Protección de datos de carácter personal en México: problemática jurídica y estatus normativo actual

Isabel Davara F. de Marcos

I. Planteamiento

Últimamente todos hablan de la protección de datos de carácter personal y su posible y futura legislación en México.

Lo cierto es que actualmente no existe actividad, pública o privada, comercial o no, que pueda sobrevivir sin tratamiento de datos de carácter personal (administrados, clientes, personal, etc.).

Es más, en nuestra opinión, el único valor añadido que la industrializada producción tiene hoy es el conocimiento de los destinatarios de sus productos y servicios, fabricados todos de manera muy similar, y la difícil competencia sólo encuentra dicha diferenciación en tanto en cuanto se conoce al consumidor final.

Y, dando un paso más allá, consideramos que hoy en día en realidad nuestra "identidad virtual" es incluso más importante, al menos cuantitativamente hablando, que nuestra única hasta el momento identidad física.

Y así dice Rodotà: "Las tecnologías de la información y de la comunicación están rediseñando el mundo, las relaciones personales, sociales, políticas y económicas. Pero esta transformación tiene un precio. (…) es justamente la información la que viene a constituir ahora la materia prima más importante y que, dentro de la información, los datos personales son especialmente preciados. (…) nuestra propia vida está volviéndose hoy en día un intercambio continuo de informaciones (…) la protección de datos asume una importancia creciente, que la conduce cada vez más hacia el centro del sistema político-institucional1".

Por otro lado, podría parecer que en esta cuestión existen posiciones extremistas, o, más bien diríamos, que hay quien puede estar interesado en hablar de posturas radicales, y fomentar así incertidumbre y prejuicios, sin contar con quienes pretenden reducir su importancia a las usuales quejas de los particulares en temas de publicidad y marketing no consentidos2.

Es en consecuencia nuestra intención plantear aquí un enfoque general de la materia, para lo que partiremos en primer lugar de algunas consideraciones preliminares que intentarán clarificar algunos extremos confusos. Continuaremos adentrándonos en la historia de este derecho a la protección de datos personales en el entorno internacional, siguiendo con el análisis de la situación nacional del mismo, para ya poder intentar analizar los elementos que componen este derecho, distinguiendo entre principios, derechos y procedimiento. Posteriormente trataremos algunas cuestiones específicas como la transferencia internacional de datos, para pasar al análisis de las reformas constitucionales, y así terminar finalmente con unas breves reflexiones a modo de conclusión.

II. Algunas consideraciones preliminares

Primera

La denominación de "protección de datos personales" ya conduce a confusión. El dato, en sí mismo, no necesita protección alguna. Sin embargo, cuando el dato se une a una persona, es algo distinto. Ya no protegemos, entonces, al dato, sino al titular del mismo, a la persona. Es más, cuando el dato se une a la persona se convierte en información personal3.

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. Es decir, el individuo es el titular del derecho. Es un derecho subjetivo, no se trata de una protección de la información per se, sino de la protección del individuo a que dicha información concierne.

Y es precisamente la información la que tiene relevancia en la sociedad de hoy en día. Tanto así que se habla de Sociedad de la Información –distinta de la Sociedad del Conocimiento, pero éste es un tema en el que no podemos divagar en este momento- empujada por la inmensa magnitud de información a nuestro alcance en la actualidad, gracias en gran parte a la existencia y uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC).

El valor de los datos personales es absolutamente innegable. De un lado, en términos de derecho de la personalidad, del individuo, y, de otro, aunque no nos guste excesivamente el planteamiento, en claros términos económicos4.

Y decimos lo anterior porque, aunque preferimos plantear el derecho como un derecho subjetivo fundamental de tercera generación, como veremos después, no es menos cierta su relevancia en términos mercantiles.

Es más, es precisamente esta importancia la que lleva a que sean tan codiciados y a que su reglamentación, además de debida por su cualidad jurídica, sea más que deseable.

Por una parte, desde el enfoque del que trata esos datos, es decir, la empresa o dependencia, hablando coloquialmente, con unos fines y utilidades determinados, para los que, como decíamos, constituyen un activo fundamental en su operación.

Pero, por otra parte, es el propio titular de los datos el que debería ser consciente, o al menos empezar a serlo, de su valor, y comenzar a actuar en consecuencia diligentemente respecto del tratamiento de su información personal5, decidiendo cada uno personal y conscientemente qué tipo de cuidado y límites desea para su información personal.

Es difícil, y hasta cuestionable, reclamar cuidado y tutela de un tercero sobre algo propio que no se cuida. Si el mismo titular no tiene diligencia sobre el cuidado de sus datos, y los entrega sin ninguna cautela, incluso llegando a comerciar con ellos a cambio de meras baratijas, después no puede enfurecerse por un tratamiento posterior que incluso él ha podido propiciar y en ocasiones hasta consentir.

Segunda

En esta materia se interrelacionan y mezclan muchos conceptos, como intimidad, privacidad y datos personales.

En cuanto a la intimidad, 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 personas6. Esta intromisión, que en algunos casos no tiene por qué ser negativa, ni mucho menos ilícita, se percibe como una amenaza potencial, desconocida.

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, se han difuminado sustancialmente, haciendo que la información personal se pueda tratar, comunicar, conservar, manipular, etc., de muy diferentes 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.

La concepción cerrada y estática del derecho a la intimidad pasa a una abierta y dinámica, que implica el reconocimiento no sólo de un derecho sino de nuevos mecanismos de protección.

En relación con la privacidad7, la privacidad es un término más profundo que la intimidad8, concepto más conocido y común en ordenamientos jurídicos de nuestro entorno, mientras que en el entorno anglosajón9 se usa indistintamente la palabra privacy entremezclada con la intimidad, y de ahí también que al castellanizar el término se fomente la confusión señalada.

Es un concepto más amplio porque está compuesta por diversas 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.

Podemos afirmar, por tanto, que privacidad es un término que se utiliza para referirnos al perfil que se puede obtener de una persona con el tratamiento de sus datos de carácter personal y que el individuo tiene derecho a exigir que permanezca en su esfera interna, en su ámbito de privacidad10.

En definitiva, los conceptos, si bien entrelazados, e incluso a veces confusos y confundidos, son distintos.

Cada sujeto define la intimidad 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, debe estar sujeta a unas normas establecidas para controlar el tratamiento de los mismos11.

En relación con la vida privada. El término vida privada, que aparece entre otros en la reforma constitucional al artículo Sexto, añade un concepto más a tener en cuenta.

La vida privada podría entenderse como vida familiar, y, en este sentido, el derecho es individualista, se manifiesta especialmente al excluir interferencias ajenas, y, por ende, la tutela es estática, negativa.

Por su parte, en la protección de datos, como hemos dicho al hablar de privacidad, la tutela es dinámica, sigue los datos en circulación, y, además, ya no es individualista sino que implica una específica responsabilidad pública. El concepto de privacidad evoluciona desde su definición original como "derecho a ser dejado solo" hasta el derecho de mantener control de la propia información y construir la propia esfera privada12.

Así, señala la Exposición de Motivos de los Lineamientos de protección de datos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (en adelante, LFTAIPG): "Atendiendo a la evolución que ha ocurrido de la noción tradicional de intimidad o vida privada limitada al derecho de impedir interferencias ajenas, o al derecho a ser dejado solo, hasta el derecho de mantener el control de la propia información y de determinar la forma de construcción de la propia esfera privada que el derecho a la protección de los datos personales se presenta como un elemento esencial para el libre desarrollo de la persona en las sociedades democráticas".

En cuanto a los datos personales, La relevante Sentencia del Tribunal Constitucional español 292/00, de 30 de noviembre, instaura jurisprudencialmente en España la autonomía e independencia del derecho fundamental a la protección de datos, diferenciándolo claramente de otros cercanos, como el de la intimidad13.

Y así señala en su Fundamento Jurídico Sexto: "el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado(...) atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer."

Igualmente reconoce la Exposición de Motivos de los Lineamientos antes mencionados: "… a efectos de lograr un uso racional y ético de las tecnologías, en el concierto de las naciones se ha legislado en materia de protección de datos personales, por lo cual los individuos gozan de un nuevo derecho denominado a la autodeterminación informativa, como garantía del ciudadano en las modernas sociedades frente al desafío del tratamiento electrónico de sus datos, entendida la garantía como la facultad del individuo de decidir quién, cuándo y bajo qué circunstancias utiliza sus datos personales, tanto en el sector público como en el privado".

