemplo, se tendrá que adoptar y aplicar el nivel alto de medidas de seguridad[131].
- Es importante tener en consideración que cuando la Ley y los Lineamientos se refieren a los datos de carácter personal, siempre lo hacen de manera enunciativa y nunca taxativa o *numerus clausus*. Esto supone que, por ejemplo, en el caso de los Lineamientos pueda considerarse la voz como dato identificativo, pese a no estar enumerado[132].

---

[131] En este sentido, los Lineamientos establecen que el nivel alto de medidas de seguridad será aplicable a *"los sistemas de datos personales que contengan datos relativos a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos."*

[132] En el ámbito internacional, volviendo de nuevo a la Directiva 95/46/CE, ésta señala que *"La*

Sistema de datos personales

La Ley y los Lineamientos, respectivamente, definen el concepto de sistema de datos personales de la siguiente manera:

LPDPDF	Lineamientos
Todo conjunto organizado de archivos, registros, ficheros, bases o banco de datos personales de los entes públicos, cualquiera que sea la forma o modalidad de su creación, almacenamiento, organización y acceso;	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 datos personales se contienen en sistemas. Los sistemas se caracterizan por ser un conjunto de datos personales organizado conforme a un criterio de búsqueda; en tanto que haya posibilidad de buscar los datos conforme a un criterio determinado, por ejemplo, apellido, identificador, etc.

Gracias a este criterio podemos encontrar y sistematizar esos datos que, por ese orden, siendo sometidos a un tratamiento, darán lugar a ese perfil de la persona, así como información personal que debemos proteger.

Es decir, si los datos no están estructurados conforme a unos parámetros de selección y búsqueda en un sistema o base de datos, sujetos a un tratamiento (automatizado o no), no se dará lugar a la información personal, pues serán únicamente datos dispersos.

Comisión estudiará, en particular, la aplicación de la presente Directiva al tratamiento de datos que consistan en sonidos e imágenes relativos a personas físicas y presentará las propuestas pertinentes que puedan resultar necesarias en función de los avances de la tecnología de la información, y a la luz de los trabajos de la sociedad de la información." (art. 33)

Conceptualmente podemos distinguir[133] entre sistemas físicos, lógicos y jurídicos. Los sistemas físicos son los sistemas en papel y/o también la ubicación física del sistema[134]. Es decir, sistema físico identifica el sistema con una ubicación geográfica. Los sistemas lógicos vienen determinados por la configuración lógica del sistema de información. Y los jurídicos se determinan por la naturaleza de los datos y la finalidad con la que éstos son tratados por el responsable del tratamiento.

En consecuencia, en realidad el interés está en determinar especialmente cuántos sistemas jurídicos[135] tenemos y aplicar las medidas legales pertinentes sobre dichos tratamientos. Determinando los sistemas jurídicos, que agrupan los datos tratados en virtud de la finalidad con la que se tratan, es posible determinar el cumplimiento de las obligaciones establecidas por la normativa aplicable.

Fuentes de acceso público

Se trata de un término utilizado en la Ley, pero definido en los Lineamientos de la siguiente manera:

> *Aquella cuya consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, sin más exigencia que, en su caso, el pago que genere el acceso a determinado medio de información. Tendrán el carácter de fuentes de acceso público los Registros Públicos, los diarios,*

---

133 Davara Rodríguez, M.A., *El abogado y la protección de datos*, Madrid: Ed. Ilustre Colegio de Abogados de Madrid, op. cit, página 25.

134 Como muy bien apunta la Resolución (73) del Comité de Ministros del Consejo de Europa, en realidad el tamaño de los ficheros no importa en absoluto, ya que pueden contener conexiones que los unan entre ellos, haciendo ficheros tan grandes como se desee:*"14. The resolution covers all data collections, irrespective of their size. It should be pointed out in this connection that computer technology makes it possible to link several small data banks into one big data bank."*

135 En definitiva, que podemos tener todo un almacén de datos, los conocidos y manejadísimos *warehouse*, y por tanto ser incluso todo un solo fichero o tratamiento lógico, y, por otro lado, poder contener a su vez diversos ficheros desde el punto de vista jurídico, tanto por los datos que se contienen, como, especialmente, la finalidad a la que se destinan dichos datos.

> *gacetas y boletines gubernamentales, así como otros medios oficiales de difusión.*

La definición es especialmente relevante pues, cuando se tratan datos que provienen de fuentes de acceso público, implica que los principios de la normativa se apliquen con excepciones. Por ejemplo, no es necesario el consentimiento del interesado para poder tratar los datos, y el principio de información también se aplica con excepciones en determinados supuestos, tal y como se analizó anteriormente.

2. Información en la recogida de datos

Los Lineamientos dedican tres numerales, del 12 al 14, al principio de información en la recogida de datos, desarrollando así lo previsto en la Ley.

Deber de información

El numeral 12 de los Lineamientos dispone lo siguiente:

> *A efecto de cumplir con el deber de información previsto en el artículo 9 de la Ley, en el momento en que se recaben datos personales, por cualquier medio, el ente público deberá hacer del conocimiento del interesado las advertencias a las que se refiere dicho artículo.*

Resulta claro que el ente público, como responsable del tratamiento, tiene que cumplir con el principio de información en el momento de recabar los datos del interesado. Como ya mencionamos, la información es un requisito casi imprescindible, salvo las tasadas excepciones que hemos visto, aun cuando no se requiera el consentimiento.

Indicamos anteriormente que la información a que se refiere la Ley tiene que proporcionarse con independencia de cuál sea el medio utilizado para su recogida. Es decir, ya sea en soporte papel o electrónico, tiene que cumplirse con este principio cuando se recaban los datos del interesado.

En cuanto a la información a proporcionar, los Lineamientos se remiten al artículo 9 de la Ley, si bien en el siguiente numeral incluyen un modelo de cláusula o leyenda informativa que permitirá a los entes públicos cumplir con la obligación de informar al interesado sobre el tratamiento de sus datos de carácter personal.

