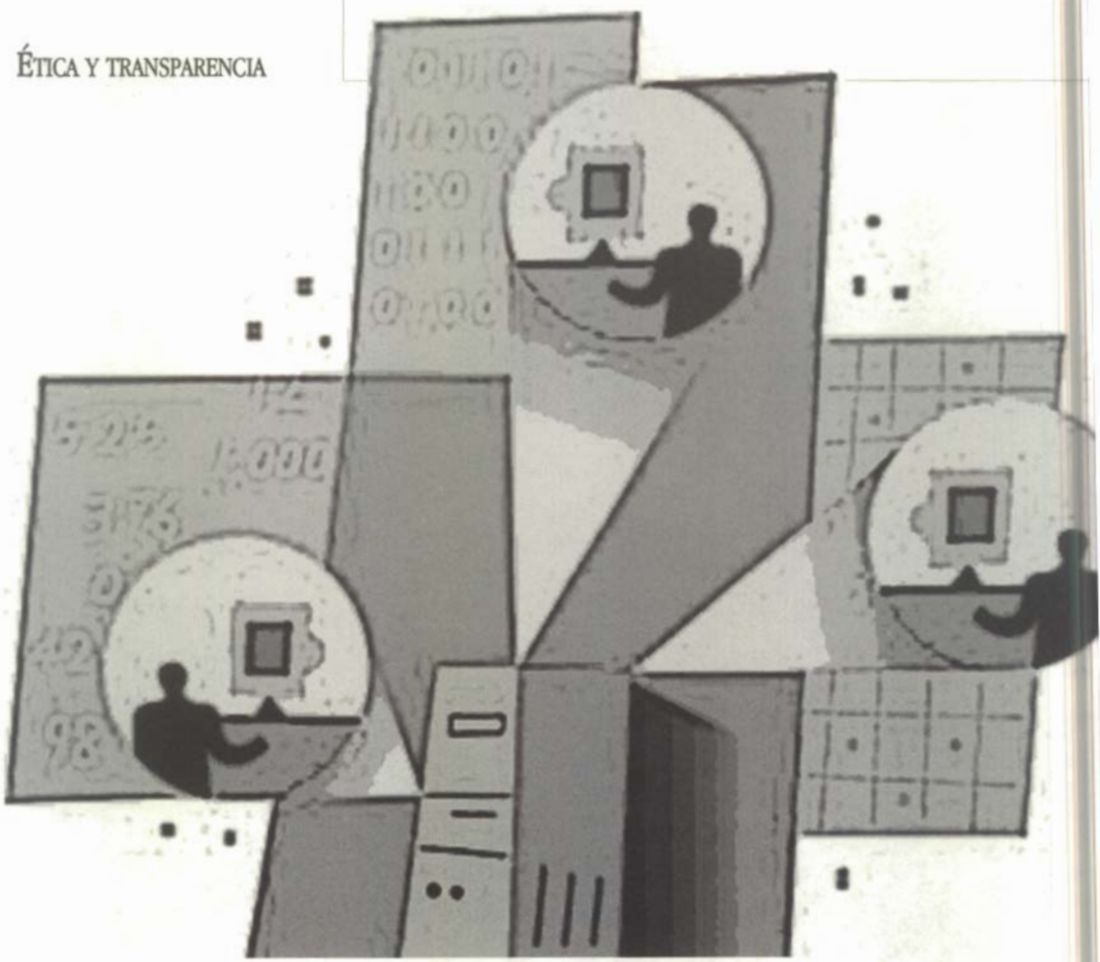
Buen Gobierno
ISSN: 1874-4271
director@revistabuengobierno.org
Fundación Mexicana de Estudios Políticos y Administrativos A.C.
México

Ornelas Nuñez, Lina
Apuntes sobre la protección de datos personales en los entes gubernamentales: Requisitos para la transmisión de datos
Buen Gobierno, núm. 8, enero-junio, 2010, pp. 100-116
Fundación Mexicana de Estudios Políticos y Administrativos A.C.
Ciudad de México, México



Apuntes sobre la protección de datos personales en los entes gubernamentales:

Requisitos para la transmisión de datos

Por Lina Ornelas Nuñez

Recibido: 26/02/2010. Aceptado: 12/03/2010.

RESUMEN

La Ley Federal de Transparencia y Acceso a la Información Publica Gubernamental regula la protección de datos personales en posesión de los poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal y cualquier otra entidad federal. Como regla general, los sujetos obligados, para difundir, distribuir o comercializar datos personales en su posesión, deberán obtener el consentimiento expreso de los individuos a que haga referencia la información. Sin embargo, se exceptúa cuando se trate de transmisiones entre sujetos obligados, y donde concurran las siguientes circunstancias: que se realicen en función de las atribuciones conferidas, en ejercicio de competencias similares o análogas y que versen sobre la misma materia.