Tercera

¿Qué podemos entender, entonces, por protección de datos personales? Al intentar definir qué se puede entender por protección de datos, seguimos a Davara14, 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, 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".

Hondius, por su parte, define el derecho a la protección de datos como "aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos15".

Pérez Luño señala que "la protección de datos personales tendría por objeto prioritario asegurar el equilibrio de poderes sobre y la participación democrática en los procesos de la información y la comunicación a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos16".

En otro orden de cosas, siguiendo igualmente el planteamiento de Davara, 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 de 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 pública a la que el individuo puede recurrir cuando se ve lesionado en el ejercicio de esos derechos como consecuencia de esos principios.

Por otro lado, en el tratamiento de datos de carácter personal podemos distinguir tres fases claramente diferenciadas: la obtención de los datos, el tratamiento de los mismos, y la utilización del resultado del tratamiento, y, en su caso, transmisión de datos a un tercero. En cada una de esas fases tenemos que atender al respeto de todos los principios y derechos prescritos en la normativa. De esta manera, si no se cumple con alguno, el tratamiento se convierte inmediatamente en ilícito.

Cuarta

¿De qué tipo de derecho hablamos? Es un derecho subjetivo, fundamental, y de tercera generación. Es un derecho subjetivo en tanto en cuanto es el titular de los datos, la persona, la que ostenta dicho derecho, a la que se protege.

Es un derecho fundamental, así reconocido internacionalmente. No obstante, en México, se le acaba de dar cabida hace apenas un año, el pasado 20 de julio de 2007, en el reformado artículo Sexto Constitucional, si bien podrían caber dudas y realizarse disquisiciones doctrinales acerca de su reconocimiento como derecho fundamental o como mera garantía "institucional" que debe desarrollarse para adquirir dicha categoría.

Es un derecho de tercera generación. Se puede hablar de una primera generación de derechos civiles y políticos, seguidos de la segunda generación de derechos sociales y culturales, para llegar a una tercera generación de derechos de los pueblos o la solidaridad. Son derechos colectivos o comunitarios (por ejemplo, derecho a la autodeterminación, a la paz, al desarrollo, a la democracia, a la integración, a recibir y producir información equitativamente, al medio ambiente sano y ecológicamente equilibrado, a beneficiarse del patrimonio común de la humanidad…) que se encuentran en distintas etapas de desarrollo internacionalmente. Son, además, derechos que por un lado implican una defensa frente al Estado y, por otro, se pueden demandar ante el mismo, que requieren de

todos los actores sociales para su cumplimiento, plantean exigencias en el plano nacional y en el internacional, y encajan en el concepto moderno de "calidad de vida" .

Quinta

Delimitación con otros derechos, en especial, el del acceso a la información pública. Ningún derecho es absoluto en un Estado de Derecho . Por lo tanto, tampoco lo es el derecho a la protección de datos de carácter personal.

Sentando lo anterior, parece que en México se ha pretendido optar por plantear el derecho a la protección de datos de carácter personal como un límite al acceso a la información pública, cuando, como hemos reiterado en multitud de ocasiones, si bien puede entrar en conflicto con la misma (y entonces habría que acudir a los conocidos instrumentos de prueba del daño e interés público para dilucidar la supremacía de alguno de los dos), como con muchos otros derechos, sería preferible, en todo caso, plantearlo como complemento.

Sin embargo, aún partiendo de la base de que la transparencia es un elemento fundamental de la democracia, como se plantea Rodotà: "¿debería eso ser un óbice para la igual defensa de la privacidad? ¿Es posible que la defensa de la privacidad conviva con esta idea de democracia? ¿Como se entrelazan, la esfera pública y la privada? ¿Cuál debería ser en esta materia la relación entre la libertad del individuo y las intervenciones del Estado?"

La privacidad, como dijimos, no puede ser ya hoy entendida como el derecho a ser dejado solo, sino que conlleva el poder de controlar la información personal , y, en concreto, el flujo de la misma.

La protección de datos cambia el paradigma, basándose ahora en la posibilidad del individuo a acceder a su información personal en posesión de cualesquiera terceros, ejerciendo éste un poder de control sobre los sujetos, públicos o privados, que disponen de sus datos personales.

Se crea así un nuevo modelo que, al reforzar la esfera privada, refuerza al mismo tiempo el peso del individuo en la esfera pública, constituyendo así un elemento básico de la que podemos denominar nueva ciudadanía electrónica, donde el test de "impacto privacidad" es imprescindible para juzgar el efectivo nivel de democracia del sistema político en cuestión.

Sexta

Y, finalmente, ¿qué implica la definición legal de dato personal? Siguiendo la máxima romana, toda definición en Derecho es peligrosa , luego los textos legales tienden a huir de las mismas. Pero, en esta supuestamente tecnificada materia sí se establecen, y,

además, la definición de dato de carácter personal es esencial, pues constituye el ámbito de aplicación objetivo de la normativa, es decir, en caso de que consideráramos que algo no es dato de carácter personal, la normativa no se aplicaría, por lo que pasamos a examinarla brevemente.

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

Como simple mención a los orígenes de la definición, expondremos un par de antecedentes en Derecho comparado.

Así, el Convenio (108) define en la letra a) de su artículo 2 el concepto de datos de carácter personal como: "cualquier información relativa a una persona física identificada o identificable ("persona concernida")".

Por su parte, la Directiva 95/46/CE, define en la letra a) del artículo 2 el concepto de datos personales de la siguiente manera: "toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

Retomando la definición de la LFTAIPG, pasamos a analizar sus componentes.

Se trata de una definición amplia, al igual que los legisladores internacionales intentaron en sus propios textos, y así el mismo Parlamento Europeo decía que dicha definición debería ser tan amplia como fuera posible para incluir toda información referente a una persona identificable. Pero tampoco es un concepto ilimitado. El objetivo es proteger los derechos y libertades fundamentales individuales en lo que se refiere al tratamiento de datos personales. Así, el ámbito de aplicación de las normas no debe llevarse a su extremo, pero también debe evitarse una limitación indebida del concepto de datos personales.

"La información": existen una serie de datos personales que todo el mundo identifica como tales, pero queda un gran espectro de información personal sobre la que no se tiene demasiado interés a menudo y que ni tan siquiera se considera como propia. No obstante, consideraciones sociológicas aparte, lo cierto es que la definición legal es, como dijimos, muy amplia, por lo que cabe toda información relacionada con una persona física, no sólo los datos ya comunes y habituales sino cualquier información que nos relacione con una persona física aunque ella misma lo desconozca.

Persona física: en la normativa mexicana sólo tiene sentido la protección de datos sobre los datos de las personas físicas . Podríamos hablar en este sentido de otras protecciones jurídicas, pero no de aplicación de la normativa en protección de datos de carácter personal..

Identificada o identificable: No sólo es que sepamos que cualquier información relacionada con una persona física es información de carácter personal, sino que, incluso cuando esa persona sólo pueda ser identificable , es decir, aunque no la tengamos identificada actualmente, eso sigue siendo información personal.

"Entre otra" y "otras análogas que afecten a su intimidad": en la definición se indican a modo de ejemplo algunos datos o clases de datos que entran dentro del concepto de dato personal y que por tanto tienen que ser protegidos por la LFTAIPG. Es decir, no se puede considerar, tal y como se deduce claramente de las expresiones "entre otra" y "otras análogas que afecten a su intimidad" utilizadas, que se trate de un numerus clausus, sino de una lista que queda abierta y en la que se proporcionan algunos ejemplos de lo que se considera dato de carácter personal.

Por otro lado, la LFTAIPG protege los datos personales bajo la figura de la información confidencial. No estamos de acuerdo con ello: no todos los datos personales son confidenciales, ni viceversa.

Un dato personal puede ser público o privado. No pierde su característica de dato personal por ser público, podría en algún caso tener que ceder algo de su protección, pero no pierde su esencia.

