Tan lejos, tan cerca

POR **RICARD MARTÍNEZ**

Desde el punto de vista del bien jurídico protegido, no existen diferencias significativas en la noción de privacidad entre España y Estados Unidos. No obstante, los mecanismos de tutela del derecho a la vida privada presentan bastantes divergencias. Lo mismo sucede con el modo de entender el significado de la garantía de este derecho en la actividad empresarial.

Los recientes acontecimientos y revelaciones de Edward Snowden sobre las actividades de la National Security Agency (NSA) han revitalizado de algún modo el debate trasatlántico sobre la privacidad. La discusión, mantenida a veces a cara de perro en la prensa, se ha caracterizado tanto por un uso político de las categorías jurídicas como por la apariencia de un desconocimiento mutuo de los respectivos modelos jurídicos.

En este sentido ha sido particularmente significativa la ofensiva de la Comisaria Viviane Reding en defensa de la Propuesta de Reglamento General de Protección de Datos como herramienta imprescindible para la garantía de los derechos fundamentales de los europeos. Y si bien es cierto que puede asistirle parte de razón, no lo es menos que en este caso concreto el derecho fundamental afectado es el secreto de las comunicaciones, el cual es un derecho autónomo del derecho a la protección de datos en las constituciones de los distintos Estados europeos y en el propio sistema del Convenio Europeo de Derechos Humanos.

Choque cultural

El debate Europa-EEUU sobre privacidad ha suscitado de modo recurrente serias discusiones diplomáticas y ha generado acuerdos no siempre bien recibidos. En tal sentido, el simple flujo de datos hacia EEUU, considerado país no seguro a efectos de la aplicación del régimen de transferencias internacionales de datos de la Directiva 95/46/CE, exigió la adopción del instrumento internacional denominado *Safe Harbour Principles*.

En la memoria de los expertos -y de muchos no expertos- persiste el escándalo Swift, empresa belga de intermediación financiera que enviaba masivamente datos bancarios de ciudadanos

Fundación Telefónica
Telefónica

europeos a EEUU. Los controles sobre el flujo internacional de pasajeros a través del acuerdo *Passengers Name Records* (PNR) desataron las iras del Parlamento Europeo. Y, por último, en una lista que no puede cerrarse aquí, cabe referirse a los quebraderos de cabeza que ha planteado la sujeción de empresas españolas a la *Sarbanes-Oxley Act* (2002), cuya extraterritorialidad de facto ha obligado a encontrar un modo de hacer compatible con la Ley española los sistemas de *whitsleblowing* que aquella impone[1].

El choque cultural no solo se produce en el ámbito gubernamental, sino también en el sector privado. Los operadores norteamericanos no acaban de entender o de aceptar la existencia de lo que podría definirse desde su punto de vista como un mercado de la *privacy* altamente regulado. Basta visitar la hemeroteca para encontrar declaraciones o artículos de diferentes CEO, gurús de Internet y *chief privacy officers* afirmando en el peor de los casos que la privacidad ha muerto, o que no alcanzan a entender lo que piensan o regulan los europeos, en el mejor de ellos. En este sentido, cada paso en la afirmación de la aplicación del Derecho europeo guarda un peligroso parecido con una batalla en el contexto de un escenario de confrontación bélica. Cada paso, desde hacer entender que en España se considera menor maduro a una persona que ha cumplido catorce años -y no los 13 requeridos por la *Children Privacy Protection Act de 1998*– hasta la garantía de los derechos de cancelación sin necesidad de acudir a la jurisdicción del Estado norteamericano de origen de la compañía, es objeto de discusión, negociación o pleito.

En el contexto actual, el caso Snowden, la evolución de la provisión de servicios informáticos a un modelo propio de las *utilities* a través de proveedores de *Cloud Computing* de matriz estadounidense que lideran el mercado, o la emergencia del *Big Data*, complican el escenario y obligan de modo urgente, si no a una convergencia de sistemas a todas luces improbable, al menos a encontrar un punto de encuentro viable entre culturas jurídicas aparentemente antitéticas. A contrastar ambas culturas se dedica este trabajo.