Palabras clave: Datos personales, Transparencia, Sujetos obligados, Protección, Transmisión.

The Federal Transparency and Public and Governmental Access Act regulates the protection to personal data held by the Federal Powers, the Constitutional autonomous Bodies, with its corresponding legal autonomy, any other federal entity. As a general rule the subjects of this Act must have the written permission of the owner of personal data before commercializing, distributing and spreading it. Nevertheless, there is an exception when there is communication between obligated subjects and in the following circumstances: in function of given attributions, in exercise of similar or analogous competencies and when they refer to the same issue.

Key words: Personal data, Transparency, Obligated subjects, Protection, Transmision.

INTRODUCCIÓN

En 1974, la revelación en la prensa francesa de un proyecto gubernamental de interconexión de todos los ficheros administrativos, a fin de crear, entre otras bases de datos, un número de identificación único de los ciudadanos, conocido como "proyecto SAFARI", creó conmoción y preocupación en la opinión pública. A partir de ello, se constituyó una comisión encargada de hacer propuestas a fin de garantizar que el desarrollo de la informática se hiciera con absoluto respeto a la vida privada, así

como a las libertades individuales y públicas. De conformidad con las recomendaciones de la comisión mencionada, se presentó ante el parlamento y se aprobó, el 6 de enero de 1978, una Ley relativa a la informática, los ficheros y las libertades, que instituyó a la vez una autoridad independiente encargada de velar por su cumplimiento"[1].

El ejemplo anterior nos ilustra acerca de cómo un proyecto gubernamental hizo que naciera en Francia la primera ley de protección de datos personales. Y es que los gobiernos, así como las grandes corporaciones privadas son los entes que mayor información personal detentan, ya sea para el cumplimiento de las leyes o, para el logro de finalidades comerciales o de proveeduría de bienes y servicios.

Nadie puede negar que los avances tecnológicos hayan traído consigo infinitas ventajas y beneficios en todos los ámbitos del quehacer humano, un ejemplo de ello, es la transmisión de información por medios remotos a grandes distancias en cuestión de segundos. Bajo esta premisa, también es cierto que dichos avances traen inmersos riesgos y nuevos retos a enfrentar, entre otros, la protección de la información de carácter personal que se transmite.

En este sentido, la protección de datos personales como derecho fundamental tiene su origen en el derecho a la intimidad y la vida privada[2], si bien cuenta con sus propios mecanismos de tutela, este nuevo derecho busca la protección de las personas en relación con el tratamiento que se puede dar a su información, a través de los nuevos desarrollos científicos y tecnológicos, en particular, de la informática.

Es en la Europa de los años sesenta, que se instauran las bases del derecho a la protección de datos personales, tratando de conciliar dos conceptos, *privacidad e informática*, de tal manera que la primera no constituya un freno al avance de la tecnología y la utilización de ésta, y que a su vez, no violente la vida privada de los individuos. Bajo esta óptica, países europeos como Alemania[3], Francia[4] y Dinamarca, aprobaron leyes nacionales para la protección de datos de carácter personal. Por lo que hace a los países Americanos, algunos años más tarde, aparecen las primeras normas de protección de datos personales. Algunos con menos fuerza y de manera sectorial, o bien en otros, apegándose al modelo europeo ya existente, germinando bajo un escenario similar respecto al tratamiento de la información de carácter personal frente a los avances inminentes de la tecnología de la información.

Así, se trabajó en diversos modelos normativos tanto a nivel doméstico como internacional que permitieron al derecho a la protección de datos personales perfilarse como un derecho independiente y autónomo del derecho a la intimidad y al de privacidad. Lo anterior, otorgó a la persona un poder de disposición y control sobre los datos que le conciernen, con base en principios

específicos respecto al tratamiento y seguridad en los datos, e imponiendo a los responsables de dicho tratamiento - ya sea entes públicos o privados-, la obligación de realizarlo con apego a los principios y a las finalidades lícitas y legítimas de la protección de datos.

Al respecto, cabe citar lo manifestado por José Luis Piñar Mañas al señalar que el derecho a la protección de datos de carácter personal:

> "[...] presenta caracteres propios que le dotan de una naturaleza autónoma, de tal forma que su contenido esencial lo distingue de otros derechos fundamentales, específicamente, del derecho a la intimidad, al honor y a la propia imagen.
>
> El derecho a la intimidad tiende a caracterizarse como el derecho a ser dejado solo y evitar injerencias en la vida privada.
>
> El derecho a la protección de datos atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, partiendo del reconocimiento de que tales datos van a ser objeto de tratamiento por responsables públicos y privados"[5].