Modelo de leyenda

El modelo de leyenda que se incluye en el numeral 13 de los Lineamientos es el siguiente:

> ***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*

En concreto —como ya vimos al analizar el principio de información—, el artículo 9 de la Ley establece que el interesado tiene que ser informado previamente a la obtención de sus datos, de manera expresa, precisa e inequívoca de los siguientes aspectos:

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

A la vista de los requisitos en materia de información exigidos por la Ley, y del modelo de leyenda que el Instituto proporciona a los entes públicos del Distrito Federal a través de sus Lineamientos, es posible incluir una tabla de comprobación del cumplimiento de dichos requisitos. Así, la tabla sería la siguiente:

Información en la recogida de datos (art. 9)		
Fracción	**Requisito**	**Lineamientos**
I	Existencia del tratamiento	*"**Los datos personales recabados serán protegidos, incorporados y tratados en el Sistema de Datos Personales** (nombre del sistema de datos personales), …"*
	Finalidad del tratamiento	*"…**cuya finalidad es** (describir la finalidad del sistema) …"*
	Destinatarios de la información	*"… **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**…"*
II	Carácter obligatorio o facultativo de las respuestas	*"**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)..."*
III	Consecuencias de la obtención de los datos o de la negativa a suministrarlos	*"… **sin ellos no podrá acceder al servicio o completar el trámite** (indicar el servicio o trámite de que se trate)…"*
IV	Consentimiento expreso para la cesión de datos	*"**Asimismo, se le informa que sus datos no podrán ser difundidos sin su consentimiento expreso, salvo las excepciones previstas en la Ley**…"*
V	Posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición	*"… **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)…"*
VI	Nombre del responsable del sistema de datos personales y de los destinatarios	*"**El responsable del Sistema de datos personales es** (nombre del responsable),..."*

Por tanto, el ente público podrá hacer uso del modelo de leyenda que se proporciona en los Lineamientos, adecuándolo a las necesidades específicas del tratamiento que vaya a llevar a cabo, cumpliendo de este modo con los requerimientos legales.

Evidentemente, a nadie se le escapa que definir la finalidad del tratamiento es la parte más complicada y "sensible", porque determinará claramente la validez y adecuación del tratamiento posterior. De cualquier modo, es algo que se tiene que delimitar tratamiento por tratamiento, caso por caso, sin que sea de ninguna manera posible proporcionar un ejemplo o modelo al respecto.

Por otro lado, si los datos no hubieran sido obtenidos del propio interesado, sino a través de un tercero, y siempre y cuando el interesado no haya sido informado con anterioridad, entonces la cláusula o leyenda informativa tiene que incluir los numerales que se indican a continuación, conforme a lo dispuesto en el artículo 9 de la Ley:

> 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;
>
> […]
>
> 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.

Excepciones al deber de información

Los Lineamientos también prevén excepciones al deber de información. En concreto, en su numeral 14 indican lo siguiente:

> En el caso de datos personales que no hayan sido obtenidos directamente del interesado, no habrá obligación de cumplir con el deber de información cuando resulte material o jurídicamente imposible o requiera de esfuerzos desproporcionados, en razón del número de interesados y/o la antigüedad de los datos.

En definitiva, las excepciones contempladas en los Lineamientos se refieren al supuesto en el que los datos no hayan sido recabados directamente del interesado. De ser así, el ente público no tendrá que informar al interesado de la recogida y tratamiento de sus datos cuando dicha obligación:

1. Resulte material o jurídicamente imposible, o
2. Requiera de esfuerzos desproporcionados, en razón del

   a) Número de interesados y/o
   b) La antigüedad de los datos.

A pesar de que reiteramos nuestros comentarios acerca de la indeterminación de los conceptos jurídicos utilizados, lo cierto es que los Lineamientos dan un paso más y procuran delimitar en la medida de lo posible dicha indefinición, al proponer los parámetros de número de interesados y antigüedad de los datos, aunque, claro, vuelven a ser de algún modo indeterminados, pues dependerá del caso en concreto.

3. Medidas de seguridad

Las medidas de seguridad son desarrolladas en los numerales 15 a 17 de los Lineamientos.

En concreto, el numeral 15 está dedicado a cuestiones generales sobre las medidas de seguridad; el numeral 16 detalla las medidas de seguridad aplicables por cada uno de los niveles establecidos por la Ley (básico, medio y alto); y el numeral 17 se refiere a la notificación de las medidas de seguridad al Instituto.

Cuestiones generales sobre las medidas de seguridad

El Capítulo de los Lineamientos dedicado a las medidas de seguridad comienza con el numeral 15, que establece:

> Las medidas de seguridad aplicables a los sistemas de datos personales responderán a los niveles establecidos en la Ley para cada tipo de datos. Dichas medidas deberán tomar en consideración las recomendaciones, que en su caso, emita el Instituto para este fin, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento.

De lo indicado en el numeral, resulta relevante lo siguiente:

2. *Niveles de medidas de seguridad aplicables*: conforme a lo dispuesto en la Ley son básico, medio y alto.

3. *Recomendaciones del Instituto*: el numeral prevé que las medidas de seguridad se adoptarán teniendo *"en consideración las recomendaciones, que en su caso, emita el Instituto para este fin, con el objeto de garantizar la confidencialidad, integridad y disponibilidad de los datos personales durante su tratamiento"*.

   La emisión de recomendaciones está sujeta a determinación del InfoDF, pero no implican necesariamente una obligación. Las recomendaciones podría devenir también después de aplicar la atribución del InfoDF de inspeccionar algún sistema de datos personales en el que se hayan detectado irregularidades en el documento de seguridad empleado por el responsable del sistema.

   Determinando los sistemas jurídicos, que agrupan los datos tratados en virtud de la finalidad con la que se tratan, es posible determinar el cumplimiento de las obligaciones establecidas por la normativa aplicable.

Niveles de seguridad

Tal y como establece la Ley, los niveles de seguridad se dividen en tres: básico, medio y alto.

Estos niveles de seguridad se aplican atendiendo a la naturaleza de los datos personales que sean objeto de tratamiento en el sistema de datos personales.

En concreto, el numeral 16, que detalla las medidas de seguridad aplicables por cada uno de los niveles, indica lo siguiente en relación con los tres niveles de medidas de seguridad mencionados:

I. **Nivel Básico**.- El nivel de seguridad básico es aplicable a todos los sistemas de datos personales.

II. **Nivel Medio.** El nivel de seguridad medio es aplicable a los sistemas de datos personales relativos a la comisión de infracciones administrativas o penales, hacienda pública, servicios financieros, datos patrimoniales, así como a los sistemas que contengan datos de carácter personal suficientes que permitan obtener una evaluación de la personalidad del individuo.

III. **Nivel Alto.** El nivel de seguridad alto es aplicable a los sistemas de datos personales que contengan datos relativos a la ideología, religión, creencias, afiliación política, origen racial o étnico, salud, biométricos, genéticos o vida sexual, así como los que contengan datos recabados para fines policiales, de seguridad, prevención, investigación y persecución de delitos.

Medidas de seguridad

A continuación, el citado numeral detalla las medidas de seguridad aplicables en cada uno de los niveles de medidas de seguridad ya indicados.