El derecho a la privacidad: un derecho de matriz norteamericana

Existe un acuerdo unánime en considerar a Samuel Warren y Louis Brandeis como los padres del derecho a la vida privada en su seminal artículo The Right to Privacy, publicado por la *Harvard Law Review* en 1890. Como suele ser común en la mejor literatura jurídica norteamericana, se trataba de dar solución a un problema concreto: determinar si el *Common Law* ofrecía alguna respuesta frente a las intromisiones en la vida privada por parte de la prensa escrita y el uso de la ‘fotografía instantánea’.

Warren y Brandeis elaboran un cuerpo teórico que trasladó el centro de gravedad desde una tutela construida sobre los cimientos de la propiedad privada a una nueva construcción cuyo fundamento es la dignidad del hombre y la inviolabilidad de la personalidad humana. Lo que caracterizaría al nuevo derecho sería la facultad del individuo de ejercer un cierto control sobre su vida privada y a ello apuntaban Warren y Brandeis cuando señalaron que el «*Common Law* garantiza a cada persona el derecho a decidir hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones». A los autores el modelo propietario no les parecía adecuado y formularon a partir de este disenso el núcleo central de su teoría, trasladando la tutela del derecho a la intimidad desde el plano de la propiedad al ámbito del

Fundación Telefónica

derecho a la personalidad (Warren y Brandeis, 1890, p. 213)[2].

Llegados a este punto, el lector español no encontrará una diferencia significativa entre el planteamiento de Warren y Brandeis y nuestro entendimiento del derecho a la intimidad. Y no andará muy errado. En realidad, donde se produce el elemento de diferenciación central es en el territorio de la distinción entre el sector público y el privado o, si se prefiere, un modo distinto de entender cómo funciona la *privacy* como derecho frente al Estado y en las relaciones entre particulares. De modo muy resumido, podría decirse que para un ciudadano norteamericano el entendimiento de la privacidad como derecho fundamental opera en sus relaciones con el Estado como límite a la actuación de este. Sin embargo, en las relaciones privadas, el contrato y el resarcimiento del daño serían el elemento determinante en el modo de entender cómo opera la *privacy*.

Intimidad en las relaciones de naturaleza privada

La característica esencial de la garantía del derecho a la privacidad consiste en operar como un derecho de naturaleza reactiva ordenado a resarcir al individuo cuando se produce algún tipo de daño y en especial el daño moral o *intentional infliction of mental distress*, en palabras de Prosser (1960). Este autor identificó cuatro tipos distintos de agravio o *tort*[3], cuyo elemento común residía en la interferencia en el derecho a ser dejado en paz. Estas cuatro categorías de *tort* son: la intrusión en la soledad o retiro o en los asuntos privados, la difusión pública de hechos privados, la información que da una imagen falsa del afectado ante los ojos del público -o *False Light*– y, por último, la apropiación en beneficio propio de la imagen o el nombre ajenos. Prosser concluye que, puesto que cada uno de los cuatro supuestos puede darse independiente o conjuntamente con los demás, lo que ha sucedido es que sobre un único concepto, la *privacy*, los jueces han amparado cuatro supuestos diferenciados de responsabilidad.

Y este es el núcleo de la cuestión: en las relaciones entre privados, el *right to privacy* tendría una naturaleza reactiva ordenada a resarcir un daño. Y si bien es cierto que el recientemente fallecido Alan Westin apuntó a una noción de la *privacy* como control sobre la información personal, sobre la que después volveremos; sin embargo, es la noción iusprivatista la que permea la filosofía empresarial norteamericana. Probablemente sea Fred H. Cate (2000) quien, en un intenso debate doctrinal con Paul Schwartz (2000), resuma mejor cuál es el sentido que se atribuye a la privacidad en las relaciones entre particulares y más concretamente en las de las empresas y corporaciones con sus clientes.