En este sentido, se ha buscado que el derecho a la protección de los datos personales prospere a la par de los avances de la tecnología de la información, en un entorno en el que la transmisión de información entre los diferentes actores, públicos o privados, constituye parte de la columna vertebral del desarrollo cotidiano de las actividades económicas y sociales a escala mundial, por lo que es necesario establecer estándares mínimos que regulen y unifiquen la libre circulación de datos, al tiempo de respetar los principios y derechos de protección de datos personales.

De acuerdo con la evidencia más reciente, estamos apenas en el inicio de una nueva era en la que la minería de datos y el acopio de información de las personas será el *"core"* de las actividades de los gobiernos y las empresas. De no contar con un enfoque precautorio que respete los principios internacionalmente reconocidos en materia de protección de datos personales, la puesta en marcha de proyectos ambiciosos que no prevean las garantías de seguridad necesarias, podrían estar en riesgo las libertades civiles y derechos fundamentales de los ciudadanos del futuro.

De tal forma que, el presente artículo tiene como propósito reflejar la regulación que hasta el momento existe en materia de protección de datos en nuestro país, con especial énfasis en las disposiciones para el tratamiento de datos por parte de los entes públicos. En específico, analizaremos las transmisiones de datos personales que se realizan entre sujetos obligados en el ámbito federal a la luz de lo establecido por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

1. DESARROLLO NORMATIVO DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO EN EL ÁMBITO PÚBLICO

El primer antecedente normativo en materia de protección de datos personales en el ámbito público federal, lo constituye la Ley Federal de Transparencia y Acceso a la Información Pública

Gubernamental -en adelante, LFTAIPG-, publicada en el Diario Oficial de la Federación el 11 de junio de 2002[6].

Dicho instrumento jurídico, si bien tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal, es decir, entes públicos en el orden federal; prevé específicamente dentro de sus objetivos, el garantizar la protección de los datos personales en posesión de dichos sujetos obligados. Para tal efecto, la LFTAIPG establece en el Capítulo IV del Título Primero, las disposiciones que deberán observar los entes públicos para el tratamiento de los datos personales.

Con la adición del segundo párrafo al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación el 20 de julio de 2007, se dio un paso fundamental en el reconocimiento del derecho a la protección de datos con una denominación específica, si bien inmerso en el derecho de acceso a la información, al incluirse de manera expresa la mención a la protección de los datos personales en poder de la Federación, los Estados y el Distrito Federal y el derecho de acceso y rectificación de los mismos, en los siguientes términos:

> "Artículo 6 … [P]ara el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> […]
>
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
>
> […]"

Trascurrieron un par de años más para que los esfuerzos iniciados en torno al reconocimiento y regulación del derecho a la protección de datos personales rindieran los primeros frutos, con la reforma al artículo 16 Constitucional, publicada en el Diario Oficial de la Federación el 1 de junio de 2009[7]. La reforma en mención tiene la peculiaridad de dotar finalmente de contenido a dicha garantía individual y situarla como un derecho fundamental y autónomo, ya no solo circunscrito a su observancia por parte del Estado. El artículo 16 constitucional establece a la letra lo siguiente:

> "Artículo 16. […]
>
> [T]oda 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.
> […]"

De esta suerte, con la reforma al artículo 16 constitucional se observan los siguientes avances normativos:

> El reconocimiento de los derechos de los titulares frente al tratamiento de sus datos, esto es, los derechos de acceso, rectificación, cancelación y oposición –mejor conocidos como, derechos ARCO- sin que se limiten dichos derechos a ser ejercidos únicamente cuando los datos obren en los archivos del gobierno en sus tres órdenes;
>
> La existencia de principios a los que se debe sujetar todo tratamiento de datos personales, y
>
> Los supuestos de excepción en cuanto a la aplicación de los principios y derechos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Ahora bien, en virtud de las disposiciones del 6º constitucional, los gobiernos se encuentran constreñidos a la debida protección de datos personales que se encuentren en sus archivos, sin embargo, no fue sino hasta el 30 de abril de 2009 que se publicó en el Diario Oficial de la Federación, la reforma al artículo 73 Constitucional que tiene por objeto dotar de facultades al Congreso Federal para que legisle en materia de protección de datos personales en posesión de los particulares.

Por lo tanto, queda aún pendiente la emisión de la regulación federal aplicable al sector privado, de modo que las personas gocen del derecho a que sus datos sean protegidos no importando si éstos se encuentran en manos de entes públicos o de particulares.

Volviendo a las disposiciones de la LFTAIPG, en cuanto al tratamiento de la información personal contenida en los sistemas de datos personales en posesión de entes públicos a nivel federal[8], se observa que dicha ley prevé lo siguiente:

> La definición de datos personales como toda información concerniente a una persona física, identificada o identificable, entre otras, 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 su intimidad;
>
> Los principios de protección de datos internacionalmente reconocidos como el de licitud, calidad, finalidad, proporcionalidad, información y consentimiento;
>
> Las excepciones al principio del consentimiento;
>
> Los derechos de los titulares de los datos exclusivamente en cuanto al acceso y rectificación de los mismos, y
>
> Los deberes, por parte de los sujetos que tratan datos personales, de adoptar las medidas necesarias que garanticen la seguridad de los datos personales, en cuanto a su confiabilidad, disponibilidad y confidencialidad.