Así y de manera meramente enunciativa, las medidas de seguridad por cada uno de los niveles previstas en los Lineamientos, conforme a lo dispuesto en la Ley, son las siguientes[136]:

Nivel básico	Nivel medio	Nivel alto
Documento de seguridad		
Funciones y obligaciones del responsable, encargado y de toda persona que intervenga en el tratamiento de los sistemas de datos personales		
Registro de incidencias		
Identificación y autenticación		
Control de acceso		
Gestión de soportes		
Copias de respaldo y recuperación		
	Responsable de seguridad	
	Auditoría	
	Control de acceso físico	
	Pruebas con datos reales	
		Distribución de soportes
		Registro de acceso
		Telecomunicaciones

Cabe recordar aquí que los niveles de seguridad son acumulables, de manera que el nivel medio tendrá que cumplir con las medidas de seguridad de nivel básico y, a su vez, el nivel alto tendrá que cumplir con las medidas de seguridad de nivel medio y básico.

Y por lo que se refiere a las medidas de seguridad en sí, a continuación se comentan brevemente.

- Documento de seguridad: El ente público, como responsable del tratamiento, *"elaborará, difundirá e implementará la normativa de seguridad mediante el documento de*

[136] Las medidas de seguridad previstas en los Lineamientos parecen seguir, casi literalmente, las que establecía en España el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad, ya derogado por el Real Decreto 1720/2007.

seguridad que será de observancia obligatoria para todos los servidores públicos del ente público, así como para toda aquella persona que debido a la prestación de un servicio tenga acceso a los sistemas de datos personales y/o al sitio donde se ubican los mismos".

El documento se convierte en el instrumento que recoge las medidas de seguridad, con independencia de cuál sea el nivel de medidas de seguridad aplicable, siguiendo la estructura mínima prevista en los Lineamientos.

Por último, es necesario recordar que el documento tiene que actualizarse cada vez que se produzcan cambios relevantes en el tratamiento y, al menos, una vez cada año.

- Funciones y obligaciones del responsable, encargado[137] y de toda persona que intervenga en el tratamiento de los sistemas de datos personales: Las funciones y obligaciones de quienes traten datos de carácter personal estarán claramente definidas y recogidas en el documento de seguridad.

  El responsable del tratamiento tiene que adoptar las medidas necesarias para dar a conocer las funciones y obligaciones al personal, así como las consecuencias en caso de incumplimiento. Por tanto, el responsable tiene la obligación de formar e informar a quienes tienen acceso a datos de carácter personal sobre la necesidad de observar y cumplir las medidas de seguridad.

- Registro de incidencias: Los Lineamientos, en su numeral 3, fracción X, definen el concepto de incidencia como: *"cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales"*.

---

[137] El apartado 16.I.b) de los Lineamientos se refiere expresamente al responsable y al encargado, si bien conforme al apartado 39, tal y como veremos más adelante, entendemos que el encargado es el usuario por ser éste una persona física o moral externa al ente público que presta un servicio que implica el tratamiento de datos. Es decir, las medidas de seguridad serán adoptadas por el responsable y el usuario, según los términos de la ley, que son quienes tratan datos de carácter personal.

Las incidencias constarán en un registro que contenga la siguiente información:

Tipo de incidencia.
Momento en que se ha producido.
Persona que realiza la notificación.
A quién se le comunica.
Efectos que se hubieran derivado de la misma.
Acciones implementadas.

Puesto que los Lineamientos no establecen nada al respecto y tampoco se han publicado recomendaciones sobre cómo cumplir con esta medida de seguridad, es posible señalar que el registro de incidencias puede encontrarse tanto en soporte papel como electrónico.

- Identificación y autenticación: Mediante la identificación se reconoce a un operario y mediante la autenticación se comprueba que es quién dice ser. La identificación y la autenticación pueden estar basadas en el uso de nombres de usuario y contraseñas respectivamente. En el caso de las contraseñas será necesario establecer un procedimiento de asignación, distribución y almacenamiento que garantice su integridad y confidencialidad.

  Además, el documento de seguridad contendrá una relación actualizada de operarios autorizados para acceder a los sistemas de datos personales.

- Control de acceso: El responsable adoptará medidas para garantizar que únicamente quienes estén autorizados para ello tengan acceso.
- Gestión de soportes: Los soportes, físicos o electrónicos, que contengan datos de carácter personal tendrán que estar etiquetados para identificar su contenido y ser inventariados. Además, la salida de soportes con información deberá ser autorizada por el responsable o estar autorizada en el documento de seguridad.

- Copias de respaldo y recuperación: En el caso de la digitalización de documentos para realizar copias de respaldo de documentos, es necesario garantizar la integridad de la información, evitando que se produzca alguna alteración o pérdida como consecuencia de dicha digitalización.
- Responsable de seguridad: los Lineamientos definen al responsable de seguridad como la *"persona a la que el responsable del sistema de datos personales asigna formalmente la función de coordinar y controlar las medidas de seguridad aplicables"*. La designación del responsable no supone delegación alguna de responsabilidad, que en todo caso corresponde en última instancia al responsable del sistema de datos de carácter personal.
- Auditoría: La auditoría de las medidas de seguridad, interna o externa, se llevará a cabo bienalmente. Como resultado de la auditoría se elaborará un informe que dictaminará la adecuación de las medidas conforme a los Lineamientos y, en su caso, las Recomendaciones emitidas por el Instituto.

  Además, el informe de auditoría identificará las deficiencias encontradas y las medidas preventivas, correctivas o complementarias que el auditor haya planteado. Dicho informe tendrá que ser comunicado al Instituto en el plazo de 20 días hábiles.

- Control de acceso físico: Únicamente las personas autorizadas en el documento de seguridad podrán acceder a las instalaciones donde se encuentren los sistemas de datos personales.
- Pruebas con datos reales: Sólo podrán llevarse a cabo cuando se garantice el cumplimiento de las medidas de seguridad correspondientes al nivel de seguridad aplicable y se realice previamente una copia de respaldo.
- Distribución de soportes: Tal y como indican los Lineamientos, cuando se distribuyan soportes con datos personales *"se realizará cifrando dichos datos, o bien*

utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su traslado o transmisión."

- Registro de acceso: El registro estará bajo el control directo del responsable de seguridad y guardará, al menos, la identificación del operario, la fecha y hora en que se realizó, el sistema accedido, el tipo de acceso y si éste fue autorizado o denegado. No podrá ser desactivado ni manipulado por terceros en ningún momento.
- Telecomunicaciones: Cuando se utilicen redes públicas de comunicaciones electrónicas, los datos tendrán que viajar cifrados o utilizando otro mecanismo que garantice la confidencialidad de la información.

