LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (PRIVACIDAD)

Isabel Davara Fernández de Marcos

Resumen
La protección de datos es un derecho fundamental. El individuo tiene derecho a decidir cuándo, cómo y quién va a tratar su información personal. En Latinoamérica queda mucho trabajo por hacer en relación con la privacidad, pues la mayor parte de los países no tienen una regulación en la materia. Sin embargo, las tendencias giran en torno a la aproximación europea, a pesar de las importantes presiones en contra que aducen la imposición de barreras comerciales, mientras que, muy al contrario, podría ser un incentivo al consumo, como un valor añadido para los consumidores. Un sistema legal de protección de datos se estructura en principios, derechos y procedimiento. Entre los principios, el consentimiento y la finalidad destacan como los principales. En México, en concreto, no existe una ley de protección de datos. La iniciativa original está parada en el Congreso desde 2001. La ley para el Acceso a la información pública, no obstante, contiene algunas de las cuestiones más importantes de este tipo de ley, aunque no se pueda considerar una ley de protección de datos.

KEY WORDS: derecho fundamental – principios – derechos – procedimiento.

Planteamiento

La protección de datos de carácter personal ha adquirido verdadera carta de naturaleza y un esencial protagonismo en los últimos años.

Siempre ha habido tratamiento de datos de carácter personal, pero, hasta la utilización masiva de la informática para dicho tratamiento, no se producía una intromisión tan importante y agresiva en la esfera personal e íntima de las personas. Esta intromisión, que en algunos casos no tiene por qué ser negativa, ni mucho menos ilícita, se percibe como una amenaza potencial, desconocida.

En este sentido, se habla de la privacidad, que es un término más profundo que la intimidad, concepto más conocido y común en nuestros ordenamientos jurídicos y en la sociedad en general. La privacidad está compuesta por un sinfín de facetas del individuo, de su personalidad, que, tratadas de manera conjunta, máxime por medios informáticos, pueden llegar a constituir un perfil que el mismo individuo, titular de esos datos aislados, desconoce, y, por tanto, no controla.

Es aquí donde esta inmensa transformación tecnológica hace que el Derecho tenga que reaccionar y proponer soluciones encaminadas a manejar este nuevo escenario en la protección de, no ya la intimidad de las personas, sino de su derecho fundamental a la protección de datos de carácter personal, o, en términos más coloquiales, a su privacidad.

No obstante, en México no existe aún una ley específica a nivel federal que regule específicamente la protección de datos personales, si bien el Estado de Colima sí cuenta con una regulación concreta[1], que sigue en gran medida la antigua y ya derogada Ley orgánica 5/92 de regulación del tratamiento automatizado de datos de carácter personal española[2].

A nivel federal la primera referencia que se encuentra en el ordenamiento jurídico está en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, promulgada el 17 de febrero de 1917, que establece que *"nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones"*.

A pesar de lo anterior, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (en adelante, LFTAIPG)[3], que, si bien es una norma cuyo objeto es, según dispone su artículo 1, *"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"*, incide directamente en la privacidad de los individuos cuyos datos personales son objeto de tratamiento, planteándolo como un límite al acceso a la información, cuestión que entendemos desafortunada, pues, más que límite, es, en todo caso, complemento.

Así, entre su objeto, la LFTAIPG comienza a destacar en su artículo 4 apartado III, como uno de los objetivos de la ley: "*Garantizar la protección de los datos personales en posesión de los sujetos obligados."*

No obstante, no se puede olvidar que la LFTAIPG se limita en su competencia a los organismos de la Administración Pública Federal, es decir, las empresas privadas, y demás organismos públicos, quedan fuera de su competencia.

Pasamos a continuación a analizar brevemente la manera en que la norma trata los elementos principales que la regulación en protección de datos, aún no siendo una ley de estas características.