Trazas de la política gubernamental relativa a la información

Cate (2000, pp. 879-891) considera los principios que han venido rigiendo la política gubernamental en lo que se refiere a la información, a saber:

– De una parte, la ponderación de los intereses en presencia en caso de conflicto y la preeminencia bajo ciertas condiciones de la libertad de expresión.

– De otra, la libre circulación de la información y de los datos personales, los cuales constituyen

Fundación Telefónica
Telefónica

la piedra angular de la sociedad democrática y de la economía de mercado, son elemento determinante para la prestación de servicios al consumidor.

– Afirma, como tercer elemento, que la elevada protección de la *privacy* individual está centrada prácticamente de modo exclusivo en la defensa frente a las intromisiones del aparato estatal y en el planteamiento de un concepto de lo privado por oposición con el ámbito de lo público en su dimensión gubernamental.

– En cuarto lugar, señala la utilización del concepto de daño como elemento de la ponderación en los conflictos en los que interviene la *privacy* y como núcleo de la evaluación de los intereses protegidos por aquella.

– Por último, subraya la preferencia del principio de autodeterminación que indica la preeminencia de las soluciones basadas en el mercado, en lo privado y destaca la mayor eficacia de las soluciones no gubernamentales. La competencia y el mercado favorecen así que las empresas, en su búsqueda al servicio del cliente, optimicen las soluciones que le ofrezcan un mayor grado de protección.

Cate examina en la práctica la aplicación de los principios de protección de la privacidad tomando como referencia la *Driver's Privacy Protection Act of 1994* y la *Transportation Appropriations Act* de 2000 y, concretamente, la preferencia por las cláusulas de consentimiento expreso (*opt-in*) o implícito (*opt-out*). El autor señala que las cláusulas de *opt-in*, al exigir una actuación positiva del interesado, no suelen ser ejercidas por los ciudadanos y elevan los costes para las empresas, que acaban repercutiendo sobre el consumidor ya que exigen contactar con cada cliente. De este modo, las limitaciones al principio de *opt-out* suponen un gran obstáculo para la libre circulación de la información sin aportar una especial protección para la vida privada y reduciendo de facto la cantidad de información que recibe el ciudadano. Por último, con referencia a la actividad empresarial, señala que en ningún caso las actividades propias del *marketing* comercial causan un daño apreciable a los individuos.

En la misma línea apuntan las conclusiones de Solove (2006) sobre la operatividad de la *Fair Credit Reporting Act* y las prácticas reguladoras a nivel federal. En esencia, si bien puede apuntarse la presencia de ciertos principios básicos de protección de datos (*fair information principles*), en la práctica rige un principio de libre uso de la información disponible y de *opting out*. Por otra parte, la ausencia de una ley que de modo global regule los tratamientos de información del sector privado comporta que la autorregulación deba jugar un papel central en muchos ámbitos.

Los derechos frente al Estado: las garantías de la Cuarta Enmienda

El catálogo de derechos fundamentales que incorporó la Constitución norteamericana incluye una garantía expresa de la privacidad en su Cuarta Enmienda que regula la inviolabilidad del domicilio. No obstante, no es el único contexto en el que se garantiza el derecho a la vida privada, ya que el conflicto con la libertad de expresión ha sido enjuiciado por el Tribunal Supremo en reiteradas ocasiones.

Fundación Telefónica
Telefónica

Por otra parte, se ha evaluado la capacidad de injerencia del Estado respecto del acceso a información contenida en registros asociativos, la penalización de la homosexualidad o en relación con las decisiones reproductivas. El Tribunal ha buscado siempre amparar el derecho en las 'sombras y penumbras' del texto constitucional, relacionando derechos expresamente reconocidos con el *Due Process of Law* para inferir un deber de abstención estatal y la necesaria garantía judicial en aquellos casos en los que se investiga un delito.