Cabe señalar, que la LFTAIPG establece como órgano garante en materia de protección de datos personales, al Instituto Federal de Acceso a la Información Pública, que debe procurar el adecuado tra-

tamiento de la información personal contenida en los sistemas de datos personales en posesión de las dependencias y entidades de la Administración Pública Federal, así como resolver los recursos de revisión interpuestos por los ciudadanos cuando les ha sido negado el acceso o corrección de sus datos de carácter personal[9]. Por lo que hace a los demás sujetos obligados, la propia ley en su artículo 61 establece la creación de sus respectivos órganos garantes en el ámbito de sus competencias.

Por lo anterior, es primordial que se expida un marco normativo comprehensivo en la materia, que permitan el ejercicio íntegro de los derechos por parte de los titulares de los datos personales y que unifique los principios en cuanto a su tratamiento, tanto para el sector público como privado. Lo anterior sin olvidar las peculiaridades y excepciones que derivan del tratamiento efectuado a los datos personales por autoridades o particulares.

2. TRATAMIENTO DE LOS DATOS PERSONALES POR PARTE DE LOS SUJETOS OBLIGADOS EN TÉRMINOS DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL (LFTAIPG)

Con el objeto de lograr una mayor comprensión de los principios y derechos que a nivel internacional regulan el tratamiento de los datos personales y los alcances de la legislación mexicana en la materia, a continuación se desarrolla un breve análisis respecto a la regulación del derecho a la protección de datos de carácter personal en términos de dos instrumentos internacionales, que por su importancia, resultan de referencia obligatoria en el estudio del derecho a la protección de datos, siendo estos: la Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas, del 14 de diciembre de 1990, por la que se establecen las directrices de protección de datos, y la Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995 relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[10].

Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas, del 14 de diciembre de 1990, por la que se establecen las directrices de protección de datos[11]. En dicho documento se establecieron los principios mínimos que deben prever las legislaciones de cada Estado, aplicables a todos los archivos informáticos y manuales, públicos y privados, principios que establecen lo siguiente:

Principio de legalidad y lealtad. Dicho principio contempla que la información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.

Principio de exactitud. Que señala que las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible, con el fin

de evitar errores de omisión, así como de actualizarlos periódicamente o cuando se use la información contenida en un archivo, mientras están siendo procesados. A este respecto, la LFTAIPG, establece que los sujetos obligados deberán procurar que los datos personales sean exactos y actualizados.

Principio de especificación de la finalidad. La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que:

a) Todos los datos personales recogidos y registrados sigan siendo pertinentes y adecuados para los fines especificados;
b) **Ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada, para fines incompatibles con aquellos especificados;**
c) El período durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados.

Al respecto, la LFTAIPG establece que los sujetos obligados podrán tratar los datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido; así mismo, no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los titulares de los datos.

Principio de no discriminación. Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

Respecto a la restricción en cuanto al tratamiento de datos sensibles, como los antes señalados, la LFTAIPG no contempla prohibición en cuanto al tratamiento de los mismos.

Principio de seguridad. Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.

Por lo que hace a las medidas de seguridad, en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), los

sujetos obligados deben adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Flujo transfronterizo de datos. Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca garantías similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan garantías recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad.

A este respecto, cabe destacar que México no cuenta actualmente con un marco normativo nacional en materia de flujos transfronterizos de datos de carácter personal, por lo que se ha optado por mecanismos más sencillos como la autorregulación, aplicable principalmente a las actividades comerciales.

Con relación a los derechos, la Resolución 45/95 establece que *cualquier persona que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios.*

Por lo que hace a la tutela de derechos, se prevé la necesidad de contar con una autoridad supervisora, que conozca de los recursos que presenten los titulares de los datos.

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995 relativa a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos —en lo sucesivo, la Directiva—[12].

En dicha Directiva, además de los principios y derechos reconocidos en la Resolución 45/95 antes expuesta, se establecen las siguientes disposiciones en materia de protección de datos:

Legitimación del tratamiento. En este principio se establece que solo podrán tratarse los datos personales si el interesado ha dado su consentimiento de forma inequívoca o si el tratamiento es necesario para:

La ejecución de un contrato en el que el interesado sea parte;
El cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento;
Proteger el interés vital del interesado;

El cumplimiento de una misión de interés público, o
La satisfacción del interés legítimo perseguido por el responsable del tratamiento.

Al respecto, la LFTAIP prevé de manera expresa la restricción en el tratamiento de los datos personales, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar del titular. Esto es, la posesión de sistemas de datos personales obedece exclusivamente a las atribuciones legales o reglamentarias y deberá tratarse para la finalidad para la cual fueron obtenidos.