Principios

Como eje central de las normativas en protección de datos, 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, se articula también en el capítulo cuarto, artículos 21 y 22, de la LFTAIPG. Sin embargo, reiterando que debemos recordar que esta ley no puede considerarse una norma en protección de datos, sino de acceso a la información, este principio no se encuentra detallado, sino que se define sólo en relación con la fase en la que los datos se transfieren a un tercero, es decir, cuando se produce la cesión o comunicación de datos a terceros, en la que el titular pierde, en su caso, aún más el control sobre su información personal.

En consecuencia, no se contempla nada acerca de la necesidad del consentimiento para el tratamiento en origen o posterior de datos de carácter personal y, como decíamos, sólo se especifica que se requiere del consentimiento en la comunicación de datos en los términos que establece el artículo 21 de la LFTAIPG, que prevé:

> *"Los sujetos obligados no podrán <u>difundir, distribuir o comercializar</u> los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones,* ***<u>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</u>****."*

Como apuntábamos, el consentimiento para el tratamiento de datos es un principio esencial en la normativa, siendo el punto de partida de licitud de dicho tratamiento. En este sentido, el tratamiento de datos, y tal y como se prevé precisamente en las definiciones de la propia LFTAIPG no sólo se refiere a los actos regulados en el artículo 21 de la LFTAIPG de "*difundir, distribuir o comercializar*" los datos personales, sino que se incluye dentro de este concepto la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación y transmisión de datos personales, y, por lo tanto, todo tratamiento requiere del consentimiento, como regla general, y no únicamente en esa fase posterior de cesión o comunicación que mencionamos.

No obstante, este consentimiento también tiene excepciones, y la ley las recoge también, aunque de nuevo únicamente respecto de la fase de comunicación, entre las que el artículo 22 de la LFTAIPG destaca el tratamiento por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento de disociación, por orden judicial, para prestaciones de servicios por terceros, o, en un caso no exento de polémica en legislaciones comparadas, 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.

Independientemente de lo que ya hemos expresado sobre la necesidad del consentimiento para recabar y tratar datos de carácter personal, en su caso comunicándolos a terceros, y las excepciones al mismo, además, los datos que se recaben, conforme al principio de calidad de los datos, deben ser pertinentes, adecuados y no excesivos para el fin que se pretenda en su tratamiento, y no podrán permanecer en el sistema de datos personales por tiempo mayor al necesario para cumplir con la finalidad para la que se obtuvieron. La información, o los datos que se recaban o que se registran en un sistema de datos personales, debe ser exacta, mantenida al día, apropiada para el fin para el que fue almacenada y obtenida por medios legales, y así se dispone en el artículo 20 de la LFTAIPG.

Asimismo, es otro principio general de protección de datos que todo ciudadano tiene derecho a ser informado de determinados extremos cuando se le solicitan datos de carácter personal con el fin de que conozca quién, cómo y para qué los va a tratar, así como poder ejercitar, en su caso, los derechos que la Ley le reconoce. En México, a nivel federal, el principio de información se ciñe a informar al interesado del propósito del tratamiento de sus datos, si bien se requiere que dicha información conste en un documento que se ponga a disposición de los individuos (lo que, por un lado, aumenta la seguridad jurídica pero implica importantes problemas logísticos), y queda regulado en el artículo 20 de la LFTAIPG.

En otro orden de cosas, y continuando con el análisis de los principios imperantes en las normas de protección de datos, a pesar de que las normas internacionales sobre protección de datos hacen referencia, de una u otra manera, a una categoría especial de datos que, por su especial naturaleza, requieren de un mayor grado o nivel de protección para garantizar la privacidad de los ciudadanos (entre los que podemos citar origen racial, vida sexual, salud, ideología, religión, creencias y afiliación sindical), la normativa mexicana que analizamos tampoco hace distinción alguna en lo que a estas distintas clases de datos de carácter personal se refiere.