Notificación del nivel de seguridad

El numeral 17 de los Lineamientos indica lo siguiente:

> Los responsables sólo deberán comunicar al Instituto el nivel de seguridad aplicable a los sistemas de datos personales para su registro.

Lo dispuesto en este numeral implica lo siguiente:

1. *Sólo el nivel de seguridad*: Entendiendo que el nivel de medidas de seguridad (básico, medio o alto) aplicable, atendiendo a la naturaleza de los datos que sean objeto de tratamiento en el sistema de datos personales, se notifica al Instituto mediante el acuerdo de creación de éste.

   Así lo prevé el numeral 7 de los Lineamientos, al indicar que dicho acuerdo deberá contener la *"indicación del nivel de seguridad que resulte aplicable: básico, medio o alto"*.

   Además de lo anterior, el nivel de medidas de seguridad también se indicará en el contenido del registro del sistema

de datos personales. Es decir, se trata de uno de los campos disponibles conforme a lo dispuesto en la fracción X, del numeral 11.

2. *El documento de seguridad quedará a disposición del Instituto*: El hecho de que el ente público tenga que comunicar al Instituto el nivel de seguridad no exime de otras obligaciones. Es así que el documento de seguridad, así como cualquier otra documentación relativa a la adopción y cumplimiento de las medidas de seguridad, tales como los informes de auditoría, quedarán a disposición del Instituto, que podrá revisarlos en cualquier momento para asegurarse de que el responsable cumple con sus obligaciones, en virtud de la Ley y su normativa de desarrollo.

4. Principios de la protección de datos

El Capítulo III del Título Segundo de los Lineamientos está dedicado a los principios que rigen en el tratamiento de datos de carácter personal. Dichos principios, tal y como establece el numeral 18 de los Lineamientos, son básicamente los de: *"licitud, consentimiento, calidad de los datos, confidencialidad, seguridad, disponibilidad y temporalidad que establece el artículo 5 de la Ley."*

A continuación, se analizan cada uno de estos principios conforme a lo dispuesto en los Lineamientos.

Licitud

Según los Lineamientos, la licitud[138] comprende una doble vertiente.

---

[138] A nivel internacional, en relación con la licitud del tratamiento, podemos destacar el considerando 28 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre, 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, publicada en el Diario Oficial de la Unión Europea serie L, número 281, de 23 de noviembre. En concreto, el citado considerando indica lo siguiente: "(28)

Así, por un lado es necesario considerar la licitud en cuanto a la finalidad con la que se tratan los datos. En este sentido, *"se considerará que la finalidad es distinta o incompatible cuando el tratamiento de los datos personales no coincida con los motivos para los cuales fueron recabados"*, tal y como indica el numeral 19.I de los Lineamientos.

Y por otro lado, la licitud referida a la obtención y tratamiento de los datos. Al respecto, el numeral 29 establece que el Instituto podrá *"requerir, mediante resolución fundada y motivada del Pleno, que los responsables de sistemas de datos personales suspendan la utilización o cesión de determinados datos."*

Si el requerimiento no fuera atendido, *"el Instituto, mediante resolución fundada y motivada del Pleno, podrá requerir la inmovilización del sistema correspondiente"*. Dicha inmovilización del sistema, ordenada por el Instituto conforme al numeral 30, busca restituir los derechos de los interesados.

Consentimiento

En relación con el consentimiento, consideramos oportuno incluir una tabla que resume las previsiones de los Lineamientos en relación con este principio de la protección de datos:

Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal con respecto al interesado; que debe referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos, y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados."

Características del consentimiento (numeral 19.II)	• **Libre**: Cuando es obtenido sin la intervención de vicio alguno de la voluntad; • **Inequívoco**: Cuando existe expresamente una acción que implique su otorgamiento; • **Específico**: Cuando se otorga referido a una determinada finalidad; e • **Informado**: Cuando se otorga con conocimiento de las finalidades para las que el mismo se produce.
Necesidad del consentimiento para la obtención de los datos (numeral 23)	• **Regla general**: El responsable deberá obtener el consentimiento del interesado para el tratamiento de sus datos personales. • **Excepciones**: Supuestos previstos en el artículo 16 de la LPDPDF.
Necesidad del consentimiento para la cesión de los datos (numeral 24)	El interesado deberá ser informado de forma que conozca inequívocamente: • la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento, así como • el tipo de actividad desarrollada por el cesionario.
Obtención del consentimiento de menores o incapaces (numeral 25)	El responsable, o en su defecto, el encargado, deberá cerciorarse de que quien otorga el consentimiento es la persona que ejerce la patria potestad, tutela o la representación legal del menor o incapaz de que se trate en términos del Código Civil para el Distrito Federal.
Forma de recabar el consentimiento (numeral 26)	• ¿Quién lo obtendrá?: El responsable. • ¿En qué forma?: Por escrito. • ¿A través de qué medios?: En el domicilio del ente público. Por correo electrónico. Por correo certificado. • Plazo: El interesado tendrá un plazo de quince días hábiles para manifestar su negativa al tratamiento. • Excepciones a los apartados anteriores: Casos previstos en el artículo 16 de la LPDPDF. Sistemas creados con anterioridad a la entrada en vigor de la LPDPDF.

Revocación del consentimiento (numeral 27)	• Requisitos: De conformidad con lo dispuesto en el artículo 16 de la LPDPDF. Los establecidos en el artículo 34 de la LPDPDF. Especificando la finalidad para la cual se revoca el consentimiento para tratar los datos personales. Acompañando la solicitud de un medio de identificación oficial. • ¿Ante quién?: Ante la Oficina de Información Pública que corresponda. • Forma: A través de los formatos que para tal efecto emita el Instituto.
Efectos de la revocación (numeral 28)	• Si resulta procedente: El responsable deberá cesar en el tratamiento de los datos, lo cual supondrá su bloqueo conforme a la LPDPDF y los Lineamientos. • Si no resulta procedente: El interesado podrá ejercitar su derecho de cancelación, en los casos que ésta resulte procedente, de conformidad con la Ley y los Lineamientos. • Si los datos se hubieran cedido previamente: El responsable deberá comunicarlo a los cesionarios en el plazo de diez días hábiles para que procedan en el mismo sentido.

