BREVE ANÁLISIS DE LA REFORMA AL ARTÍCULO 6o. CONSTITUCIONAL EN LO RELATIVO A PROTECCIÓN DE DATOS PERSONALES

Isabel DAVARA F. DE MARCOS*

SUMARIO: I. *Planteamiento*. II. *Los principios*. III. *Los derechos*. IV. *La autoridad de control*. V. *Comentarios a la reforma constitucional*. VI. *Como conclusión*.

En el presente trabajo analizaremos la reciente reforma al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos con relación a la protección de datos personales. No obstante, antes de entrar en la interpretación de dicha reforma, haremos un breve planteamiento de lo que una normativa en protección de datos conlleva, mencionando casos internacionales y nacionales.

I. 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

* Davara Abogados.

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,[1] 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.

En este mismo sentido, las normativas en protección de datos persiguen proteger al individuo frente al ilícito tratamiento de la información personal que le concierne. Por lo tanto, los conceptos, si bien entrelazados, e incluso a veces confusos y confundidos, son distintos. La intimidad o vida privada cada sujeto la define en función de sus preferencias, si bien, por supuesto, existen unas reglas en derecho que impiden ciertas intrusiones abusivas, mientras que la privacidad, derivada del tratamiento de los datos, aunque pueda ser manejada en cierta medida por su titular, principalmente por medio del consentimiento, está sujeta a unas normas establecidas para controlar el tratamiento de los mismos.

Podemos decir, continuando con la exposición anterior, que privacidad es un término que se utiliza para referirnos al perfil que se puede obtener de una persona con el tratamiento, generalmente automatizado, de sus datos de carácter personal y que el individuo tiene derecho a exigir que permanezca en su esfera interna, en su ámbito de privacidad.[2]

1 Véase Davara Rodríguez, M. A., "La protección de datos en España: principios y derechos", *Actualidad Informática Aranzadi*, Pamplona, núm. 13, 1994, pp. 1 y ss.

2 El ministro de Justicia español, al presentar el proyecto de lo que luego sería la antigua LORTAD española en el Congreso de los Diputados, dijo del entonces inexistente vocablo de privacidad: "Creo que es una formulación singular la de la propia Constitución, porque la intimidad y el honor ya están regulados en

Además, la importancia del tratamiento por medios informáticos ha tenido una especial incidencia, pues las fronteras de tiempo y espacio, que protegían en gran manera la intimidad del individuo, han desaparecido en cierto modo, o, al menos, se han modificado sustancialmente, haciendo que la información personal se pueda tratar, comunicar, conservar, manipular, etcétera, en muy distintos modos y maneras.

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, no ya de 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.

Al intentar definir qué se puede entender por protección de datos, continuamos siguiendo a Davara,[3] que entiende al respecto:

> el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad.

Es decir, el individuo es el titular del derecho. Es un derecho subjetivo, no se trata de una protección de la información *per se*,

ella, pero aquí se habla de limitar el uso de la informática. Es, sin duda, un concepto nuevo el que aquí se está afrontando; es algo distinto, es una nueva dimensión que corresponde a unos nuevos medios tecnológicos y a un nivel de desarrollo que, seguramente, es algunos años después de la Constitución cuando empieza a mostrar su auténtica dimensión y, en ese sentido, también su auténtico peligro... el uso frecuente de medios informáticos amenaza con hacer que el perfil de cada cual pueda ser conocido por cualquier persona, en cualquier sitio y en cualquier momento, afectando por eso a una dimensión nueva", *Diario de Sesiones del Congreso de los Diputados*, núm. 151, IV Legislatura, 1991, r. 7572.

3 Véase, Davara Rodríguez, M. A., *Nueva guía práctica de protección de datos. Desde la óptica del titular del fichero*, Madrid, ASNEF, 2001, p. 17.

sino de la protección del individuo a que dicha información concierne.[4]

En otro orden de cosas, el análisis de la protección de datos puede estructurarse en un triángulo cuyos tres vértices se denominarían principios, derechos y procedimiento, respectivamente. Así, diríamos 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. 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 concretan los principios teóricos en los que se basa toda la normativa. El procedimiento, finalmente, cerrando este triángulo ficticio, concreta la tutela estatal a la que el individuo puede recurrir cuando se ve lesionado en el ejercicio de esos derechos como consecuencia de tales principios.