En cuanto al principio de seguridad en el tratamiento de datos personales, cuestión cuya implementación deviene esencial para impedir el acceso a los sistemas de datos personales, en particular, y a los datos en general, a personas no autorizadas, o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos, además de para garantizar el tratamiento de datos dentro de los límites permitidos por la norma y con respeto a los derechos del afectado, asegurando la confidencialidad y la integridad de los datos personales evitando su alteración, pérdida, transmisión y acceso no autorizado. En concreto, en la fracción VI del artículo 20 se establece la obligación de quienes tengan sistemas de datos personales de: "*Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.*"

Por otro lado, como un principio de carácter general, si bien específico en relación con la normativa, el principio de confidencialidad o deber de secreto, se destaca como un deber que debe observarse por toda persona que tenga acceso a los datos, durante todo el tiempo que dure el tratamiento y aun después de que finalice el mismo, que busca garantizar que quienes traten datos de carácter personal en el desarrollo de sus funciones los guarden y garanticen el secreto sobre los mismos, aunque la LFTAIPG no establece expresamente este deber de secreto u obligación similar para quienes tratan datos de carácter personal.

Por último, es obvio que la práctica diaria de las entidades en cuanto al tratamiento de datos de carácter personal y, expresado en otros términos, la necesidad y utilización real de terceros que presten determinados servicios que implican acceso a los datos por los mismos, se recoge en las distintas legislaciones internacionales en protección de datos como una figura distinta de la comunicación de datos ya comentada. En la prestación de servicios, o acceso a los datos por terceros, se recoge un encargo por parte del responsable del sistema de datos a un tercero para que se le preste un servicio determinado, mientras que en la comunicación de datos se produce una transferencia de datos del responsable a otro responsable para que éste haga con los datos lo que considere pertinente en relación con la finalidad prevista, perdiendo el originario responsable el control sobre dichos datos, mientras que en la prestación de servicios el prestador sólo hace con los datos lo que el responsable originario le encargó que hiciera. La LFTAIPG, en este sentido, establece (fracción V de su artículo 22) que no será necesario el consentimiento del interesado para proporcionar sus datos a un tercero al que se contrate para la prestación de un servicio que requiera el tratamiento de datos personales. Como vemos, se trata por tanto de la regulación del acceso a los datos por un tercero de manera diferente a la especificada en la comunicación de datos que establece la necesidad de consentimiento expreso y por escrito o por un medio de autenticación equivalente.

Derechos

Vistos los principios que rigen el tratamiento de datos, la normativa prevé 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, de sus datos personales, haga el responsable del sistema de datos personales, y, en su caso, instarle a modificar o suprimir aquellos datos cuyo tratamiento no resulte procedente, así como a conocer qué información se está tratando sobre su persona.

El primer derecho que vamos a analizar es el derecho de acceso que faculta a los titulares de los datos para solicitar al responsable del sistema de datos personales información relativa al tratamiento de sus datos personales, pudiendo conocer qué datos tiene sobre él y a quiénes se van a comunicar. Este derecho se encuentra en la LFTAIPG en sus artículos 20 y 24, así como en el artículo 47 del Reglamento de la LFTAIPG[4].

Por su parte, los derechos de rectificación y supresión permiten al afectado o interesado, titular de los datos, por un lado, solicitar la modificación, en los casos de que los datos sean inexactos, y cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido registrados, requerir su cancelación. Si los datos que se encuentran en un sistema de datos son inexactos, incompletos o no existiera, por el motivo que fuera, derecho a su registro por parte del titular del sistema de datos personales, el afectado podrá ejercer su derecho de rectificación o su derecho de cancelación, según corresponda, remitiéndonos al artículo 25 de la LFTAIPG para su análisis más detallado.

Otro de los derechos previsto en la LFTAIPG es el derecho de consulta por los interesados a un Registro público al que los responsables de los sistemas de datos personales notifiquen la existencia de los sistemas de datos de carácter personal, y que va a permitir a los interesados obtener información con el propósito de poder dirigirse a su responsable para ejercitar sus derechos, como se dispone en el artículo 23 de la LFTAIPG y en el artículo 48 del Reglamento de la LFTAIPG.