Calidad de los datos

El análisis del principio de calidad de los datos en los Lineamientos comienza con lo dispuesto en el numeral 19.III, que indica que el dato que sea objeto de tratamiento deberá ser:

a) Cierto: Cuando los datos se mantienen actualizados de tal manera que no se altere la veracidad de la información que traiga como consecuencia que el titular se vea afectado por dicha situación;

b) Adecuado: Cuando se observa una relación proporcional entre los datos recabados y la finalidad del tratamiento;

c) Pertinente: Cuando es realizado por el personal autorizado para el cumplimiento de las atribuciones de los entes públicos que los hayan recabado; y

d) No excesivo: Cuando la información solicitada al titular de los datos es la estrictamente necesaria para cumplir con los fines para los cuales se hubieran recabado.

En concreto, los Lineamientos inciden en dos aspectos claves en relación con la calidad de los datos. Por un lado, la determinación de la finalidad con la que serán tratados los datos y, por otro lado, la actualización del dato que es objeto del tratamiento.

En cuanto al primero de los aspectos indicados, la finalidad del tratamiento, el numeral 21 indica que los datos personales en posesión de los entes públicos deberán tratarse únicamente para la finalidad para la cual fueron obtenidos, lo que debe ponerse en relación con el principio del consentimiento.

Además, dicha finalidad debe ser:

- Explícita;
- Determinada, y
- Legal.

Sólo así podrá garantizarse un tratamiento legal y leal de los datos.

Y, por otro lado, el deber de actualización, que conforme al numeral 22 implica lo siguiente:

- Datos exactos y actualizados: Los datos deberán ser exactos y actualizarse en caso de que fuera necesario para responder con veracidad a la situación actual del titular.

- Datos inexactos o incompletos: El responsable los actualizará de oficio en el momento que tenga conocimiento de la inexactitud, siempre que cuente con la documentación que justifique la actualización.
- Datos cedidos previamente: El responsable deberá comunicar a los cesionarios la rectificación efectuada en el plazo de diez días hábiles.

Confidencialidad

Los Lineamientos, en su numeral 20, recuerdan que tanto el responsable como toda persona que intervenga en cualquier fase del tratamiento de datos personales en posesión de los entes públicos, están sujetos al deber de confidencialidad.

Dicho deber supone una obligación de *"guardar absoluta confidencialidad respecto de los mismos, obligación que subsistirá aun después de finalizada la relación por la cual se dio el tratamiento."*

Además, este deber de confidencialidad o secrecía es específico en protección de datos —en forma independiente de cualquier otra obligación que deba cumplir quien trate datos en virtud del desarrollo de sus funciones, como, por ejemplo, podría ser el juramento hipocrático que recae sobre los doctores y otro personal sanitario en un hospital público— y sería distinto al deber de confidencialidad respecto al acceso que tengan a datos de carácter personal.

Seguridad

Si los datos hubieran sido cedidos, el numeral 34 indica que se analizará el carácter adecuado de las medidas de seguridad ofrecidas por el cesionario, atendiendo en particular a los siguientes aspectos:

- La naturaleza de los datos personales;
- La finalidad del tratamiento, y
- La duración del tratamiento.

Con relación a las medidas de seguridad a adoptar respecto al tratamiento de datos en los sistemas de información, nos remitimos a lo ya analizado con anterioridad para evitar reiteraciones innecesarias.

Disponibilidad

La disponibilidad de la información viene en gran parte dada por el cumplimiento de los principios de la protección de datos. Es decir, los datos estarán disponibles cuando sean tratados de manera que se observen los principios por quien correspondan, y en particular los relativos a la calidad y seguridad de los datos. Por tanto, resulta necesario organizar el sistema de manera que permita un acceso sin dilaciones a los datos, lo que se conseguirá observando los principios de la protección de datos, así como aquella otra normativa supletoria que pudiera resultar aplicable.

Por tanto, la disponibilidad de la información pasa previamente por el análisis de los principios aplicables en protección de datos, conforme a lo dispuesto en la Ley y en los Lineamientos.

Temporalidad

En relación con la temporalidad del tratamiento, cobra especial relevancia la cancelación de los datos. Al respecto, es necesario atender lo dispuesto en los numerales 31 y 32, que tratan respectivamente de la cancelación de los datos y los plazos para llevarla a cabo.

Así, el numeral 31, puede esquematizarse de la siguiente manera:

- Norma general: "*Los datos de carácter personal serán cancelados, de oficio o a petición del interesado, una vez que hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hayan sido recabados*."
- Excepción:

  Los datos deberán ser conservados "*durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica, o de la ejecución de un contrato*".

  Una vez cumplidos los plazos anteriores "*los datos sólo podrán conservarse previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley y estos Lineamientos*."

Por último, el numeral 32 se refiere a los plazos de cancelación, estableciendo que si los datos hubieran sido objeto de tratamiento y ya no tuvieran valores históricos, científicos o estadísticos, serán cancelados conforme a los siguientes plazos:

I. El que se haya establecido en el formato físico o electrónico por medio del cual se recabaron;
II. El establecido por las disposiciones aplicables; y
III. El establecido en el instrumento jurídico formalizado entre un tercero y el ente público.

5. Obligaciones de los entes públicos

El Capítulo Cuarto del Título Segundo, relativo a la tutela de datos personales, está dedicado a las obligaciones de los entes públicos.

Los numerales 35 a 39 de los Lineamientos se refieren a las obligaciones de los entes públicos, ya que éstos están en posesión de los datos personales y por ello se encuentran sujetos a lo dispuesto en la Ley y sus Lineamientos respecto a los principios, derechos y procedimiento en materia de protección de datos de carácter personal[139].

En concreto, las materias objeto de estos numerales de los Lineamientos son las siguientes:

- Obligaciones de quienes tratan datos de carácter personal (aptdo. 35)
- Tratamiento por usuarios (aptdo. 36)
- Informe anual (aptdo. 37)
- Enlace (aptdo. 38)
- Encargado (aptdo. 39)

Obligaciones de quienes tratan datos de carácter personal

El numeral 35 de los Lineamientos se refiere a las obligaciones que tienen que cumplir los responsables, encargados y usuarios, en el tratamiento de datos de carácter personal.

A efectos de los Lineamientos, las figuras de los responsables y encargados son definidas de la siguiente manera:

> Encargado: Servidor público que en ejercicio de sus atribuciones, realiza tratamiento de datos personales de forma cotidiana. (Numeral 3, fracción VII)
>
> Enlace: Servidor público que fungirá como vínculo entre el ente público y el Instituto para atender los asuntos relativos a la Ley de la materia. (Numeral 3, fracción VIII)

[139] Nos remitimos a lo ya comentado al analizar la Ley en relación con la definición de ente público y el objeto de la Ley conforme a lo dispuesto en su artículo 1.