Información a los afectados por dicho tratamiento. El responsable del tratamiento deberá facilitar información mínima a la persona de quien se recaben los datos, por ejemplo la identidad del responsable del tratamiento, fines del tratamiento y destinatarios de los datos, así como los casos de excepción.

La LFTAIPG, establece que los sujetos obligados deberán poner a disposición de los titulares, a partir del momento en el cual se recaben sus datos personales, el documento en el que se establezcan los propósitos para su tratamiento; del mismo modo, señala los supuestos de excepción en los cuales no se requerirá el consentimiento de los titulares para la trasmisión de los datos personales.

Ahora bien, en el siguiente apartado analizaremos el tratamiento de los datos personales por parte de los entes públicos, en específico, las transmisiones de datos personales que se realizan entre sujetos obligados en observancia a los principios antes referidos y en términos de la LFTAIPG.

3. TRANSMISIÓN DE DATOS DE CARÁCTER PERSONAL ENTRE SUJETOS OBLIGADOS EN TÉRMINOS DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL (LFTAIPG)

En atención a sus facultades y atribuciones, los entes públicos administran bases de datos con información de carácter personal, y realizan el tratamiento de los datos, de tal manera que les permitan de manera ágil y eficiente el desarrollo de sus actividades. Por tratamiento de datos se entiende todas aquellas operaciones y procedimientos físicos o automatizados que permitan recabar, registrar, reproducir, conservar, organizar, modificar, transmitir y cancelar datos personales. Ahora bien, la transmisión de datos personales entre sujetos obligados es una práctica obligada de apoyo institucional que favorece el cumplimiento eficiente de las actividades gubernamentales. Práctica que debe realizarse bajo la plena observancia de los principios de protección de datos personales.

En este sentido, cabe apuntar que *transmisión* refiere a toda entrega total o parcial de datos personales a cualquier persona distinta de su titular, mediante el uso de medios físicos o electrónicos[13].

Respecto a los principios que regulan el tratamiento de los datos personales, la LFTAIPG en el artículo 20 señala que los sujetos obligados serán responsables de los datos personales y, en relación con éstos deberán, entre otros,

> Tratarlos sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido (fracción II);
>
> Poner a disposición de los titulares de los datos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan **los propósitos para su tratamiento** (fracción III), y
>
> Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado (fracción VI).

Por su parte, el artículo 21 establece que los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

En este último punto, cabe resaltar que podrán divulgarse aquellos datos personales sin necesidad del consentimiento de sus titulares, cuando: a) por ministerio de ley exista una disposición que obligue su publicidad (como en el caso de los salarios de servidores públicos o el nombre y monto de las personas que reciben recursos públicos), y b) cuando existan causas de interés público a juicio de los órganos garantes, que permitan discernir que publicar un dato personal genera un bien público mayor que la afectación al titular del dato en su esfera de privacidad[14].

Ahora bien, el artículo 22 establece los supuestos de excepción en los que no se requerirá el consentimiento de los titulares para proporcionar los datos personales, en los siguientes términos:

> Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el que no puedan asociarse los datos personales con el individuo a quien se refieran;
>
> **Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;**
>
> Cuando exista una orden judicial;
>
> A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
>
> En los demás casos que establezcan las leyes.

Conforme lo anterior, los sujetos obligados deben tratar los datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los que se hayan

obtenido. En ese sentido, los datos personales únicamente pueden tratarse para la finalidad para la que fueron obtenidos, misma que debe ser determinada y legítima.

No se omite señalar que, si bien la LFTAIPG establece en su artículo 22 fracción III que no se requerirá el consentimiento de los individuos para proporcionar sus datos personales cuando se transmitan entre sujetos obligados o entre dependencias y entidades, también lo es que dichos datos deben utilizarse únicamente para el ejercicio de facultades propias de los mismos. En ese sentido, se circunscribe el tratamiento a finalidades concretas y explícitas.

Lo anterior permite hacer dinámicas las relaciones entre dichos entes, al tiempo de asegurar que el nuevo tratamiento de datos llevado a cabo sea afín o compatible a aquél en virtud del cual fueron originalmente recabados lo datos, ya que no se estaría alterando la autorización inicialmente otorgada por su titular[15].

En razón de lo anterior, en aquellos casos en que los sujetos obligados contaran con atribuciones incompatibles, las transmisiones de datos requieren del consentimiento del titular de los mismos para llevarse a cabo, a efecto de cumplir tanto con el principio de finalidad como del consentimiento.