Finalmente, en las legislaciones internacionales existen otros derechos, como el derecho de oposición recogido en la Directiva 95/46/CE europea[5] y que consiste en que el interesado, en aquellos casos en los que no resulte necesario su consentimiento para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos, pero la breve normativa mexicana, no específica en protección de datos, no lo contempla. Asimismo, la norma europea 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.

Transferencia Internacional de Datos

En otro orden de cosas, como un tema especialmente polémico, podemos hablar de la transferencia Internacional de Datos (TID), que implica un flujo de datos personales entre diversos países, lo que ha hecho surgir la necesidad de adecuar dichos tratamientos a las previsiones legales establecidas en los distintos ordenamientos jurídicos.

Tenemos que tener en cuenta que la realización de transferencias internacionales de datos no es un supuesto extraño, sino que muy al contrario está presente en la actividad diaria de muchas entidades que tienen presencia internacional, al mismo tiempo que las Administraciones Públicas también pueden requerirlo.

La legislación europea, que es la única que puede denominarse así, pues la regulación estadounidense es escasa y dispersa, establece como principios que rigen la TID los siguientes:

- ❒ Prohibición de transferencias a un país tercero que no garantice un nivel de protección adecuado (art. 25.1 Directiva 95/46/CE).
- ❒ La Comisión podrá adoptar una Decisión en la que establezca que un país tercero garantiza un nivel de protección adecuado, en cuyo caso los Estados miembros tendrán que adoptar las medidas necesarias para adecuarse a la misma (art. 25.6 Directiva 95/46/CE).

Por otro lado, en el artículo 26 de la Directiva 95/46/CE se prevé una solución contractual específica en el caso de aquellas transferencias de datos que se efectúan con destino a países que no proporcionan un nivel adecuado de protección. En este sentido, las cláusulas contractuales tipo, que han sido aprobadas mediante las correspondientes Decisiones de la Comisión, en función de cuál sea la finalidad de la transferencia, se refieren únicamente a la protección de datos, pudiendo añadirse por las partes del contrato aquellas otras cláusulas que sean necesarias para el desarrollo de su negocio.

Por su parte la normativa mexicana sobre la materia realiza la siguiente referencia:

> Lineamiento 24: *En caso de que el o los destinatarios de los datos sean personas o instituciones de otros países, las dependencias y entidades deberán asegurarse que tales países garanticen que cuentan con niveles de protección semejantes o superiores a los establecidos en estos Lineamientos, y en la normatividad propia de la dependencia o entidad de que se trate.*

Para finalizar este apartado, cabe mencionar la existencia y, en nuestra opinión, necesario fomento de la utilización de códigos de conducta, éticos o deontológicos especialmente aptos para adaptar los diversos preceptos de una ley a las características específicas de cada sector, y, en la materia objeto de nuestro estudio en concreto, lo que se pretende conseguir con estos códigos es que todo aquél que intervenga en el tratamiento de datos asimile y se conciencie de la importancia de la protección de los datos de carácter personal.

El órgano de control

El órgano de control, en el ejercicio de las funciones que se le atribuyan, ha de velar por el cumplimiento de la normativa sobre protección de datos, para lo cual puede ejercer, entre otras, las potestades inspectora, sancionadora y cualesquiera otras que se le asignen, como dar publicidad de los sistemas de datos de carácter personal que hayan sido inscritos o notificados a través del órgano correspondiente.

En la propia LFTAIPG se atribuyen determinadas funciones al Instituto Federal de Acceso a la Información Pública Gubernamental (IFAI) en relación con la normativa en protección de datos y las obligaciones al respecto que la LFTAIPG dispone, aunque, partiendo de la base de que dicha ley no es una norma en protección de datos, tampoco puede concluirse que el IFAI, consecuentemente, sea una autoridad o órgano de control en la materia, como en las normativas internacionales se configura.