> Responsable: El 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. (Numeral 3, fracción XVI)

En el caso del usuario, es necesario remitirse al artículo 2 de la LPDPDF, ya que los Lineamientos no lo definen. En concreto, el citado artículo de la Ley define al usuario de la siguiente manera:

> Usuario. Aquel autorizado por el ente público para prestarle servicios para el tratamiento de datos personales.

La siguiente tabla resume las obligaciones establecidas en el numeral de los Lineamientos que comentamos:

Figura	Obligación
Responsable	• Cumplir con lo dispuesto en la Ley, los Lineamientos y el documento de seguridad aplicable para cada sistema de datos personales.
Encargado	• Cumplir con lo dispuesto en la Ley, los Lineamientos y el documento de seguridad aplicable para cada sistema de datos personales.
Usuario	• Cumplir con lo dispuesto en la Ley, los Lineamientos y el documento de seguridad aplicable para cada sistema de datos personales.
Titular del ente público	• Designará al o los servidores públicos responsables de los sistemas de datos personales, quienes deberán estar adscritos a la unidad administrativa en la que se concrete la competencia material del sistema. • Designará al servidor público que fungirá como enlace entre el ente y el Instituto.
Enlace	• Fungirá como enlace entre el ente y el Instituto. • Coordinará a los responsables de los sistemas de datos personales al interior del ente público.

Tratamiento por usuarios

Siendo el usuario, conforme a lo dispuesto en el numeral 39 de los Lineamientos, *"aquella persona física o moral externa al ente público que le presta servicios para tratar datos personales o que implica el tratamiento de los mismos"*, el tratamiento deberá estar regulado en un contrato que cumpla con los siguientes requisitos:

1. Deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido;

2. El usuario:
   a) únicamente tratará los datos conforme a las instrucciones del responsable;
   b) no los aplicará o utilizará con una finalidad distinta a la que figura en el contrato,
   c) ni los comunicará a otras personas.

3. Estipulará las medidas de seguridad que se deban implementar.

4. Una vez concluida la relación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable.

En definitiva, el contrato tiene que prever todos los aspectos del tratamiento de datos de carácter personal, a efectos de garantizar el cumplimiento de los principios y las obligaciones exigibles en materia de protección de datos tanto para el ente público, ya que es el poseedor de los datos, como para el usuario, que tiene acceso a éstos para prestarle un servicio.

Informe anual

Por lo que se refiere al informe anual, los Lineamientos desarrollan lo dispuesto en la fracción III, del artículo 21, de la LPDPDF[140] y establecen que aquél incluirá los siguientes apartados:

I. Número de solicitudes de acceso, rectificación, cancelación y oposición de datos personales presentadas ante el ente público, así como su resultado;
II. El tiempo de respuesta a la solicitud;
III. El estado que guardan las denuncias presentadas ante los órganos internos de control, así como de las vistas dadas por el Instituto;
IV. Dificultades observadas en el cumplimiento de la Ley;
V. Descripción de los recursos públicos utilizados en la materia;
VI. Sistemas de datos personales creados, modificados y/o suprimidos;
VII. Acciones desarrolladas para dar cumplimiento a las disposiciones contenidas en la Ley; y
VIII. Cesiones de datos personales efectuadas que deberá detallar:

a) Identificación del sistema mediante número de folio otorgado por el Instituto, del ente cedente y del cesionario;

b) Finalidad de la cesión;

c) La mención de si se trata de una cesión total o parcial de un sistema de datos personales y, en su caso, las categorías de datos de que se trate;

---

[140] En concreto, el citado artículo de la Ley establece lo siguiente:
Artículo 21.- El titular del ente público designará al responsable de los sistemas de datos personales, mismo que deberá:
[…]
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.
En cuanto a la responsabilidad por omitir el informe, el artículo 41 de la Ley, que tipifica las infracciones, indica que constituirá infracción: *"IX. Omitir o presentar de manera extemporánea los informes a que se refiere la presente Ley."*

d) Fecha de inicio y término de la cesión y, en su caso, la periodicidad de la misma;

e) Medio empleado para realizar la cesión;

f) Medidas y niveles de seguridad empleados para la cesión;

g) Obligaciones al término del tratamiento; y

h) El nivel de seguridad aplicado por el cesionario.

Por tanto, se trata de una especie de memoria detallada que se centra en las siguientes cuestiones:

- *Estadísticas:* Número de solicitudes de acceso, rectificación, cancelación y oposición así como el resultado de éstas. Además, el tiempo de respuesta a la solicitud del interesado.
- *Denuncias:* Estado de las denuncias y vistas realizadas por el Instituto.
- *Cumplimiento de la Ley:*

  Dificultades observadas para su cumplimiento.
  Acciones desarrolladas para dar cumplimiento a la Ley.

- *Recursos públicos:* Utilizados respecto a protección de datos.
- *Sistemas de datos personales:* Creados, modificados y/o suprimidos.
- *Cesiones de datos:* Detallando la información establecida por los Lineamientos en relación con cada una de ellas.

Enlace

El numeral 38 de los Lineamientos se refiere a las obligaciones del enlace entre el ente público y el Instituto. En concreto, el numeral

establece las siguientes obligaciones a cumplir por quien sea designado como enlace:

I. Coordinar a los responsables de sistemas de datos personales al interior del ente público para el cumplimiento de la Ley, los Lineamientos y demás normativa aplicable;
II. Supervisar que los responsables mantengan actualizada la inscripción de los sistemas bajo su responsabilidad en el Registro electrónico creado por el Instituto;
III. Coordinar las acciones en materia de capacitación; y
IV. Remitir el informe a que hace referencia la fracción III del artículo 21 de la Ley.

A la vista de este numeral, el enlace desempeñará funciones de coordinación, supervisión y remisión de información, tanto internamente como en relación con el Instituto.

Es así que el enlace:

- Coordinará:

  a los responsables de los sistemas de datos, en lo que se refiere al cumplimiento de la normativa sobre protección de datos; y

  las acciones de capacitación en materia de protección de datos en el ente público.

- Supervisará: que los responsables mantengan actualizada la relación de sistemas inscritos en el Instituto.
- Remitirá: el informe anual al Instituto.

Por último, tal y como indicaba el numeral 35, el enlace será designado por el titular del ente público.

Encargado

El numeral 39, relativo al encargado, resulta clave para la interpretación de la Ley y los Lineamientos.

En concreto, se definen aquí las figuras del "encargado" y del "usuario" en los siguientes términos:

- Encargado: una persona que labore en el ente público.
- Usuario: aquella persona física o moral externa al ente público que le presta servicios para tratar datos personales o que implica el tratamiento de los mismos.