La Cuarta Enmienda y el modo de ser aplicada, ilustran de modo muy preciso esta filosofía. Esta dispone: «El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas».

Se trataba de garantizar la libertad personal y también de asegurar el pleno respeto al derecho de propiedad, evitándose así los registros -personales o dominicales- y las aprehensiones de bienes, documentos, etc. Para ello, este tipo de actuaciones debían sujetarse a ciertas condiciones preestablecidas. En esencia, el precepto suponía una doble exigencia, consistente en la emisión de un mandato por un juez neutral en presencia de un hecho que justificase tal acción, lo que se ha dado en llamar 'causa probable'.

Un país, dos modelos

Desde la perspectiva de la protección de la *privacy* pueden situarse dos etapas claramente diferenciadas en la evolución de la figura. La primera puede definirse como la de la *privacy-property*, cuyo mejor exponente es el caso *Olmstead v. United States*[4]. Esta fase estuvo marcada por una concepción del derecho como garante de la propiedad privada frente a las intromisiones del Estado y delimitada por la regla del *trespass*, por la necesidad de que se produjese algún tipo de intromisión física, para delimitar la existencia de una intromisión en el bien protegido por la Enmienda. En la segunda etapa, encarnada por casos como Warden[5] y Katz[6], se abre paso una concepción más espiritualista basada en la tutela de la *privacy* desligándola, al menos en parte, del modelo propietario.

En resumen, el ciudadano posee una esfera de protección frente las acciones del Estado a la hora de realizar una entrada o registro, tomar imágenes del interior de una vivienda o interceptar una comunicación telefónica. Esta esfera, proporcionada por el derecho a la vida privada garantiza que las intromisiones, físicas o no, requerirán de un mandato judicial basado en una causa justificada o probable.

Este planteamiento evolucionó a marchas forzadas con la aparición de las tecnologías de la información, dando lugar a la *Privacy Act de 1974*. Esta ley se inspira sin lugar a dudas en la noción de *informational privacy*. Esta teoría tiene en Alan F. Westin (1970) su máximo exponente, en cuya obra se analizan concienzudamente los distintos problemas que aquejaban en las décadas de 1960 y 1970 a la vida privada en los EEUU.

Westin plantea un nuevo modo de entender la privacidad concebida desde el punto de vista de

Fundación Telefónica
Telefónica

la relación del individuo con la sociedad que comporta una exclusión voluntaria y temporal, una suerte de retiro solitario o en un grupo reducido respecto del resto, e incorpora la reclamación de la capacidad de decidir cuándo comunicar información a los demás[7]. A este planteamiento se llega gracias a un exhaustivo análisis sobre el fenómeno y el influjo sobre la privacidad de las innovaciones tecnológicas de modo que en relación con la informática Westin precisa su noción de *informational privacy*, que define como un derecho a decidir sobre la propia información, un derecho de propiedad que permite excluir las interferencias públicas o privadas. Junto a este concepto, es necesario entender que la información personal, cuando circula, constituye una mercancía peligrosa y crea especiales deberes y responsabilidades para quienes la tratan[8].

Westin plantea un enfoque claramente informacional de la vida privada, ya que la protección de esta incluso alcanzaría a ciertos comportamientos que generan espacios de naturaleza privada incluso en lugares públicos. Finalmente, debe subrayarse que atribuye un papel esencial a la *privacy* para conformar la actuación de los individuos y de los grupos en que se integran en el contexto de un gobierno democrático.