Por otro lado, en el tratamiento de datos de carácter personal podemos distinguir varias fases claramente diferenciadas: la recogida de los datos, el tratamiento de los mismos y la utilización del resultado del tratamiento, así como, en su caso, la cesión de datos a un tercero. En cada una de esas fases tenemos que atender al respe-

4 Por su parte, en los ordenamientos anglosajones, el derecho a la privacidad se encuadra en los derechos de la propiedad. En el conocidísimo artículo de los jueces del Tribunal Supremo, Samuel D. Warren y Louis D. Brandeis de finales del siglo XIX, se explica la evolución de dicho derecho, apoyándose en un tratado muy renombrado sobre injurias de otro juez, llamado Cooley, donde defendía el derecho a "ser dejado en paz", y comienzan así a definir lo que en dichos ordenamientos se entiende la privacidad en la era moderna. No obstante, hay que tener en cuenta, en primer lugar, que se trata de un artículo de 1890, por lo que obviamente las preocupaciones hay que ponerlas en consonancia con las entonces existentes, pero, sobre todo, no deja de llamar la atención, en nuestra opinión, la idea de que se refirieran a "*aparatos mecánicos*", lo que podría, en una exégesis muy amplia, englobar el posterior desarrollo de la electrónica, y que ya se pudiera pergeñar el daño que la intrusión en la privacidad del individuo podía causar. Véase "The Rigth to Privacy", *Harvard Law Review*, vol. IV, 15 de diciembre de 1890, núm. 5, consultado, con modificaciones, en *http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html*, 2 de julio de 2004.

to de todos los principios[5] y derechos[6] prescritos en la normativa. De esta manera, si no se cumple con alguno, el tratamiento se convierte inmediatamente en ilícito.

Como hito histórico, la conocida sentencia del Tribunal Federal Alemán de 1983,[7] sobre la licitud del tratamiento de los datos del censo de un ciudadano alemán, abrió un nuevo e importante camino, al menos doctrinal, en la protección de datos en Europa e internacionalmente. Podemos decir que en esta sentencia se asienta el conocido principio a la autodeterminación informativa (que la doctrina, en un juego de palabras, en muchas ocasiones denomina "autodeterminación informática") que señala que el titular de los datos es el único que tiene derecho a decidir cómo, cuándo, dónde y por quién se tratan sus datos y que dará lugar a un importante desarrollo normativo.[8]

5 Consentimiento, calidad, información, datos especialmente protegidos, datos de salud, medidas de seguridad, deber de secreto, comunicación de datos y acceso a los datos por cuenta de terceros que veremos un poco más detalladamente después.

6 Acceso, rectificación, supresión, oposición, impugnación de valoraciones, acceso al Registro General de Protección de Datos, recurso a las vías ordinarias, que veremos más adelante.

7 La Ley alemana del Censo de Población de 1983 fue aprobada por el Bundestag, el 4 de marzo de 1983. Se presentó un recurso de amparo constitucional el 5 de marzo de ese mismo año por una ciudadana que reclamaba que la Ley del Censo lesionaba los derechos protegidos en los artículos 1o., 2o., 5o. y 19 de la Ley Fundamental de Bonn, en particular el derecho al libre desenvolvimiento de la personalidad y a la dignidad humana, la libertad de expresión y las garantías procesales. El recurso dio lugar a una sentencia cautelar del Tribunal Constitucional del 13 de abril que concluía que existían fundamentos para la suspensión provisional de la vigencia de la Ley hasta la resolución de fondo, que se produjo mediante la sentencia de 15 de diciembre de 1983 y que anula parcialmente la Ley impugnada. Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, *Boletín de Jurisprudencia Constitucional*, 1984, pp. 126 y ss.

8 En términos normativos, en Europa, además de las resoluciones del Comité de Ministros de 1973 y 1974 (resolución R (74) 29 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector público, adoptada el 20 de septiembre de 1974, en la 236a. reunión del Consejo de Ministros), pasando por el Convenio 108 (Convenio (108) del Consejo de Europa, para la protección de las personas con relación al tratamiento

No obstante, en México no existe aún una ley específica a nivel federal que regule la protección de datos personales, si bien el estado de Colima sí cuenta con una regulación concreta,[9] que sigue en gran medida la antigua, derogada y ya mencionada LORTAD española.