Finalmente, si los datos se someten a un procedimiento de disociación, que el lineamiento 20º define como "procedimiento por el cual los datos personales no pueden asociarse al titular de los datos, ni permitir por su estructura, contenido o grado de desagregación, la identificación individual del mismo", estos dejan de ser datos de carácter personal, porque pierden su característica más esencial, que es identificar o hacer identificable a una persona. En otras palabras, el dato deja de cumplir una función identificativa de la persona para convertirse en anónimo.

En conclusión, cualquier información, en cuanto asociada a un titular, es información de carácter personal, no por la información en sí, sino por su asociación con la persona física a la que se protege. Así, no se puede hablar de datos de carácter personal en sentido neutro, sino que tan sólo adquieren este carácter en cuanto se asocian a un titular.

III. Un poco de historia

Se suele decir que existen dos enfoques claramente diferenciados: el europeo y el estadounidense. Pero la normativa en protección de datos personales ha encontrado su

desarrollo en el continente europeo, y en la multitud de diferentes territorios que han adoptado su modelo, adecuándolo a su entorno socio jurídico (Japón, Australia, Canadá, Argentina, entre otros…) Por su parte, el denominado modelo estadounidense sólo se aplica en Estados Unidos.

Hay quien argumenta que esta preeminencia doctrinal y legislativa europea es la respuesta defensiva al injusto e ingente tratamiento y uso de la información personal por parte de los totalitarismos sufridos en diferentes países europeos durante el siglo XX, donde el control por parte del Estado de dicha información personal posibilitó en diversas ocasiones actos de barbarie. Sin embargo, esto no explicaría las también muy conocidas persecuciones sufridas en Estados Unidos y otros territorios .

Podríamos incluso intentar comparar las diferencias a grandes rasgos y decir que en Europa hay un enfoque social, los principios de protección se establecen en las leyes, el tratamiento de datos se da cuando es necesario, existen autoridades reguladoras independientes, y la protección se extiende a los no nacionales, mientras que en Estados Unidos el enfoque es individual, los alcances de la protección se delimitan ante los tribunales, el tratamiento de datos se realiza cuando es conveniente, el mercado es el regulador (con intervención de algún organismo sectorial como la Federal Trade Commission), y sólo se protege a los ciudadanos norteamericanos.

No obstante, a pesar de que muchos autores y políticos sostienen las grandes divergencias que entre los dos enfoques existen, no deja de haber voces que proclaman que las metas pueden ser idénticas, es decir, que se puede llegar al mismo punto aún partiendo de dos concepciones muy distintas .

Habiendo expuesto entonces la controversia entre los dos enfoques, pasamos a realizar un breve recorrido histórico internacional, europeo y estadounidense en la materia.

Ya la Declaración Universal de los Derechos Humanos, de 1948, establece en su artículo 12: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Asimismo el artículo 8 del Convenio Europeo para la Protección de los Derechos y las Libertades Fundamentales, de 1950, reconoce bajo el derecho al respeto de la vida privada y familiar que : "1 Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2 No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

Por su parte, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, de

1966, afirma "1. 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. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.".

La Convención Americana sobre derechos humanos de 1969 en su artículo 11, apartados 2 y 3, señala, bajo el epígrafe de "protección de la honra y de la dignidad" que "2. 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. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) adoptó en 1980 sus "Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales", que constituyen el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos personales.

La Asamblea General de la Organización de las Naciones Unidas emitió la Resolución 45/95 en 1990 con una lista básica de principios como el de licitud, exactitud, finalidad, acceso, no discriminación, entre otros.

La Asociación para la cooperación económica Asia-Pacífico (APEC) enfocada en que la protección de datos acompañe el crecimiento económico emitió en 1998 su Marco de Privacidad, similar al de la OCDE, que establece los principios de prevención de daño, aviso, limitación a la recolección de información personal, usos de la información o datos personales, elección, integridad de la información personal, seguridad, acceso y corrección, y responsabilidad.

La Red Iberoamericana de Protección de Datos aprobó su Reglamento en Mayo de 2008 destacando su impulso e implantación del derecho fundamental a la protección de datos de carácter personal instando a los gobiernos a elaborar una normativa que logre la obtención de la declaración de adecuación por parte de la Comisión Europea.

En Europa, como sucinta mención normativa, podemos partir de la Resolución 509 de la Asamblea del Consejo de Europa sobre derechos humanos y nuevos logros científicos y técnicos de 1968, continuar con las Resoluciones del Comité de Ministros de 1973 y 1974, pasando por el Convenio 108 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, 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 hace lo propio en el sector de las comunicaciones electrónicas junto con la Directiva 2006/24/CE de retención de datos de comunicaciones electrónicas. Como logro especialmente importante, la Carta Europea de Derechos

Fundamentales, en su artículo 8, señala el derecho a la protección de datos de carácter personal como uno de los derechos fundamentales en el ámbito europeo. Finalmente, incluso, la polémica Constitución europea incorpora el artículo I-51 dedicado al derecho a la protección de datos personales.

Finalmente, el pasado 5 de noviembre de 2009 se aprobó y presentó la denominada Resolución de Madrid, que contiene los Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal, en la sede de la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada ese mismo día en Madrid .

Además del iter normativo (utilizando el adjetivo en sentido amplio), como hito histórico esencial, la conocida sentencia del Tribunal Federal Alemán de 1983, sobre la licitud del tratamiento de los datos por la Ley del censo de un ciudadano alemán, abrió un nuevo e importante camino en la protección de datos internacionalmente.

Podemos decir que en esta sentencia se asienta el conocido principio a la autodeterminación informativa -que la doctrina suele llamar, en un juego de palabras, "principio a la autodeterminación informátiCa" aludiendo al tratamiento automatizado de los mismos- 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, dando lugar a un importante desarrollo normativo internacionalmente.

En Estados Unidos tenemos que comenzar por el conocidísimo artículo de los Jueces del Tribunal Supremo, Samuel D. Warren y Louis D. Brandeis , de 1890, donde 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 se entiende por privacidad en la era moderna en dichos ordenamientos.

En Europa y Canadá, como decíamos, existen leyes nacionales comprehensivas que se aplican a través de diferentes categorías.

En Estados Unidos, existe un mosaico de leyes federales y estatales que protegen ciertos sectores , además de la denominada "autorregulación industrial" desarrollada esencialmente por el sector privado, y cuya efectividad depende, en gran parte, del poder de coacción de quien formula dichos códigos y de la aplicación de las sanciones previstas en ellos.

Como breve nota común a las mencionadas regulaciones podemos destacar los ampliamente aceptados fair information practice principles (Información (Notice), Elección (Choice), Acceso (Access) y Seguridad (Security)), que en 1973 desarrolló el Departamento de Sanidad, Educación y Bienestar de los Estados Unidos en su informe sobre la protección de la privacidad en la era de la recogida de datos.

IV. Escenario legal actual en México

El actual Plan Nacional de Desarrollo 2007-2012 plantea entre sus estrategias "Desarrollar el marco normativo que garantice que la información referente a la vida privada y a los datos personales estará protegida (…) es necesario el desarrollo de una Ley Federal (…) Dicha regulación deberá incluir los principios de protección de datos personales reconocidos por los tratados internacionales en la materia, que el Estado mexicano debe observar."

Así, antes de adentrarnos en el análisis de los principios, veamos brevemente en qué estado legislativo nos encontramos actualmente en México.

Lo anterior no es una misión sencilla, ya que el caos y la confusión parece prevalecer. Comencemos por lo relevante y medianamente claro.

De un lado, tenemos la reforma al artículo sexto de la Constitución incorpora un párrafo destinado a la protección de datos personales que después veremos. Aquí ya tenemos una pequeña "victoria" y reconocimiento al derecho -o mera garantía institucional, en su caso como dijimos antes-, aunque encuadrado dentro de la reforma al acceso a la información pública gubernamental.

De otro lado, actualmente están en discusión otras dos reformas constitucionales mucho más relevantes para la materia, la del artículo decimosexto, que estaría totalmente dedicada a la inclusión y protección de datos personales, y la del artículo Septuagésimo Tercero, para lograr una regulación a nivel federal del tema en el Sector Privado.

No obstante, como decíamos, en el entorno legislativo, la situación es sumamente confusa. El iter de iniciativas ha sido, como mínimo, desordenado. Se pueden encontrar unas cuantas generales, muchos incluso hablan de alguna "fantasma", e incluso algunas otras reformas de mayor o menor calado a diferentes cuerpos legislativos .