En congruencia con lo anterior y de forma ilustrativa se puede mencionar que la Agencia Española de Protección de Datos, ha emitido diversos informes jurídicos respecto a la cesión de datos entre organismos públicos, por lo que a manera de referencia se cita a continuación el informe 2009-0392 "Comunicación de datos entre Organismos Públicos"[16], en la que en su parte conducente señala:

> "La consulta plantea, si resulta conforme con la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal la comunicación de determinados datos por parte de la Comunidad de Regantes a la Confederación Hidrográfica del Duero y viceversa.
>
> Como cuestión previa, conviene recordar que el supuesto sometido a Informe constituye una cesión de datos de carácter personal, definido en el artículo 3 j) de la Ley Orgánica como "Toda revelación de datos realizada a una persona distinta del interesado".
>
> La cesión debe sujetarse al régimen general de comunicación de datos de carácter personal que según dispone el artículo 11.1 de la citada Ley Orgánica, **"los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado"**. Esta disposición se ve complementada en el supuesto que ahora nos ocupa por lo dispuesto en el artículo 11.2 a) de la Ley Orgánica, del cual se desprende que será posible la cesión cuando una Ley lo permita.
>
> [...]
>
> En definitiva, nos encontramos en presencia de dos organismos públicos, por lo que si la cesión se realizará en el presente supuesto entre dos órganos de la Administración Pública, la Confederación

> hidrográfica del Duero y las Comunidades de Regantes, debe analizarse si procede la aplicación del artículo 21.1 de la LO 15/1999 según el cual "Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus **atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas,** salvo, cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos." Y en su número 4 señala que "En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley".
>
> **Lo decisivo es la prohibición expresa de que los datos se comuniquen para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas a aquellas que motivaron la recogida de los datos, de modo que para que pueda procederse a la cesión descrita en la consulta sin el consentimiento de los interesados, la petición de datos formulada por la Confederación hidrográfica debería determinar con claridad que los datos se solicitan para el ejercicio de competencias sobre la misma materia.**
> [...]
>
> En conclusión, las cesiones previstas entre ambos organismos se encuentran amparadas en el artículo 21.1 de la Ley Orgánica 15/1999 en caso de que la los datos se utilicen única y exclusivamente para las finalidades vinculadas con el ejercicio de potestades de derecho público y se incorporen a los ficheros de de los que sea responsable cada entidad. En caso contrario, la utilización de los datos resultaría contraria a lo dispuesto en el artículo 4.2 de la Ley Orgánica 15/1999, a cuyo tenor "los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos".
>
> [Énfasis añadido]

En este tenor se puede concluir que, la transferencia de datos entre sujetos obligados, sin el consentimiento de los titulares, resulta procedente, cuando la comunicación de los datos se realiza en función de las atribuciones conferidas, en ejercicio de competencias similares o análogas y que versen sobre la misma materia. Siendo responsabilidad de los transmisores de información el corroborar que el sujeto obligado al que se le transmiten los datos cuente, además de las atribuciones y funciones antes señaladas, con las medidas de seguridad necesaria para mantener la integridad, confiabilidad y disponibilidad de los datos transferidos.

4. A MANERA DE CONCLUSIÓN

Queda claro de lo antes expuesto que en las transmisiones de datos entre entes gubernativos es necesario observar los principios de protección de datos personales, así como las medidas para garantizar que dichas transmisiones, contemplen si resulta necesario requerir el consentimiento de los titulares y las medidas de seguridad adecuadas.

Lo anterior toma mayor relevancia día con día toda vez que presenciamos una tendencia irreversible a que los gobiernos lancen políticas públicas encaminadas al cumplimiento de sus atribuciones, que involucran el uso de nuevas tecnologías y el acopio de ingentes cantidades de datos personales. Los avances de la técnica permitirán la identificación fehaciente de las personas; la proveeduría de mejores servicios de salud; la localización de grupos vulnerables; el otorgamiento de subsidios, y el mejor cobro de impuestos entre otros aspectos[17].

Si bien, podría resultar muy útil y factible tecnológicamente concentrar todo tipo de información de una persona: datos de contacto; estado de salud; cumplimiento de obligaciones fiscales; información curricular, entre otras cuestiones, no debe perderse de vista que el Estado solo puede hacer todo aquello que tenga expresamente permitido por Ley. Lo anterior es una primera garantía frente al titular de los datos, ya que de manera intrínseca, sería violatorio concentrar en una sola base de datos un sinnúmero de aspectos relativos a un individuo, así como transmitir los datos para finalidades incompatibles.

Es la generación de perfiles de los individuos la que puede en un momento dado conculcar otros derechos y libertades. Las conclusiones del proyecto Safari mencionado al inicio de este artículo siguen vigentes actualmente en toda Europa y en otros países de diversos continentes. El derecho a la protección de datos personales consagrado recientemente en nuestra Constitución, dota de un haz de facultades al titular de los datos para conocer de manera informada acerca del tratamiento que se dará a su información y los destinatarios de la misma.