La primera referencia a nivel constitucional se encontraba hasta el pasado 20 de julio de 2007 en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos que establece que "nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones". Sin embargo, como decíamos, con la publicación,

automatizado de los datos de carácter personal, de 28 de enero de 1981, firmado en Estrasburgo por el plenipotenciario de España el 28 de enero de 1982 y ratificado mediante instrumento de 27 de enero de 1984 (*Boletín Oficial del Estado*, núm. 274, 15/9/1985) del Consejo de Europa, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal y a la libre circulación de estos datos de 28 de enero de 1981; 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 (*D.O*. L 281, 23/11/1995), por su parte, vino a asentar un régimen normativo específico, un marco definido para esta teoría con el mandato consecuente de implantación para todos los Estados miembros, asimismo la directiva 2002/58 del Parlamento Europeo y del Consejo, de 12 de julio, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas, *D.O*. L 201, 31/7/2002), hace lo propio en el sector de las comunicaciones electrónicas. Finalmente, como hito importante, la Carta Europea de Derechos Fundamentales (Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000), en su artículo 8o., señala el derecho a la protección de datos de carácter personal como uno de los derechos fundamentales en el ámbito europeo. En España, en particular, tenemos que remontarnos a la Constitución Española de 1978 (*Boletín Oficial del Estado*, núm. 311, de 29 de diciembre de 1978), que en su artículo 18.4 remite a desarrollo legal, desarrollo que no fue realidad sino hasta 14 años después, con la 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*, núm. 262, del 31 de octubre, que fue la antecesora de la actual Ley Orgánica 15/99 de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el *Boletín Oficial del Estado*, núm. 298, de 14 de diciembre.

9 Ley de Protección de Datos Personales del Estado de Colima, aprobada por decreto núm. 356 del 14 de junio de 2003.

el mencionado pasado 20 de julio de 2007, en el *Diario Oficial de la Federación*, en sus páginas 2 y 3, del "Decreto por el que se adiciona un segundo párrafo con siete fracciones al artículo sexto de la Constitución Política de los Estados Unidos Mexicanos", se hace una referencia explícita a la protección de datos personales, si bien dentro del artículo destinado al derecho de acceso a la información. No obstante, para detenernos someramente en el análisis de esta reforma entendemos que antes debemos hacer una breve aproximación a la protección de datos en general, por lo que volveremos posteriormente a este análisis en concreto.

A pesar de lo anterior, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (en adelante, LFTAIPG),[10] que, si bien es una norma cuyo objeto es, según dispone su artículo 1o., "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", regula directamente 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.[11]

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

10 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el *Diario Oficial de la Federación* del 11 de junio de 2002, y reformada el 11 de mayo de 2004.

11 De igual modo, esta Ley tiene toda una regulación de desarrollo y, específicamente, en protección de datos, que iremos mencionando concisamente a lo largo del trabajo, en concreto: Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (primera sección) (*Diario Oficial de la Federación* del 11 de junio de 2003); lineamientos que deberán observar las dependencias y entidades de la administración pública federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares (*Diario Oficial de la Federación* del 6 de abril de 2004); Lineamientos de Protección de Datos Personales (*Diario Oficial de la Federación* del 30 de septiembre de 2005).

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.

Para analizar entonces los elementos que una regulación en protección de datos debe contener, pasamos a continuación a analizar brevemente la manera en que la LFTAIPG trata los elementos principales de la regulación en protección de datos antes mencionados, pues aun no siendo una ley de protección de datos propiamente dicha, es la que más contenido tiene al respecto. Sin embargo, añadiremos aquellas cuestiones de las que la Ley adolece realizando un análisis doctrinal al respecto basado en las normas internacionales en la materia.

II. Los principios

Como eje central de las normativas en protección de datos, el principio del *consentimiento* por el cual 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 comentado antes), se articula también en cierta medida en el capítulo IV de la LFTAIPG en sus artículos 21 y 22.

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 original 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.[12]

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 en 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.