Como adelantábamos, la primera referencia a nivel constitucional que se encontraba, hasta el pasado 20 de julio de 2007, estaba 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, con la publicación, 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, 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, en México, no existe aún una ley específica a nivel federal que regule específicamente la protección de datos personales, aunque sí existen referencias en diferentes cuerpos legislativos . Por su parte, a nivel estatal, el Estado de Colima sí cuenta con una regulación concreta desde el 2003, que sigue en gran medida la antigua y derogada

LORTAD española -tanto que, como mera curiosidad, habla de "ficheros" en lugar de "archivos"-, aunque sin que haya tenido aplicación en la práctica. Igualmente, por otro lado, Guanajuato, Jalisco y Sinaloa también han desarrollado previsiones legales al respecto, y la Ley de Protección de Datos del Distrito Federal se encuentra asimismo a punto de publicarse. Y, todo lo anterior sin olvidar que muchas de las reformadas leyes de transparencia dan un ámbito de actuación mayor a los Estados, por lo que habrá que esperar regulaciones cercanas y ambiciosas .

A pesar de lo anterior, la LFTAIPG, 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", también destaca 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", por lo que regula directamente la privacidad de los individuos cuyos datos personales son objeto de tratamiento por la Administración Pública Federal, planteándolo, al igual que la reforma constitucional, como un límite al acceso a la información, cuestión que entendemos desafortunada, pues, más que límite, es, en todo caso, complemento.

En el presente trabajo atenderemos, por razones de generalidad, a la regulación establecida por la LFTAIPG y a sus Lineamientos de protección de datos personales.

Es más, en realidad nos guiaremos fundamentalmente por los Lineamientos, porque desarrollan y profundizan en la regulación, pues, como dijimos, la LFTAIPG es claramente limitada a este respecto, entre otras cosas, porque no es una norma de protección de datos personales, sino de acceso a la información pública.

V. Los principios

Según los Lineamientos, los principios rectores de la protección de datos son la licitud, la calidad, el acceso y corrección, la información, la seguridad, la custodia y el consentimiento para la transmisión.

Dado que son, como apuntábamos, la referencia más clara de la doctrina del hasta ahora más general órgano de tutela seguiremos su agrupación en el análisis por cuestiones didácticas teniendo en cuenta la coyuntura regulatoria actual.

Sin embargo, queremos dejar claro desde el inicio igualmente que no estamos de acuerdo con no mencionar otros principios esenciales, especialmente el del consentimiento en origen, aunque sea aclarando que no se necesita por estar en una excepción al mismo, entre esos principios rectores de carácter general

Pasamos entonces a analizar muy sencillamente dichos Lineamientos evitando engorrosos reenvíos legales a otros textos para simplificar la exposición.

Licitud

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

Como decíamos, los Lineamientos, siguiendo su ámbito subjetivo particular, tan sólo establece el consentimiento en la fase de transmisión, sin tratarlo en origen.

En nuestra opinión, aunque en este artículo 6º.1 establece la licitud del tratamiento al reiterar que sólo será posible aquél que esté dentro de las atribuciones legales o reglamentarias de la dependencia, debería especificar que por tanto no es necesario dicho consentimiento, es decir, que se excepciona el mismo. Sin embargo, entendemos que no se haya hecho así, porque no podría irse vía Lineamientos contra la reglamentación de la LFTAIPG, que no trata tampoco el consentimiento en origen.

Es más, al establecer que el tratamiento sólo podrá hacerse dentro de dichas atribuciones, en realidad está supliendo, incluso de una manera muy magistral, la posible ilicitud ab initio de dicho tratamiento. Es decir, los Lineamientos, en este punto, parecen estar diseñados por alguien que ha tenido muy claro dicha deficiencia y la ha salvado con una excepción general al consentimiento, la atribución legal o reglamentaria, pero esto, en nuestro parecer, no tendría por qué haber impedido una referencia más general al consentimiento.

Y continúa el lineamiento entendiendo asimismo que la licitud también comprende que "los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos".

Sólo se podrá valorar la bondad de un tratamiento en cuanto a los fines del mismo, que deben de ser determinados y legítimos, por cuanto circunscriben las posibilidades de actuación sobre los datos objeto del mismo en relación, reiteramos, con la finalidad. Parece un círculo vicioso –o virtuoso- pero no hay tratamiento legítimo (ni lícito) si su finalidad no está determinada, y ésta no puede tampoco ser válida si no lo es a su vez.

Calidad

El artículo Séptimo de los Lineamientos, acerca de la Calidad de los datos, dice que "el tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo respecto de las atribuciones legales de la dependencia o entidad que los posea".

En nuestra opinión, estas cualidades deberían predicarse no respecto de las atribuciones de la dependencia, sino de la finalidad del tratamiento, que además debe de estar previsto dentro de dichas atribuciones, porque, si no, podría decirse que se cumple con la calidad porque la atribución legal lo permite cuando en realidad no se estaría cumpliendo por estar fuera de la finalidad del tratamiento en sí.

Es decir, las atribuciones legales de las dependencias son mucho más amplias que las finalidades de tratamientos concretos llevados a cabo por las mismas.

Además, al omitir la posibilidad de atribuciones reglamentarias previstas en el artículo anterior -por descuido, error o voluntad- circunscribe excesivamente dichas atribuciones.

Por otro lado, el lineamiento 14º obliga a los Responsables, Encargados o usuarios que detecten que hay datos inexactos a actualizarlos de oficio en cuanto tengan conocimiento de la inexactitud y siempre que posean los documentos justificativos que justifiquen la actualización. Si bien pudiera parecer que deja abierta la puerta a la indefinición temporal, no es muy sencillo que pueda concretarse más este extremo, y, al exigir contar con documentación acreditativa del hecho subsana posibles actualizaciones carentes de prueba justificativa posteriormente.

Acceso y corrección

El lineamiento 5º tan sólo señala que los sistemas deberán almacenarse para permitir el ejercicio de los derechos de acceso y corrección en los términos previstos en la Ley, el Reglamento y los Lineamientos.

Por lo tanto, el principio, aún denominado acceso y corrección, en realidad no desarrolla nada, y además, en nuestra opinión, no es la colocación adecuada sistemáticamente hablando, por lo que nos remitimos a su análisis en el apartado destinado a los derechos.

Información

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.

Así, el Lineamiento 9º dice que se debe hacer del conocimiento del titular de los datos al momento de recabarlos y de forma escrita el fundamento y motivo de ello, así como los propósitos para los que se tratarán dichos datos.

Seguridad

La implementación del principio de seguridad 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.

El lineamiento 20º, al hablar de seguridad, dice que se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado y posteriormente el capítulo IV se dedica a ahondar detalladamente en dichas medidas de seguridad .

Custodia y cuidado de la información

El lineamiento 11º señala que los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento, sin que exista una obligación similar en la LFTAIPG.

Consentimiento para la transmisión

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

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

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

El consentimiento se articula en cierta medida en el Lineamiento 12º, aunque no se contempla nada acerca de la necesidad del consentimiento para el tratamiento en origen o posterior de datos personales.

Sólo se exige, excepciones aparte, en la fase en la que los datos se transfieren a un tercero, es decir, cuando se produce la transmisión de datos a terceros, en la que el titular

pierde, en su caso, aún más el control sobre su información personal. No obstante, ya hemos dicho al hablar de la calidad que los lineamientos no podían señalar lo contrario ya que irían contra la regulación de la LFTAIPG.

El tratamiento de datos, según la propia definición de la LFTAIPG, no sólo se refiere a la transmisión -definida en el artículo 21 de la LFTAIPG como "difundir, distribuir o comercializar los datos personales"- sino que incluye la recogida, grabación, conservación, elaboración, modificación, bloqueo, cancelación y transmisión de datos personales, y, por lo tanto, todo tratamiento debería requerir del consentimiento, como regla general, y no únicamente en esa fase posterior de transmisión.

Además, el Lineamiento 23 va más allá y exige que cuando el consentimiento no esté excepcionado para la transmisión, entonces se necesitará que una disposición legal lo prevea de modo expreso y que medie el consentimiento expreso de los titulares. En nuestra opinión, al exigir los dos requisitos rompe de nuevo el principio vertebral, pues el consentimiento por sí solo no parece bastar para la transmisión.