Como se observa, es necesario que los servidores públicos conozcan y dimensionen los alcances de las disposiciones en materia de protección de datos personales aplicables a los entes públicos, a efecto de generar una cultura en torno a este nuevo derecho y sus mecanismos de implementación. La protección de datos no debe percibirse como un obstáculo para la concreción de proyectos gubernamentales, antes bien, permite aclarar y delimitar ámbitos de actuación y respetar garantías individuales. Asimismo, permite contar con calidad en las bases de datos y regular un flujo normado y seguro de las transmisiones, evitando pérdidas o accesos no autorizados a información que detenta el gobierno.

Por ello, ser requiere impulsar reformas al marco normativo para adecuar las nuevas disposiciones constitucionales. En el ámbito público por ejemplo, deberán contemplarse, además de los derechos de acceso y rectificación, los correspondientes a la cancelación del dato cuando este ha dejado de ser necesario, así como el derecho de oposición a un determinado tratamiento, por razones legítimas.

Lina Ornelas Nuñez

Es egresada de la Facultad de Derecho de la Universidad de Guadalajara y es Maestra en Cooperación Legal Internacional por la Universidad Libre de Bruselas (Vrije Universiteit Brussel). Ha trabajado desde hace mas de 10 años en el sector público, en particular para la Comisión Europea y las Secretarías de Economía y Gobernación, en ésta última como Directora General Adjunta de Estudios Legislativos participando en el grupo redactor de la Iniciativa de Ley de Acceso a la Información que envió el Poder Ejecutivo al H. Congreso de la Unión. También fue Directora General Adjunta en la Unidad para la Promoción y Defensa de los Derechos Humanos de dicha secretaría.

Actualmente, coordina subgrupos de trabajo de la Red Iberoamericana de Protección de Datos Personales, es miembro del Consejo Editorial de la Revista de Protección de Datos de la Comunidad de Madrid "Data Protection Review", miembro de la Asociación Internacional de Profesionales de Privacidad (IAPP); coautora del capítulo sobre México del libro "Privacidad y Derechos Humanos 2005, 2006 y 2007" publicado por la organización Electronic Privacy Information Center, (EPIC), así como del libro "Protección de datos personales en México: El caso del Poder Ejecutivo". También ha publicado numerosos artículos académicos en la materia. Se desempeña desde 2003, como Directora General de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información Pública (IFAI).

Así mismo, haría falta introducir la necesidad de llevar a cabo manifestaciones de impacto a la privacidad *ex ante* a la publicación de cualquier norma o disposición legal o secundaria que involucre el tratamiento de datos personales, a efecto de mitigar los impactos indeseables en la esfera del ámbito de privacidad de las personas.

Finalmente y aunque no se abordó en el presente artículo la transmisión de datos que puede darse entre un ente público y un "encargado", dado el intenso intercambio de datos que ocurre entre el gobierno y empresas que prestan servicios de tratamiento de datos subrogados *(outsourcing)*, resulta inaplazable una Ley de protección de datos en posesión de los particulares, para que no se comprometan proyectos de gran envergadura y necesarios para la modernización y crecimiento económico del país. De no ser así, cualquier mal uso de los datos personales por terceros, quedaría impune.

Queda claro entonces que son amplias las disyuntivas que se presentan en materia de protección de datos personales, lo que confirma la necesidad de contar con un marco normativo en la materia, que establezca de manera clara las directrices a seguir en cuanto al tratamiento de los datos personales y garantice el ejercicio de los derechos de los titulares, no solo para el sector público sino para el privado.

REFERENCIAS

[1] Disponible para su consulta en la página oficial de la Comisión Nacional de Informática y Libertades (CNIL, por sus cifras en francés) en el vínculo siguiente: http://www.cnil.fr/fileadmin/documents/es/La_ley_francesa_de_proteccion_de_datos.pdf

[2] La Declaración Universal de los Derechos del Hombre del 10 de diciembre de 1948, establece en el artículo 12 el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques. Por su parte, el Convenio para la Protección de los Derechos y las Libertades Fundamentales del 14 de noviembre de 1950, en el artículo 8 reconoce el derecho de la persona al respeto de su vida privada y familiar, de su domicilio y correspondencia.

El Pacto Internacional de Derechos Civiles y Políticos del16 de diciembre de 1966, señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Artículo 17.

Asimismo la Convención Americana sobre derechos humanos del 22 de noviembre de 1969, en su artículo 11, apartado 2 establece que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

[3] Ley de Protección de Datos de la República Federal Alemana publicada en 1977.

[4] La ley "Informática y Libertades" data de 1978.

[5] *Vid.* Piñar Mañas, José Luís. *La Red Iberoamericana de Protección de Datos (Declaraciones y Documentos)*, Tirant lo Blanch, Valencia, 2006, p. 32.