A las aportaciones de Westin y la doctrina hay que sumar el informe *Records, Computers and the Rights of Citizens* (HEW Report, 1973), cuyos principios se sitúan en el origen e inspiración de la *Privacy Act* de 1974:
– No deben existir sistemas de tratamiento de datos personales de carácter secreto.
– Los individuos deben disponer de un modo de conocer el tipo de información que sobre ellos pueda existir en un fichero y conocer cómo se utiliza.
– El individuo debe poder impedir que el dato personal obtenido para una finalidad se use con un propósito diferente.
– Debe existir un procedimiento que permita rectificar la información disponible.
– La organización que trata los datos debe ofrecer condiciones de fiabilidad y/o confianza y adoptar medidas que eviten usos indebidos.

La *Privacy Act* fija a partir del *HEW Report* un conjunto de principios que regulan el tratamiento de datos personales por las agencias gubernamentales. A los arriba señalados se añaden límites al uso del número de la Seguridad Social como identificador único, una regulación estricta del principio de finalidad y de la conservación de los datos, ofreciendo un procedimiento de tutela ante las vulneraciones.

El papel emergente de la Federal Trade Commission

Solove y Hartzog (en prensa) destacan que en EEUU no existe un cuerpo sólido de jurisprudencia que relacione el derecho a la privacidad con la actuación de las compañías. En la práctica, el despliegue de funciones de enforcement de la Federal Trade Commision (FTC) en los últimos quince años ha dado lugar a un corpus cuasi jurisprudencial de conocimiento basado en los acuerdos que esta Agencia alcanza con las compañías, sus informes, la elaboración de buenas prácticas y de *guidelines*.

Como se ha señalado, en EEUU convive un doble escenario regulador y de tutela, según nos refiramos al sector público o al privado, junto con una fragmentación normativa particularmente

Fundación Telefónica
Telefónica

significativa. Por otra parte, la necesaria concurrencia de la acreditación de un daño hace que la jurisprudencia de los tribunales en casos civiles vinculada al *Tort Law* sea prácticamente inexistente en lo que a privacidad se refiere. Sin embargo, la FTC puede evaluar y actuar para verificar hasta qué punto las empresas vulneran o incumplen los compromisos de privacidad que adquieren con sus clientes e incurren en prácticas engañosas o desleales. Ello, en caso de empresas no sometidas a regulación específica, convierte a la FTC en regulador primario y confiere a su práctica en un cuerpo normativo singular.

Una de las características del derecho a la vida privada a partir de la década de 1990 y en paralelo al crecimiento de Internet ha sido el hecho de que las políticas de privacidad se desgajan en un documento separado de los términos y condiciones legales. Las políticas de privacidad surgieron como un mecanismo de autorregulación aceptado que fue incluso incorporado como deber en las leyes sectoriales posteriores como la *Graham-Leach-Bliley Act* de 1999. Estas políticas incorporan una suerte de compromiso exigible (*enforceable promise*) cuyo garante primario sería la FTC.

La FTC juega un rol determinante frente a prácticas y actos desleales o fraudulentos o que causen o puedan causar un perjuicio grave a los consumidores que estos no puedan evitar. En la práctica, esto ha convertido a la FTC, en opinión de los citados autores, en una autoridad de protección de datos de facto. Añádase el papel fundamental que se le confiere sometiendo a su jurisdicción las compañías americanas que suscriben el acuerdo *Safe Harbour*, crucial para el flujo de datos entre la UE y EEUU. Pero además, su influencia se acrecienta por cuanto puede transferir credibilidad a los mecanismos de autorregulación empresarial y someterlos a su *enforcement*, especialmente cuando la compañía no asume ningún tipo de responsabilidad o cláusula de compensación al cliente ante un incumplimiento. En cualquier caso, su capacidad de sanción no es elevada, aunque -subrayan los autores- el impacto reputacional de sus decisiones resulta significativo.