El consentimiento deberá otorgarse en forma libre, expresa e informada. Además tendrá que darse por escrito incluyendo la firma autógrafa y la copia de la identificación oficial o bien mediante un medio de autenticación, debiendo en todo caso las dependencias cumplir con las disposiciones sobre firmas electrónicas.

En cuanto a la forma en la que se puede otorgar el consentimiento, con carácter general cabe distinguir entre consentimiento presunto, tácito, expreso y expreso por escrito .

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

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

Otras obligaciones y materias relacionadas

A pesar de que las normas internacionales sobre protección de datos hacen referencia, de una u otra manera, a unas categorías especiales de datos, también denominados datos sensibles, 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 no hace distinción alguna en lo que a estas distintas clases de datos de carácter personal se refiere.

En otro orden de cosas, 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 transmisión de datos ya comentada.

En la prestación de servicios, o acceso a los datos por terceros se establece un encargo por parte del responsable del sistema de datos a un tercero para que se le preste un servicio determinado.

En la transmisión 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.

El lineamiento 21º dice que cuando se contrate a terceros para que realicen el tratamiento de datos personales deberá estipularse en el contrato respectivo la implementación de medidas de seguridad y custodia así como las penas convencionales por incumplimiento.

VI. Los 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 haga el responsable del sistema de datos personales.

En el entorno internacional hispanoparlante goza de cierta popularidad denominarlos como los derechos "ARCO", acrónimo que sintetiza el acceso, rectificación, cancelación y oposición.

El derecho de acceso (regulado en los arts. 20 y 24 LFTAIPG y en el artículo 47 de su Reglamento) 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.

Los derechos de rectificación y supresión (según el art. 25 de la LFTAIPG) permiten al 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.

Otro de los derechos previsto en la LFTAIPG (en su art. 23 y 48 del Reglamento) 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.

Así, el "Sistema Persona" se crea en el Capítulo VI de los Lineamientos para facilitar el ejercicio de los derechos de acceso y corrección de los particulares, incluyendo asimismo el derecho de consulta a dicho Sistema.

Finalmente, como decíamos, en las legislaciones internacionales existen otros derechos, como el derecho de oposición recogido en la Directiva 95/46/CE europea, 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 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.

Por otro lado, nos parece importante asimismo volver a recalcar que no sólo se tienen derechos, pues, además de las limitaciones que los derechos de los demás imponen a los propios, que deben ceder, por ejemplo, ante un interés o bien público, el titular de los datos tiene un deber de diligencia o de cuidado sobre los mismos.

El individuo debe ser consciente del valor de sus datos y su posterior utilización, y actuar en consecuencia, para que si consiente a que se traten sus datos lo haga de una manera sensata y razonada, evitando comerciar con ellos a cambio de regalos, premios o invitaciones puntuales que en muchas ocasiones conllevan el consentimiento para su utilización con múltiples finalidades.

VII. El procedimiento y 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.

El histórico "habeas corpus" protegía la integridad corporal del sujeto. El "habeas data", como evidente desarrollo del anterior, protege la integridad corporal electrónica del sujeto, es decir, la información personal.

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.

En el artículo 33 de la LFTAIPG se prevé 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."

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 archivos 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.

El IFAI, por su parte, 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, ni que el IFAI sea una autoridad o órgano de control en la materia, como en las normativas internacionales se configura.

El 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.

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

VIII. Otras cuestiones

Dentro de la normativa de protección de datos de carácter personal hay muchos otros temas de especial relevancia, como la transferencia internacional de datos, o tratamien-

tos de datos específicos (como datos de salud, datos con fines de solvencia patrimonial y crédito o 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.

Todos ellos son aspectos concretos de la regulación que sería imposible tratar en este trabajo por razones de espacio y metodología, pero entendemos especialmente interesante por diversas cuestiones detenernos brevemente en la problemática de la transferencia internacional de datos y la utilización de códigos de conducta.

La transferencia internacional de datos

La globalización del comercio, en el más amplio sentido de la palabra, conlleva en la mayoría de las ocasiones la necesidad de tratar datos de carácter personal, dando lugar a la Transferencia Internacional de Datos (TID) entre diversos países.

Estos tratamientos tienen que adecuarse a las previsiones legales establecidas en los diversos ordenamientos jurídicos en juego, que tienen como fin garantizar al individuo, cuyos datos son objeto de tratamiento, su derecho fundamental a la protección de datos , y así facilitar la realización de transacciones internacionales , comerciales y no comerciales.

La legislación europea exige para realizar cualquier transacción que involucre datos de carácter personal, es decir, casi todas, que el destinatario cuente con un nivel adecuado de protección, bien vía país de destino o vía contractual.

En este sentido, la legislación europea establece unas reglas muy delimitadas para que estas TID se puedan llevar a cabo. Así, los principios que rigen esta regulación son:

1. Prohibición de transferencias a un país tercero que no garantice un nivel de protección adecuado (art. 25.1 Directiva 95/46/CE).

   Lo que nos lleva inmediatamente a preguntarnos qué se entiende por nivel de protección adecuado. El artículo 25.2 de la Directiva dispone que dicho carácter adecuado se evalúa atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos, y, en particular: la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. En definitiva, se busca que el sistema de protección proporcione un buen nivel de cumplimiento de las normas, apoyo y ayuda a los sujetos de datos individuales en el ejercicio de sus derechos y una reparación adecuada a las partes perjudicadas cuando no se cumplan las normas . La Comisión podrá adoptar una Decisión en la que establezca que un país tercero ga-

rantiza 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).

2. No obstante, la Directiva prevé a continuación una serie de excepciones a los principios en su artículo 26, como el consentimiento inequívoco del interesado, la ejecución de un contrato con determinados requisitos, o la salvaguardia de un interés público importante o para el reconocimiento de un derecho en un procedimiento judicial.

3. Finalmente, también se podrá autorizar esta TID cuando el responsable del tratamiento ofrezca garantías suficientes, pudiendo incluirse las mismas en cláusulas contractuales apropiadas, incluyendo la utilización de unas cláusulas contractuales predispuestas y redactadas por la Comisión.

En la actualidad, podemos decir que las TID en función del país destino se podrán realizar conforme a la legislación europea:

En caso de que el país tercero destinatario de los datos esté declarado como país que proporciona un nivel adecuado de protección. Aquí se encontrarían las siete Decisiones de la Comisión Europea declarando a Suiza, Hungría (aunque esta Decisión está ya un poco vacía de contenido porque Hungría ya pertenece a la Unión Europea), Canadá, Argentina, Guernsey, Isla de Man y Jersey, como terceros países que proporcionan un nivel adecuado de protección. En el caso de Estados Unidos se declara la adecuación mediante un sistema de adhesión voluntaria al programa de "Puerto Seguro". La sustancial diferencia entre estos dos grupos es que las primeras determinan que las legislaciones de dichos países garantizan un nivel adecuado de protección, mientras que en el caso de EE.UU. no se está reconociendo que proporcione un nivel de protección adecuado, sino que son las entidades que cumplen con el Acuerdo de Puerto Seguro las que obtienen la presunción de "adecuación".

En el caso de que el país de destino no proporcione un nivel adecuado de protección y no estemos en una de las excepciones del art. 26 de la Directiva se podrá optar por el contrato propuesto por la Comisión, cuyas cláusulas ofrecen las garantías respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas y el respeto al ejercicio de los respectivos derechos. Estas cláusulas contractuales tipo han sido aprobadas mediante las correspondientes Decisiones de la Comisión, en función de cuál sea la finalidad de la transferencia y se refieren únicamente a la protección de datos, pudiendo añadirse por las partes del contrato aquellas otras necesarias para el desarrollo de su negocio.

En definitiva, se puede realizar una TID a un país tercero, cuando se tenga el nivel adecuado de protección o se esté en una excepción, o, finalmente, se utilice un mecanismo de cláusulas contractuales .

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."