[6] Disponible en la página oficial del Instituto Federal de Acceso a la Información Pública (IFAI) en el vínculo siguiente: http://www.ifai.org.mx/transparencia/LFTAIPG.pdf

[7] Para consulta en el vínculo siguiente: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf

[8] De acuerdo con la definición aportada por la propia LFTAIPG, en su artículo 3, fracción XIII, se entiende por sistemas de datos personales al *"Conjunto ordenado de datos personales"*.

[9] El IFAI desde 2003 al día de hoy (17 de febrero de 2010), presenta la siguiente relación de solicitudes de información ingresadas a la Administración Pública Federal por tipo de acceso, a saber:

Tipo de solicitud	2003	2004	2005	2006	2007	2008	2009	2010	Total acumulado
Corrección de datos personales		174	347	334	537	530	637	98	2,657
Datos personales	1,212	2,765	5,090	7,853	13,691	17,464	18,958	2,451	69,484
Información Pública	22,885	34,793	44,690	52,026	80,495	87,256	98,002	13,744	433,891
Total	24,097	37,732	50,127	60,213	94,723	105,250	117,597	16,293	506,032

[10] Para mayor información sobre otros instrumentos internacionales en materia de protección de datos personales ver Ornelas Núñez, Lina y López Ayllón Sergio, "La recepción del derecho a la protección de datos en México: Breve descripción de su origen y estatus legislativo". Memorias del II Congreso Mexicano de Derecho Procesal Constitucional, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, México (2007).

[11] Para consulta en la página oficial de la Agencia Española de Protección de Datos, en el vínculo siguiente: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

[12] Para consulta en el vínculo siguiente: http://www.cmt.es/es/normativas/general/doc14684/Directiva_95-46-CE.pdf

[13] *Vid.* Lineamiento Tercero, fracción VIII de los Lineamientos de Protección de Datos Personales. Cabe señalar, que en artículo 3, inciso i), de la Ley Orgánica 15/1999, de 13 de Diciembre de Protección de Datos de Carácter Personal, de la Agencia Española de Protección de Datos, se señala que se entenderá por cesión o comunicación de datos, a toda revelación de datos realizada a una persona distinta del interesado.

[14] El análisis que debe hacer la autoridad se conoce como prueba de interés público o del equilibrio. En derecho comparado, existe una vasta experiencia en la materia y siempre se garantiza el derecho de audiencia del titular del dato, así como que la carga de la prueba recae en quien solicita el dato personal.

[15] Se considera que los titulares otorgan su consentimiento de manera tácita para que el gobierno pueda utilizar sus datos, dado que por ministerio de ley, resulta necesario recabar y utilizar datos personales.

[16] Disponible para consulta en la página oficial de la Agencia Española de Protección de Datos, en el vínculo siguiente: https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0343_Cesi-oo-n-de-datos-a-juntas-de-personal.pdf

[17] Tal es el caso, y solo por mencionar dos ejemplos, del proyecto para la emisión de una Cédula de Identidad Ciudadana y Personal que impulsa la Secretaría de Gobernación, derivado de sus facultades legales en materia de identificación de las personas; o el proyecto para la emisión de una Norma Oficial Mexicana para que cada mexicano pueda contar con un expediente clínico electrónico. En ambos proyectos se efectuarán transmisiones de datos.

BIBLIOGRAFÍA

Agencia Española de Protección de Datos,
https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/naciones_-unidas/common/pdfs/D.3BIS-cp—Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

https://www.agpd.es/portalweb/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2009-0343_Cesi-oo-n-de-datos-a-juntas-de-personal.pdf

Agencia de Protección de Datos de la Comunidad de Madrid (2008) *Protección de datos personales para la Administraciones Pública Locales.* Madrid, España.

Agencia de Protección de Datos de la Comunidad de Madrid (2003) *Manual de Protección de Datos para las Administraciones Públicas.* Madrid, España.

Cámara de Diputados, http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf

Comisión Nacional de Informática y Libertades, http://www.cnil.fr/fileadmin/documents/es/La_ley_francesa_de_proteccion_de_datos.pdf

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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,
http://www.cmt.es/es/normativas/general/doc14684/Directiva_95-46-CE.pdf

Gómez Robledo, Alonso y Lina Ornelas Núñez (2006) *La Protección de datos personales en México: El caso del Poder Ejecutivo Federal.* Ed. UNAM, México.

Piñar Mañas, José Luis (2006) *La Red Iberoamericana de Protección de Datos (Declaraciones y Documentos)*. Ed. Tirant lo Blanch, Valencia.

Piñar Mañas, José Luis (2005) "El derecho fundamental a la protección de datos personales", en *Protección de Datos de Carácter Personal en Iberoamérica* (II Encuentro Iberoamericano de Protección de Datos La Antigua-Guatemala 2-6 de junio de 2003). Ed. Tirant lo Blanch, Valencia.