De las características que conforman el consentimiento se dice en la doctrina y el derecho comparados que debe ser:[13] *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).

12 "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".

13 Véase, siguiendo a Castán Tobeñas, Alonso Martínez, C., *Protección de datos de carácter personal. El consentimiento en entidades financieras*, Madrid, ASNEF, 2002, pp. 56-69.

Por otro lado, en cuanto a la forma en la que se puede otorgar el consentimiento, con carácter general cabe distinguir[14] entre consentimiento presunto, tácito, expreso y por escrito.[15] En cualquiera de los casos señalados, la cuestión se concentra en la prueba de la obtención del consentimiento. Es decir, tanto en el consentimiento tácito, principalmente, como en el expreso que no sea escrito, parece que hay que implementar procedimientos estandarizados de recogida de dicho consentimiento para que luego se pueda probar la obtención del mismo. Dicha prueba recae en quien solicita el consentimiento para el tratamiento de datos de carácter personal, es decir, el responsable del archivo. Por tanto, deberá hacerse uso de vías que permitan acreditar que se solicitó del interesado una manifestación en contra para oponerse al tratamiento de sus datos, de manera que su omisión pueda ser entendida como consentimiento al tratamiento, dando un plazo prudencial para que el interesado pueda conocer que su omisión implica la aceptación del tratamiento.

No obstante, este consentimiento tiene excepciones, y la ley las recoge también (según señala con carácter general el reformado artículo 6o. de la Constitución), aunque de nuevo la LFTAIPG lo hace 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

14 Si se atiende a la regulación de la temida LOPD española, por ejemplo, puede concluirse que en algunos casos tiene que ser expreso (datos que hagan referencia al origen racial, a la vida sexual y a la salud), exigiéndose en otros que sea expreso y por escrito (datos relativos a ideología, afiliación sindical, religión y creencias), y finalmente en el resto de los casos puede ser tácito o expreso (véase la argumentación de la Agencia Española de Protección de Datos en su *Memoria*, 2000, p. 381).

15 Aunque no parece necesario volver a recalcarlo, en un trabajo dedicado al derecho de las tecnologías de la información y las comunicaciones, el concepto de escrito no puede circunscribirse al soporte papel.

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.[16]

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

16 Es cierto que hay quienes defienden que el principio fundamental es el de calidad de los datos, argumentando que este principio 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 el eje del mismo. El hecho de que tenga excepciones no quiere decir que no sea la regla, sino más bien lo contrario. 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 los mismos con una finalidad determinada. Si bien es absolutamente imprescindible definir la finalidad del tratamiento, en cuanto 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. En definitiva, no consideramos que pueda decirse que porque nunca se pueda prescindir de la calidad del tratamiento (como tampoco de la seguridad del mismo por ejemplo), deba entenderse que una cualidad adjetiva de dicho tratamiento deba ponerse por encima de la manifestación de voluntad del sujeto titular del derecho, aunque, reiteramos, esta manifestación pueda ser excepcionada en algunos casos.

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 *unas categorías especiales de datos*[17] 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 a personas no autorizadas el acceso a los sistemas de datos personales, en particular, y a los datos en general, o para evitar el desvío de la información, malintencionadamente o no, hacia sitios no previstos, además de para garantizar el tratamiento de datos en 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 perso-

17 Algunos autores denominan estos datos como sensibles, pero preferimos continuar con la nomenclatura legal, de un lado, porque nos parece más formal, pero sobre todo porque esta denominación no implica en ningún caso una carga subjetiva, sino un criterio objetivo, que tan sólo apunta al especial tratamiento que merecen estas categorías de datos.

nales de: "Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado".[18]

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 res-

18 Además de que alguna de las normas ya mencionadas, como los lineamientos, establecen consideraciones al respecto, resultan muy interesantes las recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidas por el IFAI a modo de "propuestas y sugerencias específicas para lograr la mayor protección de los datos personales, por lo que las dependencias y entidades podrán utilizarlas como modelo a seguir, para lograr con ello un estándar de seguridad, sin perjuicio de que éstas establezcan medidas adicionales que coadyuven a la mejor protección mencionada". Recomendaciones disponibles en: *http://www.ifai.org.mx/datos_personales/seguridad/Recomendaciones_SDP.pdf*.

ponsable 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.