El Acuerdo de Puerto Seguro

El denominado Acuerdo de "Puerto seguro" es una excepción a las demás Decisiones adoptadas por la Comisión, fruto de las intensas y no siempre exentas de polémica negociaciones mantenidas, durante más de dos años, entre el Departamento de Comercio de Estados Unidos y la Comisión Europea, partiendo de los diferentes enfoques que los EE.UU. y la UE dan a la protección de la vida privada de sus ciudadanos, basándose el planteamiento de los EE.UU. en una mezcla de normas legales y autorregulación por parte del sector privado.

Es un Acuerdo muy complicado, tanto que normalmente estas Decisiones sobre el nivel adecuado tienen una extensión de un par de hojas, y este Acuerdo es muy largo, precisamente por todas las complicaciones de gestión y de negociación que conllevó .

En el Acuerdo de Puerto Seguro la Comisión no declara, al contrario que en el resto, que Estados Unidos sea un país con un nivel de protección adecuado, o equiparable a la Unión Europea, sino que se acuerda que las entidades estadounidenses, que voluntariamente decidan adherirse a los principios contenidos en el mismo, podrán recibir datos personales de responsables establecidos en alguno de los Estados miembros de la UE al entenderse que las mismas proporcionan una protección suficiente.

El Acuerdo se compone de unos Principios -que, en opinión de la mayoría de las autoridades europeas, son muy laxos, máxime en comparación con sus legislaciones nacionales- y de unas Preguntas Más Frecuentes que explican dichos principios.

Las entidades que puedan y quieran adherirse a este Acuerdo tienen que adherirse a un programa de autorregulación que ya contenga dichos principios o bien por autorregulación de la entidad en cuestión si dicha autorregulación los respeta. El método de adhesión es por un sistema de autocertificación, mediante una carta firmada por uno de los responsables de la entidad, ante el Departamento de Comercio, y aplicándose sobre todos los datos personales recibidos desde la Unión Europea.

Las cláusulas contractuales tipo

Tal y como decíamos, existe una tercera vía disponible desde la norma comunitar-

ia que puede calificarse como una solución específica a la necesidad de garantizar el cumplimiento de las disposiciones en materia de protección de datos en el caso de aquellas transferencias de datos que se efectúan con destino a países que no proporcionan un nivel adecuado de protección, tanto si se trata de una transferencia que tenga por objeto la comunicación de los datos a un responsable del tratamiento establecido en un país tercero como si es a un encargado del tratamiento para la prestación de un servicio por cuenta del responsable del tratamiento.

Con este fin, la Comisión Europea ha aprobado dos Decisiones que tienen por objeto aprobar clausulados contractuales tipo que contemplan las transferencias efectuadas a países terceros que no otorguen un nivel de protección equivalente al que proporciona la Directiva.

Así, en concreto, la Comisión está trabajando en las conocidas "Binding Corporate Rules (BCR)" o Reglas Corporativas Vinculantes, que es un catálogo de medidas en protección de datos aplicables a las empresas multinacionales y demás grupos similares que garantizan un nivel adecuado de protección cuando la información es transferida fuera de la Unión Europea a un país que no tiene dicho nivel .

Pero evidentemente, dado que los modelos tipo que proporciona la Comisión son una guía orientativa, las partes también pueden diseñar su propia solución contractual, que deberá ser evaluada mediante los mismos criterios que para un sistema de protección de datos ya hemos mencionado.

Los Códigos Tipo

Los códigos tipo, o deontológicos, o de buena conducta o práctica profesional, son un elemento de autorregulación especialmente apropiado para el entorno del Derecho de las Nuevas Tecnologías , y, más en concreto, para la generación de la tan nombrada y necesitada confianza.

Cuando hablamos de autorregulación no queremos con ello decir que estos códigos puedan sustituir a la regulación clásica, y menos en los países de nuestro entorno, claramente guiados por el sistema regulatorio, en contra de otros ordenamientos que promulgan y fomentan mucho más la participación industrial en estos temas, como el estadounidense ya mencionado.

La autorregulación, plasmada en los códigos de conducta y en otras medidas que tienen por objeto garantizar la privacidad de los usuarios, se configura como una solución complementaria especialmente adecuada al esquema legislativo, y como un modo de hacer y dirigir los negocios, con respeto a la normativa.

Se debe prestar especial atención a las garantías de cumplimiento y respeto de estos códigos, como la obtención de una satisfacción en caso de incumplimiento de lo dis-

puesto, o, simplemente, el establecimiento de unos procedimientos serios y consistentes en relación con una posible reclamación.

Si no se establecen, y se cumplen, las mencionadas reglas, se puede caer fácilmente en una mera declaración de principios o intenciones que no justifique en realidad la existencia del código, es más, que ni tan siquiera sea un código como tal.

Las notas que caracterizan a la autorregulación frente a las normas emanadas de un poder público son las siguientes:

Derivan de la iniciativa de un sector concreto, público o privado, pero nunca del propio Estado que es el único órgano con el poder necesario para la elaboración de una norma legal.

Si bien pueden haber previsto un mecanismo de sanciones en caso de incumplimiento de las normas contenidas en el mismo, estas pueden ser insuficientes al no ser impuestas por un órgano superior, como es el caso del Estado.

Dan una respuesta mucho más rápida ante situaciones de vacío legal o cuestiones que requieren un tratamiento específico para su posterior regulación.

IX. La reforma al artículo 6 de la Constitución

Pasando al comentario de la inclusión en la Constitución, el pasado 20 de julio de 2007, de un nuevo artículo 6 que engloba a la protección de datos, si bien dentro del derecho al acceso a la información del ciudadano, 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 dar a entender, 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.

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 pro-

cedimientos 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:

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 Derecho, y nos inquieta que el legislador no profundice sobre el verdadero sentido de la protección de datos, de manera independiente.

El texto diferencia entre la vida privada y los datos personales. Como decíamos supra los conceptos se interrelacionan. 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 . La normativa gira en torno a cuestiones objetivas, donde el tratamiento de los datos personales, públicos o privados, tiene que seguir unas ciertas reglas. Sin embargo, lo que sí resulta en todo caso resaltable, como decíamos, es que se exige la protección.

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 gratuidad 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.

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) de 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.

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 expresamente sólo se refiere al acceso a la información. No obstante, en una labor exegética lo cierto es que podríamos entender que también se tendría que hacer en las mismas condiciones para el acceso a datos personales. 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.

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.

X. La reforma al artículo 16 Constitucional

La propuesta de la Comisión de Puntos Constitucionales de reforma del artículo 16 constitucional, fue aprobada por el Senado el 4 de diciembre de 2008 y por la Cámara de Diputados el 11 de diciembre de 2008.

Conceptualmente engloba mucho más coherentemente la materia tratada, como la misma reforma señala "el texto que se dictamina permitiría concluir el trabajo iniciado con la reciente reforma al artículo 6 de la CPEUM (…) y por su parte el artículo 16 establecerá el derecho a la protección de datos personales, que, aunque mencionado en la fracción II del 6° se estaría dotando finalmente de contenido a este derecho fundamental".

Asimismo señala como su propósito "consolidar el derecho a la protección de datos en nuestro país, extendiendo su ámbito de aplicación a todos los niveles y sectores, apuntalando, por una parte, la estructura edificada a través del artículo 6 fracción II de la Constitución Federal y de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para los sistemas de datos personales en posesión de los entes públicos federales y, por la otra, reconociendo la existencia del mismo respecto de los datos personales en poder del sector privado".

El texto de la reforma propuesta es el siguiente: "Artículo Único. Se adiciona un segundo y tercer párrafos recorriéndose los subsecuentes en su orden al artículo 16, de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue: "Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y en su caso, obtener su rectificación, cancelación y manifestar su oposición en los términos que fijen las leyes. La Ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden, seguridad y salud públicos o para proteger los derechos de terceros."

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

En primer lugar, como ya decíamos, la inclusión del reconocimiento independiente y autónomo del derecho en este artículo constitucional es mucho más pertinente y adecuada.

"toda persona": el término persona da cabida, a menos de que posteriormente se circunscribiera, lo que parece difícil al venir así dispuesto en la norma constitucional, a las personas morales.

"derecho a acceder a sus datos personales": el ejercicio de los derechos es personalísimo, sólo puede ser por su titular o el representante del mismo en caso de incapacidad legal.

"en su caso, obtener su rectificación, cancelación": la atención a los derechos de rectificación y cancelación no implica necesariamente la concesión de los mismos. El titular de los datos deberá justificar y probar con la documentación acreditativa pertinente dichos cambios, y, además, puede suceder que el responsable del archivo entienda que no procede dicha rectificación o cancelación.