Consent orders

En opinión de Solove y Hartzog, las *consent orders* de la FTC permiten establecer patrones y directrices capaces de orientar el cumplimiento normativo para el sector. En esencia, la FTC puede desarrollar investigaciones que incluyan algún mandato vinculante (*corrective action*), pero además se permite a las compañías negociar un acuerdo que evite el baldón público de admitir un incumplimiento, lo que al parecer resulta particularmente eficaz. De hecho, solo en dos de 150 casos se ha llegado a un litigio. Las sanciones impuestas han ido de los mil a los treinta y cinco millones de dólares, aunque los acuerdos no tienen por qué suponer el pago de una sanción.

La estructura de sus *consent orders* suele incluir sanciones económicas, prohibiciones de hacer y requerimientos de realizar actuaciones que corrijan la conducta. Además, pueden incluir informes y *guidelines* con previsiones de cumplimiento que pueden extenderse a los siguientes años, con el deber de reportar periódicamente a la FTC. Las resoluciones pueden comportar el deber de notificar al consumidor y de ofrecerle alguna forma de reparar la acción errónea, lo que no implica necesariamente una compensación económica. También pueden incorporar deberes de borrado de datos, cambios en las políticas de privacidad, programas integrales de

Fundación Telefónica
Telefónica

cumplimiento normativo en privacidad o sometimiento a auditorías regulares por profesionales independientes.

El resultado práctico del escenario que acabamos de dibujar parece caracterizarse por varios factores determinantes. Primero, la existencia de una amplia zona de disposición para el tratamiento de la información personal que favorece el desarrollo de nuevos modelos de negocio basados en el uso intensivo de información personal. En segundo lugar, la aparición en el mercado de empresas altamente especializadas en la explotación y comercialización de datos personales; o de empresas -como buscadores y redes sociales- que explotan al máximo las posibilidades que ofrece el tratamiento de datos personales. El último factor, y quizá el más determinante, reside en el sistema de tutela al que nos referíamos al inicio. Con excepción de las limitadas competencias de la Federal Trade Commision, no parece que exista un método de tutela comparable al sistema europeo.

Este conjunto de factores parecen impulsar los pasos de la Administración Obama en orden a legislar mediante su propuesta de *Privacy Bill of Rights*[9], que busca una regulación integral de la privacidad que encuentre un equilibrio de derechos que facilite el ritmo de innovación y, a la vez, refuerce la capacidad de *enforcement* de la FTC.

La privacidad a este lado del Atlántico

En el contexto europeo y en particular en el español, resulta necesario en muchas ocasiones diferenciar entre privacidad, derecho a la intimidad y derecho fundamental a la protección de datos. Por lo que se refiere a este trabajo, en la medida que constituye el objeto central del debate nos ocuparemos de la protección de datos personales.

Es sabido que el llamado derecho a la autodeterminación informativa nace en la República Federal Alemana con la sentencia dictada por el Tribunal Constitucional Federal Alemán (TCFA) en la sentencia sobre la Ley del Censo. El TCFA afirma en la sentencia que el derecho general de la personalidad comporta la atribución al individuo de la capacidad de decidir, en el ejercicio de su autodeterminación, qué extremos desea revelar de su propia vida. Para el TCFA, «la autodeterminación del individuo presupone -también en las condiciones de las técnicas modernas de tratamiento de la información- que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma consecuente con la decisión adoptada».

Esta libertad de decisión, de control, supone además que el individuo tenga la posibilidad de acceder a sus datos personales, que pueda no solo tener conocimiento de que otros procesan informaciones relativas a su persona, sino también someter el uso de estas a un control, ya que, de lo contrario, se limitará su libertad de decidir por autodeterminación». La consecuencia de este razonamiento es el reconocimiento jurisprudencial de un derecho fundamental a la autodeterminación informativa basado en el derecho general de la personalidad y que ofrece protección frente a la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos de carácter personal y «garantiza la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y la utilización de sus datos personales».