III. Los derechos

Vistos los principios que rigen el tratamiento de datos, según habíamos explicado anteriormente, la normativa prevé la existencia de ciertos 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 brevemente 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.

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 finali-

dad 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 y a los ya mencionados lineamientos emitidos al efecto.

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, ya citada, y que consiste en que el titular, 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, repetimos, no es 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 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.

IV. La autoridad de control

Para cerrar el triángulo del que hablábamos al principio, tenemos que tratar el vértice procedimental, al que puede recurrir el titular de los datos lesionado en sus derechos. En el caso mexicano, al ser esta regulación muy escasa, lo cierto es que más que de procedimiento vamos a hablar de la necesaria existencia de una autoridad de tutela ante la que se gestionaría dicho procedimiento.

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 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 propia 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 u 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, que 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.[19]

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 6o.;

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;[20]

19 En España, por poner un ejemplo de un país concreto de similar tradición jurídica y en este caso de más asentado respeto a la materia, en principio existen dos procedimientos diferenciados en materia de protección de datos: el denominado "tutela de derechos" y el "procedimiento sancionador". En realidad, para ser puristas, el único procedimiento que el titular de los datos puede originar es el de tutela de derechos, es decir, cuando se ve lesionado en sus derechos puede acudir ante el órgano competente, la Agencia Española de Protección de Datos en el ámbito nacional y las agencias autonómicas (locales/"cuasi federales") existentes en el caso de los ficheros públicos de las comunidades autónomas que cuenten con dicha agencia. El procedimiento sancionador, por su parte, sólo puede ser instado por la agencia, por su director, aunque pueda traer causa, sin que esto sea muy formal decirlo, de una denuncia previa y un expediente de tutela de derechos.

20 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...".

Como decíamos, 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 de la LFTAIPG).

Asimismo, la LFTAIPG prevé como causas de responsabilidad las acciones y omisiones que se indican en el artículo 63.[21]

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 tenemos que repetir que la LFTAIPG sólo destina un capítulo, de siete artículos, y algunas referencias más dispersas, a la protección de datos.

Además, dentro de la normativa de protección de datos de carácter personal hay muchos otros temas de especial relevancia, co-

21 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...

mo la transferencia internacional de datos,[22] el tratamiento de datos de salud o de datos con fines de solvencia patrimonial y crédito, el tratamiento de datos en el entorno de las telecomunicaciones, o, finalmente, 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, para que todo aquel que intervenga en el tratamiento de datos asimile y se tome conciencia de la importancia de la protección de los datos de carácter personal. Todos ellos son aspectos concretos de la regulación que sería imposible tratar en este trabajo por razones de espacio, pero que dejamos simplemente apuntado para elaboraciones futuras.

22 En el caso concreto de las transferencias internacionales de datos, éstas implican un flujo de datos personales entre diversos países, que hace necesario adecuar dichos tratamientos a las previsiones legales establecidas en los distintos ordenamientos jurídicos. La legislación europea marco establece como principios que rigen las transferencias internacionales de datos los siguientes: 1. Prohibición de transferencias a un país tercero que no garantice un nivel de protección adecuado (artículo 25.1 directiva 95/46/CE).

2. 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 (artículo 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, 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 otras cláusulas que sean necesarias para el desarrollo de su negocio.

Por su parte, la normativa mexicana en el lineamiento 24 dice: "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".

V. Comentarios a la reforma constitucional

Pasando finalmente a lo que en realidad originaba nuestra disertación, esto es, la inclusión en la Constitución de un nuevo artículo 6o. que engloba a la protección de datos, si bien dentro del derecho al acceso a la información del ciudadano, tenemos en este sentido que expresar en primer lugar sucintamente nuestra opinión acerca de dicha inserción.

A este respecto, consideramos que nuestra opinión se podría resumir, con los riesgos que ello conlleva, en lo ya dicho anteriormente respecto del objeto de la LFTAIPG, es decir, que dicha colocación dentro del artículo del derecho de acceso puede llegar a parecer, a no ser que se profundice en la interpretación, que también la Constitución plantea a los datos personales como un límite al acceso a la información, cuestión que, como decíamos, entendemos desafortunada, pues, más que límite, es, en todo caso, complemento.