"manifestar su oposición": la filosofía subyacente a este derecho, con claras aplicaciones al entorno publicitario, es, como dijimos, la posible negación del 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, cuando existan motivos fundados y legítimos, y el responsable del archivo tendrá que proceder a la exclusión de los mismos.

"Supuestos de excepción": tal y como señala la iniciativa, hay dos finalidades importantes al recalcar la existencia de las excepciones: "dar certidumbre al gobernado

respeto de los casos en los que será posible tratar sus datos sin que medie su consentimiento, desde el nivel constitucional" y "dejar claro que este derecho encuentra límites frente a otros, en los que previa valoración de las circunstancias particulares, el derecho a la protección de datos puede ceder frente a los mismos".

XI. La reforma al artículo 73 Constitucional

Por su parte, la Iniciativa de la Comisión de Puntos Constitucionales de reforma del artículo 73 constitucional, asimismo aprobada por unanimidad por el Pleno de la Cámara de Diputados el pasado 20 de septiembre de 2007, y por el Senado el 4 de diciembre de 2008, tiene como finalidad "otorgarle la facultad exclusiva al Congreso de la Unión de legislar en materia de protección de datos personales en posesión de los particulares".

El texto propuesto dice: "Artículo Único. Se adiciona la fracción XXIX-Ñ al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue: Artículo 73. El Congreso tiene facultad: XXIX-Ñ. Para legislar en materia de protección de datos personales en posesión de particulares."

La justificación de la reforma incide en que los datos se utilizan usualmente para llevar a cabo transacciones comerciales y dicha materia es competencia exclusiva federal.

Como ya hemos visto, en la actualidad el IFAI tiene competencia sobre los datos personales en poder de la Administración Pública Federal, pero lo que la Iniciativa persigue es que los datos en posesión de los particulares, es decir, del Sector Privado, no puedan ser sometidos a legislaciones estatales, ya que se podría dar de facto lugar a desigualdades y mercados territoriales de información personal.

XII. Algunas reflexiones finales

El derecho a la protección de datos de carácter personal se encuentra aún lejos de ser valorado en su magnitud. No sólo es generalmente desconocido, sino, lo que es peor, minusvalorado.

El individuo tiene derecho a decidir cuándo, cómo y quién va a tratar su información personal.

A pesar de ser un derecho elevado a la categoría de fundamental en muchos ordenamientos, aún no se puede decir que se encuentra en igualdad de condiciones en la práctica, al menos respecto de los demás derechos fundamentales.

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. México no

cuenta tampoco con una regulación federal específica, si bien se observan movimientos hacia ello, como la reforma del artículo sexto constitucional y la propuesta al artículo 16 del mismo texto, que confiemos den pronto los frutos esperados afirmando la necesaria independencia y autonomía del derecho a la protección de datos personales.

La privacidad es irrenunciable, inalienable, y, más aún en una sociedad en la que, como hemos dicho, el valor más importante es la información. En consecuencia, la información personal aún debería adquirir una relevancia mayor dentro de la escala de gradación.

En cuanto a su relación con otros derechos o intereses, en nuestra opinión, el justo medio, aún tan difícil de encontrar, parece la solución adecuada. Se debe garantizar la privacidad, y afirmamos al mismo tiempo que no tiene por qué ser un inhibidor del comercio, entendiendo el respeto a dicho derecho fundamental como un valor añadido en la gestión empresarial y pública.

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 económico.

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.

Las TIC no deben ser sólo una amenaza para esta privacidad, sino que incluso pueden ser utilizadas precisamente para ayudar en su preservación, fomentando la implementación de las tecnologías de protección de la privacidad, como complemento, que no sustituto, de la legislación adecuada.

Tampoco debe invocarse situaciones especiales, de riesgo o miedo ante posibles ataques, sacrificando la privacidad del individuo, sino llegarse al equilibrio entre los intereses en conflicto, sin dejar que pretendidas amenazas aniquilen el derecho fundamental de los seres humanos a controlar su información personal y el tratamiento de la misma.

Nos permitimos así abogar desde estas líneas por la información y la formación del usuario acerca sus derechos y obligaciones en el cuidado de su información personal, huyendo de los extremismos, con objetividad, así como por un asentamiento legal, jurisprudencial, social y cultural del derecho a la protección de datos personales en México.

Referencias normativas

Carta de los derechos fundamentales de la Unión Europea de 7 de diciembre de 2000 (2000/C 364/01).

Constitución europea incorpora el artículo I-51 dedicado al derecho a la protección de datos personales, http://es.constitutio.com/051.php, disponible a 25 de septiembre de 2008.

Convención Americana sobre derechos humanos de 1969, http://www.oas.org/juridico/spanish/Tratados/b-32.html, disponible a fecha de 19 de septiembre de 2008.

Convenio (108) del Consejo de Europa, para la protección de las personas con relación al tratamiento automatizado de los datos de carácter personal, de 28 de enero de 1981.

.Convenio Europeo para la Protección de los Derechos y las Libertades Fundamentales, http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/SpanishEspagnol.pdf, a fecha de 19 de septiembre de 2008.

Decisión 2001/497/CE de la Comisión, de 15 de junio, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a un tercer país previstas en la Directiva 95/46/CE (D.O. L 181, de 4 de julio)

Decisión 2002/16/CE de la Comisión, de 27 de diciembre, relativa a las cláusulas contractuales tipo para la transferencia internacional de datos personales a los encargados de tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE (D.O. L 6, de 10 de enero de 2002).

Decisión 2000/520/CE de la Comisión, de 26 de julio (Diario Oficial de la Unión Europea serie L, núm. 215, de 25 de agosto).

Decisión 2002/518/CE de la Comisión, de 26 de julio (Diario Oficial de la Unión Europea serie L, núm. 215, de 25 de agosto)

Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001 (Diario Oficial de la Unión Europea serie L, núm. 2, de 4 de enero de 2002)

Decisión 2003/490/CE de la Comisión, de 30 de junio (Diario Oficial de la Unión Europea serie L, núm. 168, de 5 de julio)

Decisión 2003/821/CE de la Comisión, de 21 de noviembre (Diario Oficial de la Unión Europea, serie L, núm. 308, de 25 de noviembre)

Decisión 2004/411/CE de la Comisión, de 28 de abril (Diario Oficial de la Unión Europea serie L, núm. 151, de 30 de abril)

Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008 (Diario Oficial de la Unión Europea serie L, núm. 138, de 28 de mayo).

Declaración Universal de los Derechos Humanos, de 1948, http://www.un.org/spanish/aboutun/hrights.htm a fecha de 19 de septiembre de 2008

Directiva 2002/58/CE 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).

.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).

Directrices relativas a la protección de la privacidad y flujos transfronterizos de datos personales (1980), Organización para la Cooperación y el Desarrollo Económicos.

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

Ley de protección de datos personales para el Estado y los Municipios de Guanajuato de 19 de mayo de 2006.

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.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, publicada en el Boletín Oficial del Estado número 298, de 14 de diciembre

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, publicada en el Boletín Oficial del Estado número 262, de 31 de octubre (derogada por Ley Orgánica 15/1999).

Lineamientos de protección de datos personales, publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005.

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 (DOF Martes 6 de abril de 2004)

Marco de Privacidad (1998) de la Asociación para la cooperación económica Asia-Pacífico.

Pacto Internacional de Derechos Civiles y Políticos, http://www.unhchr.ch/spanish/html/menu3/b/a_ccpr_sp.htm, a fecha de 19 de septiembre de 2009.

Plan Nacional de Desarrollo 2007-2012 http://pnd.calderon.presidencia.gob.mx/index.php?page=transparencia-y-rendicion-de-cuentas, disponible a 11 de septiembre de 2009.

Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales emitidas por el IFAI disponibles en http://www.ifai.org.mx/datos_personales/seguridad/Recomendaciones_SDP.pdf, a 20 de agosto de 2009.

Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee_on Automated Personal Data System, Julio, 1973. Disponible en http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm, disponible a 22 de septiembre de 2009.