Es decir, el encargado forma parte del personal del ente público que tiene acceso a datos de carácter personal para el desarrollo de sus funciones, y el usuario es una tercera persona, física o moral, que accederá a datos del ente para prestarle un servicio. El acceso es por tanto necesario para prestar el servicio de que se trate, como por ejemplo, alojamiento de bases de datos, reparación de equipos informáticos que contengan datos de carácter personal, etc.

El numeral añade que *"[e]l acceso a los sistemas de datos personales por parte de la persona encargada del tratamiento, no se considerará una cesión o delegación de responsabilidades por parte del responsable del sistema."* Entendiendo que la referencia está hecha al encargado, la responsabilidad sobre el incumplimiento de la Ley y los Lineamientos recae sobre el responsable del sistema y, en última instancia, sobre el ente público por ser quien posee los datos conforme a lo dispuesto en el objeto de la Ley.

Por último, en relación con el usuario debe tenerse en consideración, de nuevo, lo dispuesto en el numeral 36 en cuanto al contenido del contrato que debe existir entre el ente público y el usuario, a efectos del tratamiento de los datos de carácter personal.

6. Derechos en protección de datos y procedimiento

Los Lineamientos dedican el Título Cuarto a los derechos de acceso, rectificación, cancelación y oposición y al procedimiento para su ejercicio. En concreto, los numerales 42 a 52 se refieren a cada uno de estos derechos y profundiza en el procedimiento a seguir por el interesado y el responsable para su ejercicio y atención.

El análisis de este Título, siguiendo los Lineamientos, se divide en: cuestiones generales sobre el procedimiento; derecho de acceso; derecho de rectificación; derecho de cancelación y derecho de oposición.

Cuestiones generales sobre el procedimiento

En relación con los derechos y el procedimiento para su ejercicio, conforme a lo dispuesto en los Lineamientos, y remitiéndonos al análisis ya realizado de los artículos correspondientes en la Ley para un mayor detenimiento, en términos generales es posible señalar lo siguiente:

1. *Los derechos son personalísimos:* Esto supone que sólo puedan ser ejercitados por el interesado o su representante legal. Se ejercitarán ante el responsable del tratamiento o del sistema de datos personales, por conducto de la Oficina de Información Pública de cada ente.

2. *La atención al ejercicio de los derechos se llevará a cabo a través de INFOMEX*[141]*:* Puesto que, entre otros, este sistema

---

[141] Conforme a la fracción XI, del apartado 3, de los Lineamientos, INFOMEX es el:

> **Sistema electrónico mediante el cual las personas podrán presentar sus solicitudes** de acceso a la información pública y **de acceso, rectificación, cancelación y oposición de datos personales** y es el sistema único para el registro y captura de todas las solicitudes recibidas por los entes públicos a través de los medios señalados en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal y la Ley de

permite a los entes públicos, como sujetos obligados por la Ley, atender las solicitudes de acceso, rectificación, cancelación y oposición de los interesados.

Tal y como veremos al analizar cada uno de los derechos de manera específica, el InfoDF ha publicado en su sitio web los formatos para realizar las solicitudes de acceso, rectificación, cancelación y oposición[142].

Es importante tener en consideración que INFOMEX resulta un sistema complementario a lo dispuesto en la Ley y los Lineamientos para aquellos entes públicos que se encuentran sujetos a la LPDPDF. Es decir, la atención al ejercicio de los derechos por los entes públicos tiene que cumplir con los requisitos establecidos por la Ley, sus Lineamientos y, además, llevarse a cabo conforme a INFOMEX.

3. *La Oficina de Información Pública[143] atenderá el ejercicio de los derechos:* En caso de que la solicitud que se le dirija no se refiera al acceso, rectificación, cancelación u oposición, sino a información pública, deberá orientar al solicitante.

   Dicha Oficina, conforme a lo dispuesto en la Ley, es la designada para recibir las solicitudes de ejercicio de los derechos en protección de datos.

Protección de Datos Personales para el Distrito Federal, así como para la recepción de los recursos de revisión interpuestos a través del propio sistema.

142 En este sentido, con carácter general en cuanto a los formatos para el ejercicio de los derechos, véase la siguiente dirección de Internet en la que se encuentra un enlace a éstos http://www.infodf.org.mx/web/index.php?option=com_content&task=view&id=412&Itemid=313.

143 Siendo definida ésta por el artículo 2 de la LPDPDF como:

> La unidad administrativa receptora de las solicitudes de acceso, rectificación, cancelación y oposición de datos personales en posesión de los entes públicos, a cuya tutela estará el tramite de las mismas, conforme a lo establecido en esta Ley y en los lineamientos que al efecto expida el Instituto.

A continuación, tal y como se indicó anteriormente, se atiende específicamente a cada uno de los derechos en protección de datos reconocidos por la Ley.

Derecho de acceso

Como ya indicamos al analizar el derecho de acceso en la Ley, éste tiene por objeto que el interesado pueda obtener información sobre:

1. Sus datos de carácter personal sometidos a tratamiento.
2. La finalidad del tratamiento que, en su caso, se realice.
3. La información disponible sobre el origen[144] de dichos datos.
4. Las comunicaciones realizadas o previstas de los mismos.

Tal y como prevé el segundo párrafo del numeral 44 de los Lineamientos, el interesado que ejercite el derecho de acceso podrá obtener información relativa a:

- Datos concretos;
- Datos incluidos en un determinado sistema;
- La totalidad de los datos sometidos a tratamiento en los sistemas de datos personales en posesión de un ente público.

[144] Nótese que origen no significa necesariamente procedencia. Es decir, el origen puede ser una fuente de acceso público pero los datos pueden proceder de un tercero, un cedente, que los obtuvo a su vez de aquella fuente.

El interesado debe poder saber en todo momento quién es el responsable del tratamiento, a efectos de poder dirigirse a éste para ejercitar su derecho de acceso. Por tanto, será a través de la información que reciba el interesado en el momento de que se recaben sus datos como podrá dirigirse al responsable y obtener la información sobre el tratamiento de sus datos personales en virtud de este derecho.

Por último, queremos señalar que el INFODF ha publicado en su sitio web el formato para realizar una solicitud de acceso a datos personales[145]. Esta solicitud es un modelo dirigido a los entes públicos sujetos a la LPDPDF, de manera que éstos podrán establecer un procedimiento estandarizado que les permita cumplir con todos los requisitos de la Ley y los Lineamientos en materia del ejercicio del derecho de acceso y su atención.

Derecho de rectificación

Tal y como establece la Ley y ya comentamos anteriormente, el derecho de rectificación permite al interesado instar al responsable del sistema de datos a rectificar aquellos que resulten inexactos o incompletos.