Entrando ahora en el análisis concreto de dicho nuevo artículo, en lo que afecta a protección de datos personales, la reforma ha sido la siguiente:

> Artículo Único. Se adiciona un segundo párrafo con siete fracciones al artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:
>
> Artículo 6o. ...
>
> Para el ejercicio del derecho de acceso a la información, la Federación, los estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> (…) II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

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

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

Como breves comentarios a esta reforma, podemos hacer los siguientes:

1. En todo caso, alabamos la inclusión en el texto constitucional del absolutamente ya reconocido y establecido internacionalmente derecho a la protección de datos. Pero no podemos dejar de preocuparnos, como decíamos, ante la colocación de la referencia, como un límite al derecho de acceso a la información aparentemente. Las interpretaciones siempre son peligrosas en el derecho, y nos inquieta que el legislador no profundice sobre el verdadero sentido de la protección de datos, de manera independiente. No obstante, ya tenemos no sólo conocimiento sino participación en alguna iniciativa de reforma constitucional al artículo 16 de la Constitución que consagraría de manera independiente la tan necesitada y urgente reforma que incluyera a los datos personales y la indispensable protección frente a un tratamiento ilícito. Con dicha reforma confiamos en que se cierre el círculo y se dé cabida independiente a ambos derechos, que, como decíamos, en muchos casos pueden llegar a ser complementarios.
2. El texto diferencia entre la vida privada y los datos personales. Como decíamos arriba, los conceptos se interrelacionan.[23]

23 En este sentido señala el dictamen de las Comisiones Unidas de Puntos Constitucionales y de la Función Pública, con proyecto de decreto por el que se reforma el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos, al comentar la iniciativa: "La fracción segunda. En ella se establece una

No obstante, por supuesto que la vida privada y los datos personales son dos cosas diferentes. Lo que la normativa en protección de datos personales trata de proteger es el tratamiento de la información personal por terceros, máxime en un entorno automatizado. El concepto de vida privada es más subjetivo, y depende de parámetros personales e individuales.[24] La normativa gira en torno a cuestiones objetivas, donde el tratamiento de los datos personales, públicos o privados, tiene que seguir ciertas reglas. Sin embargo, lo que sí resulta en todo caso resaltable, como decíamos, es que se exige la protección.

3. El párrafo III ordena: "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", puede parecer algo exagerado si no se analiza un poco más detenidamente. No se está otorgando nada que no se deba, salvo una precisión acerca de la gratui-

segunda limitación al derecho de acceso a la información, misma que se refiere a la protección de la vida privada y de los datos personales. Esta información no puede estar sujeta al principio de publicidad, pues pondría en grave riesgo otro derecho fundamental, que es el de la intimidad y la vida privada. Es fundamental esclarecer que aunque íntimamente vinculados, no debe confundirse la vida privada con los datos personales. La primera se refiere al ámbito de privacidad de las personas respecto de la intervención tanto del Estado como de otros particulares. Los datos personales, en cambio, son una expresión de la privacidad". No estamos del todo de acuerdo con esta diferenciación, sino que más bien, como decimos, entendemos que los datos personales, privados o no, son relativos a la información personal del titular que serán, en su caso, sometidos a tratamiento. Y, además, por supuesto, son un derecho fundamental diferente e independiente del de la intimidad.

24 Siguiendo así a Davara que, en su *Manual de derecho informático*, diferencia entre datos públicos y privados, dependiendo del grado de secreto a los que se les someta, y, dentro de los privados distingue, a su vez, entre íntimos y secretos, según la confidencialidad con la que se traten, e, incluso, dentro de los secretos, diferenciando asimismo entre profundos y reservados, huyendo de otras calificaciones doctrinales más subjetivas que utilizan adjetivos como sensibles para destacar ciertos datos. Véase, Davara Rodríguez, *Manual de derecho informático,* Pamplona-Navarra, Aranzadi Thomson, 2005, pp. 117 y ss.