Reforma propuesta al Artículo 16 Constitucional, Gaceta Parlamentaria, Cámara de Diputados, número 2343-II, martes 18 de septiembre de 2007. http://gaceta.diputados.gob.mx/Gaceta/60/2007/sep/20070918-II.html#Dicta20070918Art16Const

Reforma propuesta al Artículo 73 Constitucional, Gaceta Parlamentaria Congreso de Diputados número 2339, miércoles 12 de septiembre de 2007. http://gaceta.diputados.gob.mx/Gaceta/60/2007/sep/20070912-II.html#Dicta20070912Articulo73

Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. (Primera Sección) (DOF Miércoles 11 de junio de 2003)

Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas

Resolución 509 (1968) de la Asamblea del Consejo de Europa sobre derechos humanos y nuevos logros científicos y técnicos.

Resolución R (73) 22 relativa a la protección de la vida privada de las personas físicas respecto de los bancos de datos electrónicos en el sector privado.

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.

Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, Madrid: Boletín de Jurisprudencia Constitucional, año 1984, páginas 126 y ss.

Bibliografía recomendada

AGRE, PHILIP E. AND MARC ROTENBERG, editores, Technology and Privacy: The New Landscape, Cambridge, 1997, MA: MIT Press, 334 páginas.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M., "Protección de la intimidad en el tráfico de datos en Internet (2001-2002)", Quince años de Encuentros sobre Informática y Derecho, Madrid: Ed. Universidad Pontificia Comillas, 2002, páginas 561-570.

BAYENS, S., The search and seizure of computers: are we sacrificing personal privacy for the advancement of technology?, Drake Law Review, 2000

CARBONELL, M. "La reforma constitucional en materia de acceso a la información: una aproximación general", en Hacia una democracia de contenidos: la reforma constitucional en materia de transparencia, Instituto de Investigaciones Jurídicas, UNAM, Diciembre 2007.

COATS, W. The Practitioner's Guide to Biometrics. Ed. ABA Section of Science& Technology Law. 2007 Chicago, Illinois.

DAVARA FERNÁNDEZ DE MARCOS, I.:

Breve análisis de la reforma al artículo 6º constitucional en lo relativo a protección de datos personales, en Hacia una democracia de contenidos: la reforma constitucional en materia de transparencia, Instituto de Investigaciones Jurídicas, UNAM, Diciembre 2007.

Protección de datos de carácter personal, Revista Abogado Corporativo, Asociación Nacional de Abogados de Empresa, nº 3, Enero - Febrero 2008

La protección de datos en España, en La protección de datos en el mundo, México D.F.: Senado de la República, México D.F., Septiembre 2006.

DAVARA RODRÍGUEZ, M.A.:

Guía Práctica de Protección de Datos para abogados, Madrid: Editorial DaFeMa, 2004.

Manual de Derecho Informático. 6ª edición, Pamplona: Editorial Aranzadi, 2004.

DE ASÍS ROIG, A. E., "Protección de datos y derecho de las telecomunicaciones", Régimen Jurídico de Internet, Madrid: Ed. La Ley , Enero 2002, páginas 201-228.

ESCALANTE GONZALBO, F., El derecho a la Privacidad, Cuadernos de transparencia nº 2, México: IFAI, Agosto 2004.

FERNÁNDEZ LÓPEZ, J. M., "El derecho fundamental a la protección de datos personales", OTROSÍ num. 25, Madrid: Ed. Colegio de Abogados de Madrid, 2001, páginas 56-60.

FROOMKIN, M., The Death of Privacy? Stanfrod Law Review , Vol. 52:1461, 2000.

FREIXES SANJUÁN, T.: Libertades informativas e integración europea, Madrid: Ed. Constitución y Leyes, 1996.

GARCÍA GONZÁLEZ, A., La protección de datos personales: derecho fundamental del Siglo XXI. Un estudio comparado. Boletín Mexicano de Derecho Comparado, Número 120, Septiembre-Diciembre 2007, Instituto de Investigaciones Jurídicas de la UNAM.

GARZÓN VALDÉS, E., Lo íntimo, lo privado y lo público, Cuadernos de transparencia nº 6, México: IFAI, Abril 2005.

GÓMEZ ROBLEDO y ORNELAS NUÑEZ, Protección de datos personales en México: el caso del Poder Ejecutivo Federal, México: UNAM, 2006.

HAGEL, J. y J.F. RAYPORT, The Coming Battle for Customer Information, Harvard Business review, vol 75 n 30, 1997.

HONDIUS, F. W., A decade of international data protection, "Netherlands of International Law Review", vol. 30, n° 2, 1983.

HUTCHINS, J.; U.S. Data Breach Notification Law: State by State. Ed. ABA Section of Science & Technology Law. 2007.

JAMES, MICHAEL, Privacy and human rights: An international and comparative study, with special reference to developments in information technology, Paris : UNESCO, 1994.

KANG, J., Information Privacy In Cyberspace Transactions, 50 Stanford Law Review 1193, Abril 1998.

LÓPEZ AYLLON, Sergio Derecho de la Información, Ed. McGraw-Hill/Interamericana Editores, S.A. de .C.V; 1997 México.

LÓPEZ-IBOR MAYOR, V., "Los límites al derecho fundamental a la autodeterminación informativa en la Ley Española de Protección de Datos", Actualidad Informática Aranzadi núm. 8, Pamplona: Ed. Aranzadi, 1993, páginas 1-3.

LUCAS DURÁN, M., El acceso a los datos en poder de la Administración Tributaria, Pamplona: Ed. Aranzadi, 1997, páginas 265 y ss.

LUCAS MURILLO DE LA CUEVA, P., "Las funciones de la Agencia de Protección de Datos", Jornadas sobre el Derecho Español de la Protección de Datos Personales, Madrid: Ed. Agencia de Protección de Datos, 28, 29 y 30 de Octubre de 1996, páginas 276 y ss.

OLIVER LALANA, A. D., "Autorregulación, normas jurídicas y tecnológicas de privacidad. El lado virtual del derecho protección de datos", XVII Encuentros sobre Informática y Derecho, Madrid: Ed. Universidad Pontificia Comillas, 2002-2003, páginas 85-102.

PECES-BARBA, G., "Derechos Fundamentales", Madrid: Ed. Guadiana de Publicaciones, 1976, 318 páginas.

PÉREZ LUÑO, A. E., Cibernética, Informática y Derecho. (Un análisis metodológico), Bolonia: Ed. Real Colegio de España, 1976. 166 Páginas.

POSNER, RICHARD, The Economics of Privacy, The American Economic Review, Vol. 71, No. 2, Mayo 1981.

RODOTÀ, S.:

- "Democracia y protección de datos", Cuadernos de Derecho Público, Madrid: INAP, núms. 19-20, mayo-

diciembre de 2003.

- Tecnología y derechos fundamentales, Agència Catalana de Protecció de Dades, 2004, disponible en www.apd.cat a 25 de agosto de 2008.

RUBÍ NAVARRETE, J., "Los códigos tipo: la alternativa de la autorregulación", Actualidad Informática Aranzadi núm. 35, Pamplona: Ed. Aranzadi, 2000, páginas 1-5.

Rule, J, Privacy in Peril. Ed. Oxford University Press, 2007.

SANCHO VILLA, D., Transferencia Internacional de Datos Personales, Madrid: Ed. Agencia de Protección de Datos, 2003.

SOOKMAN, B., Computer, Internet and Electronic Commerce Terms: Judicial, Legislative and Technical Definitions. Ed. Thomson Carswell. 2002 Canadá.

SULLIVAN, J; HIPPA A Practical Guide to the Privacy and Security of Health Data. Ed. American Bar Association. Chicago, Illinois.

VV.AA., Privacy & Human Rights. Ed. Electronic Privacy Information Center and Privacy International. First edition 2007.

WESTBY, J. et al., International Guide to Privacy. Ed. Section of Sience &Technology Law, American Bar Association. 2004 Chicago, Illinois.

WESTIN, A., Privacy and Freedom, Nueva York: Ed. Atheneum, 1967.

WU, S., et al: A Guide to Hipaa Security and the Law. Ed: ABA Section of Science & Technology Law.2007 Chicago, Illinois.

ZÚÑIGA URBINA, F., El derecho a la intimidad y sus paradigmas, "Ius et praxis", Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Chile, año 3, n° 1, 1997.