En el caso de México, y dentro de la breve referencia que en la norma analizada se realiza a la protección de datos, se dispone en el artículo 33 de la LFTAIPG lo siguiente:

> *"El Instituto Federal de Acceso a la Información Pública es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades."*

El IFAI se regula en el artículo 37 de la LFTAIPG que le atribuye, entre otras, las funciones de:

> *"I. Interpretar en el orden administrativo esta Ley, de conformidad con el Artículo 6;*
> *II. Conocer y resolver los recursos de revisión interpuestos por los solicitantes;*
> *VIII. Elaborar los formatos de solicitudes de acceso a la información, así como los de acceso y corrección de datos personales;*
> *IX. Establecer los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales, que estén en posesión de las dependencias y entidades;"*

En este mismo sentido, hay que tener en cuenta lo previsto en el artículo 62 del Reglamento de la LFTAIPG al establecer:

> *"Sin perjuicio de lo dispuesto por el artículo 37 de la Ley, el Instituto podrá:*
> *I. Diseñar procedimientos y establecer sistemas para que las dependencias y entidades reciban, procesen, tramiten y resuelvan las solicitudes de acceso a la información, así como a los datos personales y su corrección;*
> *II. Establecer sistemas para que las dependencias y entidades puedan enviar al Instituto resoluciones, criterios, solicitudes, consultas, informes y cualquier otra comunicación a través de medios electrónicos, cuya transmisión garantice en su caso la seguridad, integridad, autenticidad, reserva y confidencialidad de la información y genere registros electrónicos del envío y recepción correspondiente;"*

El IFAI cumple con alguna de las funciones en materia de control y tutela de los derechos de la normativa en protección de datos, sin que pueda afirmarse que exista en México, en la actualidad, un verdadero procedimiento en la materia, al estilo de lo que se ha denominado el “habeas data” como mecanismo de protección y tutela del ciudadano que se ve lesionado en su derecho a la protección de datos.

En México este procedimiento ante el IFAI se regula en los artículos 49 a 60 de la LFTAIPG, pudiendo iniciarse en concreto ante la negación de acceso a la información o la inexistencia de los documentos solicitados (artículo 49 LFTAIPG).

Por su parte, la LFTAIPG prevé como causas de responsabilidad las acciones y omisiones que se indican en el artículo 63, entre las que destacamos las siguientes:

I. Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de manera indebida información que se encuentre bajo su custodia, a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

II. Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a la Ley;

III. Denegar intencionadamente información no clasificada como reservada o no considerada confidencial conforme a la Ley;

V. Entregar información considerada como reservada o confidencial conforme a lo dispuesto por la Ley;

VI. Entregar intencionadamente de manera incompleta información requerida en una solicitud de acceso, y

La responsabilidad por el incumplimiento de alguna de las obligaciones establecidas en la LFTAIPG será exigida conforme a lo dispuesto en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, resaltando, de nuevo, que las sanciones se refieren a la “información”, pues, de nuevo, tenemos que repetir que la LFTAIPG sólo destina un capítulo, de 7 artículos, y algunas referencias más dispersas, a la protección de datos.

Breve conclusión

La protección de datos es una materia fundamental dentro del entorno de las consecuencias jurídicas del uso de las nuevas tecnologías. En países de tradición legislativa debe añadirse al espectro regulatorio, estando éste incompleto sin contar con una normativa de este tipo.

Debe tenerse en cuenta, a este respecto, los principios y derechos que conforman la estructura de dichas leyes, procurando encontrar un equilibrio entre la protección individual y el desarrollo empresarial y comercial.

Finalmente, la existencia de un órgano de control deviene imprescindible, quedando su estructura y composición, así como su funcionamiento y facultades, necesitadas de concreción y ajuste al entorno socio cultural en concreto, siempre manteniéndose unos mínimos requisitos.

---

[1] Ley de protección de datos personales del Estado de Colima, aprobada por Decreto número 356 de 14 de junio de 2003.

[2] Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), publicada en el Boletín Oficial del Estado número 262, de 31 de octubre

[3] Ley federal de transparencia y acceso a la información pública gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2002, reformada el 11 de mayo de 2004.

[4] Reglamento de la ley federal de transparencia y acceso a la información pública gubernamental, Diario Oficial de la Federación de 11 de junio de 2003

[5] 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).