dad infinita que haremos a continuación. El titular tiene acceso a sus datos, porque son suyos. El hecho de que no tenga que acreditar interés o justificar nada es porque accede a algo que le concierne a él mismo. No obstante, en relación con la rectificación creemos que, de nuevo, el desarrollo legal posterior deberá concretar este extremo. Cuando se va a rectificar un dato se tiene que demostrar, en lo que esto signifique en cada caso, que es erróneo, pues, de otra manera el titular del archivo podría tener consecuencias no deseadas. Es decir, no se tendrá que justificar la rectificación, o, en su caso, en un paso más allá, la cancelación, si por justificar se refiere el texto a, coloquialmente, "dar explicaciones", pero sí tendrá el titular de los datos, aunque esta sutil diferenciación parezca contradictoria, que probar, en la mayoría de los casos, de alguna manera dicha rectificación, aportando los datos pertinentes, adecuados y exactos.

4. No obstante, continuando con el párrafo III, y a pesar de que alabamos la intención garantista del Constituyente en relación con los derechos en que se concreta la protección de datos, es igualmente cierto que la excesiva apertura, especialmente en lo relacionado a la obligatoria gratuidad (párrafo III), que dicho derecho puede ocasionar problemas indeseados en la práctica, ya sea por negligencia, o, incluso, aprovechamiento por parte del no siempre indefenso titular de los datos. No obstante, si en el desarrollo legal —o reglamentario— posterior, se circunscribe este extremo de una manera justa y equitativa que no impida el comercio preservando dichas garantías, diciendo, por ejemplo, que será gratuito en la primera ocasión y siempre que no se repita en un plazo adecuado, entonces no veríamos ningún problema.
5. Por su parte, y como ya hemos visto en la exposición teórica antecedente, la concreción del extremo procedimental (párrafo IV) resulta indispensable. El único problema es que el párrafo sólo se refiere expresamente al acceso a la información. No obstante, en una labor exegética lo cierto es que po-

dríamos entender que también se tendría que hacer en las mismas condiciones para el acceso a datos personales. Y, si bien las interpretaciones excesivas son peligrosas, en una disertación como la presente podemos elucubrar un poco. En todo caso, lo que queremos resaltar es que sin el establecimiento de un procedimiento adecuado y expedito el derecho se quedaría vacío de contenido, al menos en parte. Es fundamental que se prevea una autoridad independiente, con plena capacidad de obrar y de decisión propias, que no tenga que estar sujeto a ningún poder en concreto, por lo menos en términos de sumisión. Hay que resaltar que la protección de datos es una materia que se introduce en todos los ámbitos de la sociedad en general. En la actualidad, no existe actividad alguna que no requiera en algún momento del tratamiento de la información personal y, por ende, no puede haber ningún ámbito que se sustraiga a la debida tutela.

6. Finalmente, las sanciones son imprescindibles, máxime en una materia como la que nos ocupa, de nueva introducción y gran desconocimiento, inclusive para el titular del derecho en sí. Sin unas adecuadas sanciones, severas pero proporcionadas al caso y las circunstancias, y un procedimiento eficaz y eficiente con una autoridad de tutela garantista, el derecho, como ya habíamos dicho, queda vacío de contenido, de fuerza y eficacia en la práctica.

VI. Como conclusión

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

La protección de datos es un derecho fundamental. El individuo tiene derecho a decidir cuándo, cómo y quién va a tratar su infor-

mación personal. En América Latina queda mucho trabajo por hacer en relación con la privacidad, pues la mayor parte de los países no tienen una regulación en la materia.

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 sociocultural en concreto, siempre manteniéndose unos mínimos requisitos.

La reforma al artículo 6o. constitucional, en lo relativo al derecho de acceso a la información, dedica unas importantes referencias a los datos de carácter personal. Si bien, como hemos repetido, resulta de alabar que dicha referencia se haga en un texto constitucional, en nuestra opinión, no debe hacerse exclusivamente como un límite al derecho de acceso a la información, ya que se trata de dos derechos fundamentales independientes entre sí, más complementarios que excluyentes, en su caso. En cuanto al contenido de la reforma, y reiterando que no se trata de una reforma de protección de datos en sí (que entendemos y esperamos que venga en camino en el artículo 16 de la Constitución), todavía adolece de algunas lagunas que hemos resumido en el presente trabajo, si bien reiterando, de nuevo, nuestra complacencia acerca de la referencia constitucional.