En virtud del ejercicio del derecho de rectificación, el interesado podrá controlar que los datos sobre su persona que sean tratados estén actualizados y se ajusten a la realidad, cumpliendo así, por tanto, con el principio de calidad de los datos.

En concreto, el numeral 46 de los Lineamientos indica que *"[l]os datos serán considerados exactos si corresponden a la situación actual del interesado."*

---

[145] Al respecto, véase la siguiente dirección de Internet http://www.infodf.org.mx/web/index.php?option=com_docman&task=doc_download&gid=101&Itemid=293.

Al igual que en el caso del derecho de acceso, el INFODF también ha publicado un formato específico[146] para el ejercicio del derecho de rectificación y su atención por los entes públicos sujetos a la LPDDF, que permite, de nuevo, como decíamos, diseñar un procedimiento estandarizado de atención al ejercicio del derecho.

En virtud de lo dispuesto en el numeral 47 de los Lineamientos, la solicitud del interesado para rectificar sus datos deberá contener los siguientes requisitos:

- Indicar qué datos se requiere que sean rectificados o completados.
- Acompañar la documentación que justifique lo solicitado.

En este sentido, es importante tener en cuenta que los anteriores requisitos son específicos en relación con el derecho de rectificación, sin perjuicio de otros que tengan que cumplirse o adjuntarse como consecuencia del ejercicio de los derechos en protección de datos en general.

En su solicitud de rectificación, el interesado tiene que indicar los datos personales que resultan ser incorrectos, así como los correspondientes datos correctos que constituyen su solicitud de rectificación. Y al mismo tiempo, como señalan los Lineamientos, adjuntar los documentos probatorios que se anexan a la solicitud de rectificación de los datos personales.

Por último, una vez más, es necesario recordar que el derecho de rectificación, como el resto, está sujeto a excepciones, ya que el artículo 28 de la Ley señala que *"[n]o obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo o en un proceso judicial, aquellos se considerarán exactos siempre que coincidan con éstos."* Esta previsión de la Ley es recogida específicamente en el numeral 50 de los Lineamientos.

---

[146] Disponible en la siguiente dirección de Internet http://www.infodf.org.mx/web/index.php?option=com_docman&task=doc_download&gid=102&Itemid=293.

Derecho de cancelación

En virtud del derecho de cancelación, como ya habíamos indicado al analizarlo en la Ley, el interesado puede solicitar al responsable del sistema de datos personales que cancele los datos que resulten ser inadecuados o excesivos para el tratamiento que se lleva a cabo.

De nuevo, es necesario aclarar que la cancelación no dará lugar a la supresión o borrado de los datos, sino que éstos serán bloqueados y, una vez que se cumplan los plazos legalmente establecidos, se podrá proceder a eliminar los datos.

El numeral 48 de los Lineamientos indica que se considerarán datos:

1. Inadecuados:
   a) Los que no guarden relación con el ámbito de aplicación y finalidad para la que fueron recabados;
   b) Si dejaron de ser necesarios con respecto a la finalidad para la que fueron recabados.

2. Excesivos:
   a) Si los datos obtenidos son más de los estrictamente necesarios en relación con la finalidad del tratamiento.

Además, el derecho de cancelación también procede cuando los datos sean tratados de manera que el tratamiento "no se ajuste a lo dispuesto en la Ley o en los Lineamientos."

A efectos de ejercitar su derecho de cancelación, el numeral 49 de los Lineamientos indica que el interesado, en su solicitud, tendrá que aportar *"la documentación que justifique las razones por las cuales considera que el tratamiento no se ajusta a lo dispuesto en la Ley."*

Al igual que en el caso del derecho de rectificación, la cancelación no procederá *"en los supuestos en que así lo disponga una Ley"*,

conforme al numeral 50 de los Lineamientos. Al respecto, volviendo de nuevo a la LPDPDF, ésta indica en su artículo 29 que *"[l]a supresión de datos no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando exista una obligación legal de conservar dichos datos."*

Y por último, también el INFODF ha publicado en su sitio web un formato para el ejercicio del derecho de cancelación[147]. Mediante dicho formato, el interesado tendrá que especificar en forma clara y precisa los datos personales de los que solicita su cancelación, así como las razones por las que considera que éstos deben ser cancelados.

Derecho de oposición

La Ley y los Lineamientos también reconocen al interesado el derecho de oposición al tratamiento de sus datos de carácter personal.

En virtud del numeral 51 de los Lineamientos, y tal y como ya había sido indicado al analizar este derecho en el articulado de la Ley, el derecho de oposición tiene por objeto que el interesado pueda oponerse al tratamiento de sus datos de carácter personal cuando se cumplan los requisitos establecidos en la Ley y en los Lineamientos.

En concreto, recordamos nuevamente que los requisitos para poder ejercitar el derecho de oposición por el interesado al que se refieren los datos objeto del tratamiento son los siguientes:

- El consentimiento del interesado no sea necesario para el tratamiento de sus datos;
- Exista un motivo legítimo y fundado del interesado; y
- Una Ley no disponga lo contrario.

---

147 Véase el formato disponible en la siguiente dirección de Internet http://www.infodf.org.mx/web/index.php?option=com_docman&task=doc_download&gid=103&Itemid=293.

Y de nuevo, la oposición del interesado dará lugar al bloqueo de sus datos y, una vez que transcurran los plazos legalmente establecidos para depurar las responsabilidades que pudieran surgir, procederá la cancelación de éstos.

Finalmente, también el INFODF ha publicado en su sitio web un formato para el ejercicio del derecho de oposición[148]. En su solicitud de oposición el interesado tendrá que especificar de forma clara y precisa los datos personales de los que se opone a su tratamiento, así como las razones de dicha oposición.

[148] El formato para el ejercicio del derecho de oposición se encuentra disponible en la dirección de Internet http://www.infodf.org.mx/web/index.php?option=com_docman&task=doc_download&gid=104&Itemid=293.

Instituto de Acceso a la Información Pública del Distrito Federal

Ley de Protección de Datos Personales
para el Distrito Federal,Comentada
-GODF 03 de octubre de 2008-

Primera Edición

Se terminó de imprimir en los talleres de
Servicio Editorial Gráfico
Calle 1513 No. 139
Unidad 6 de San Juan de Aragón,
con un tiraje de 2,000 ejemplares.

Ley de Protección de Datos Personales para el Distrito Federal Comentada

La Morena No. 865, Col. Narvarte,
Del. Benito Juárez, C.P. 03020, México, D.F.

www.infodf.org.mx