Fundación Telefónica

El derecho a la protección de datos en la jurisprudencia del Tribunal Constitucional

Este planteamiento, incorporado a nuestro país por la más reputada doctrina (Lucas, 1990), ha sido acogido finalmente por la jurisprudencia del Tribunal Constitucional, que ha alumbrado el derecho fundamental a la protección de datos a través de un conjunto de sentencias dictadas en el periodo que va de 1993 a 2000. Debe señalarse que la primera sentencia, la No. 254/1993, recoge el derecho, al que denomina libertad informática, de un modo ciertamente confuso, para después ir poco a poco perfilando el contorno del nuevo derecho.

Será en la STC 292/2000 donde el Alto Tribunal diseñe con nitidez el contenido del derecho fundamental a la protección de datos. El fundamento jurídico quinto de la sentencia confirma la interpretación conforme a la cual el artículo 18.4 CE incorpora un nuevo derecho fundamental, dotándolo de plena autonomía respecto del derecho a la intimidad: «Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran».

En el mismo fundamento se describe el contenido del derecho fundamental a la protección de datos, que incluye un haz de garantías y facultades que se traducen en determinadas obligaciones de hacer. Se trata del derecho a que se requiera el previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos.

Junto a ello, la evolución normativa en Europa ha tomado un camino que conduce irremediablemente al reconocimiento de este derecho. El derecho fundamental a la protección de datos se ha consolidado claramente en el Contexto del Consejo de Europa mediante el Convenio 108/1981 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y en la reiterada jurisprudencia del Tribunal Europeo de Derechos Humanos. Por otra parte, el conjunto de Directivas dictadas por la UE en esta materia, la juridicidad conferida a la *Carta Europea de Derechos Fundamentales*, junto con la reciente Propuesta de Reglamento General de Protección de Datos de la Comisión Europea, marcan una tendencia muy clara.

La apuesta europea

Europa apuesta por una conformación del derecho fundamental a la protección de datos como un derecho de clara naturaleza prestacional. No solo concede facultades reactivas ante una vulneración -como el derecho de tutela judicial o administrativa, el derecho de rectificación o cancelación-, sino también un conjunto de deberes, de obligaciones de hacer que se imponen

Fundación Telefónica
Telefónica

al responsable. Estas obligaciones, según el tipo de trasposición realizada por cada Estado miembro, incorporan un deber de registro previo de los ficheros, el deber de información en la recogida de los datos personales y de obtención leal del consentimiento, la garantía de los derechos de acceso, rectificación cancelación y oposición al tratamiento, la garantía de la seguridad y el secreto y la formalización de procedimientos en casos de comunicaciones de datos personales, prestaciones de servicios o transferencias internacionales.

Sin embargo, la trasposición dio lugar a realidades normativas muy diversas que la Propuesta de Reglamento arriba referida pretende ahora unificar. La Propuesta no solo incorpora los principios descritos, sino que supone una seria profundización en el modelo por cuanto:
– Incrementa la capacidad de *enforcement* de las autoridades de protección de datos.
– Impone deberes de diseño previo basado en privacidad (*privacy by design*, *privacy impact assessment*).
– Refuerza las labores de documentación de los tratamientos.
– Generaliza la figura del *Data Protection Officer.*
– Refuerza el valor del consentimiento.
– Profundiza en la garantía de la seguridad e incorpora la notificación de incidentes a reguladores y usuarios.
– Fija condiciones de protección de los derechos de los menores.
– Precisa las condiciones de aplicación extraterritorial de la norma de la Unión Europea a los operadores que traten datos de personas ubicadas en suelo europeo.

El resultado práctico es una evolución hacía un modelo que acentúa las divergencias con el norteamericano. Allí donde en EEUU operan principios de libre comercio y *opting out*, en la UE se refuerza la metodología del consentimiento expreso y la posición jurídica del afectado. Si en EEUU la eficacia de los derechos fundamentales entre particulares es muy débil, en la UE se afirma con rotundidad. En esencia, la regulación europea profundiza en su carácter tuitivo obligando a los operadores de matriz norteamericana a incorporar prácticas ajenas a su cultura jurídica.

Tal vez vaya siendo hora de recuperar el diálogo trasatlántico y encontrar un punto de encuentro en la Resolución de Madrid sobre una propuesta conjunta de estándares internacionales de protección de datos y privacidad.

Bibliografía

Agencia Española de Protección de Datos (AEPD) (2007). *Creación de sistemas de denuncias internas en las empresas (mecanismos de whistleblowing)* [informe jurídico en línea]. Madrid: AEPD. Disponible en:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/index-ides-idphp.php

– (2009). *Resolución de Madrid sobre una propuesta conjunta de estándares internacionales de protección de datos y privacidad* [en línea]. Disponible en:
https://www.agpd.es/portalwebAGPD/internacional/Estandares_Internacionales/conferencia-ides-idphp.php

Fundación Telefónica
Telefónica

Cate, F. H. (1997). *Privacy in the Information Age*. Washington, D. C.: Brookings Institution Press.

– (2000). Principles on Internet Privacy. *Connecticut Law Review*, 32, 877-896.

Lucas Murillo de la Cueva, P. (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

Prosser, W. (1960). Privacy. *California Law Review*, 48, 383-423.

Schwartz, P. M. (2000). Internet privacy and the State. *Connecticut Law Review*, 32, 815-859.

Secretary's Advisory Committee on Automated Personal Data Systems (1973, july). Records, Computers and the Rights of Citizens [en línea]. Secretary's Advisory, Department of Health, Education, and Welfare [new Health and Human Services]. Disponible en: *http://epic.org/privacy/hew1973report/* [Consulta: 2013, 12 de diciembre]

Solove, D. J y Hoofnagle, C. J. (2006). A Model Regime of Privacy Protection. *University of Illinois* [en línea], 2006(2), 357-403. Disponible en: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=881294##.*

Solove, D. y Hartzog, W. (en prensa). The FTC and the New Common Law of Privacy, *Columbia Law Review* [en línea]. Disponible en: *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2312913*

Warren , S. D. y Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, IV(5), 193-220.

Westin, A. F. (1970). *Privacy and freedo*m. 6a. ed. New York: Atheneum.

Notas

[1] Véase el informe de la Agencia Española de Protección de Datos sobre Creación de sistemas de denuncias internas en las empresas (mecanismos de whistleblowing). Disponible en: *https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2007-0128_Creaci-oo-n-de-sistemas-de-denuncias-internas-en-las-empresas-mecanismos-de-whistleblowing.pdf*. [Consulta: 2013, 12 de diciembre].

[2] En el original: «*We must therefore conclude that rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate*

Fundación Telefónica

when it extend this protection to the personal appearance, sayings acts, and to personal relation, domestic or otherwise» (Warren y Brandeis, 1890, p. 213).

[3] Véase la voz *tort*, en *The Lectric Law Library's Lexicon On* [en línea]. Disponible en: *http://www.lectlaw.com/def2/t032.htm* [Consulta: 2013, 12 de diciembre].

[4] Olmstead v. United States, 277 U. S. 438 (1928).

[5] Warden v. Hayden, 387 U. S. 294 (1967).

[6] Katz v. United States, 389 U. S. 347 (1967).

[7] Texto original: «*Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extend information is comunicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonimity or reserve*» (Westin, 1970, p. 7).

[8] Texto original: «*First, personal information, thought of as the right of decision over one's private personality, should be defined as a property right, with all the restraints on interference by public or private authorities and due-process guarantees that our law of property has been so skillful in devising. Along with this concept should go the idea that circulation of personal information by someone other than the owner or his trusted agent is handling a dangerous commodity in interstate commerce, and creates special duties and liabilities on the information utility or government system handling it*» (Westin, 1970, pp. 324-325).

[9] Véase: *http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights* [Consulta: 2013, 12 de diciembre].

Fundación Telefónica
Telefónica