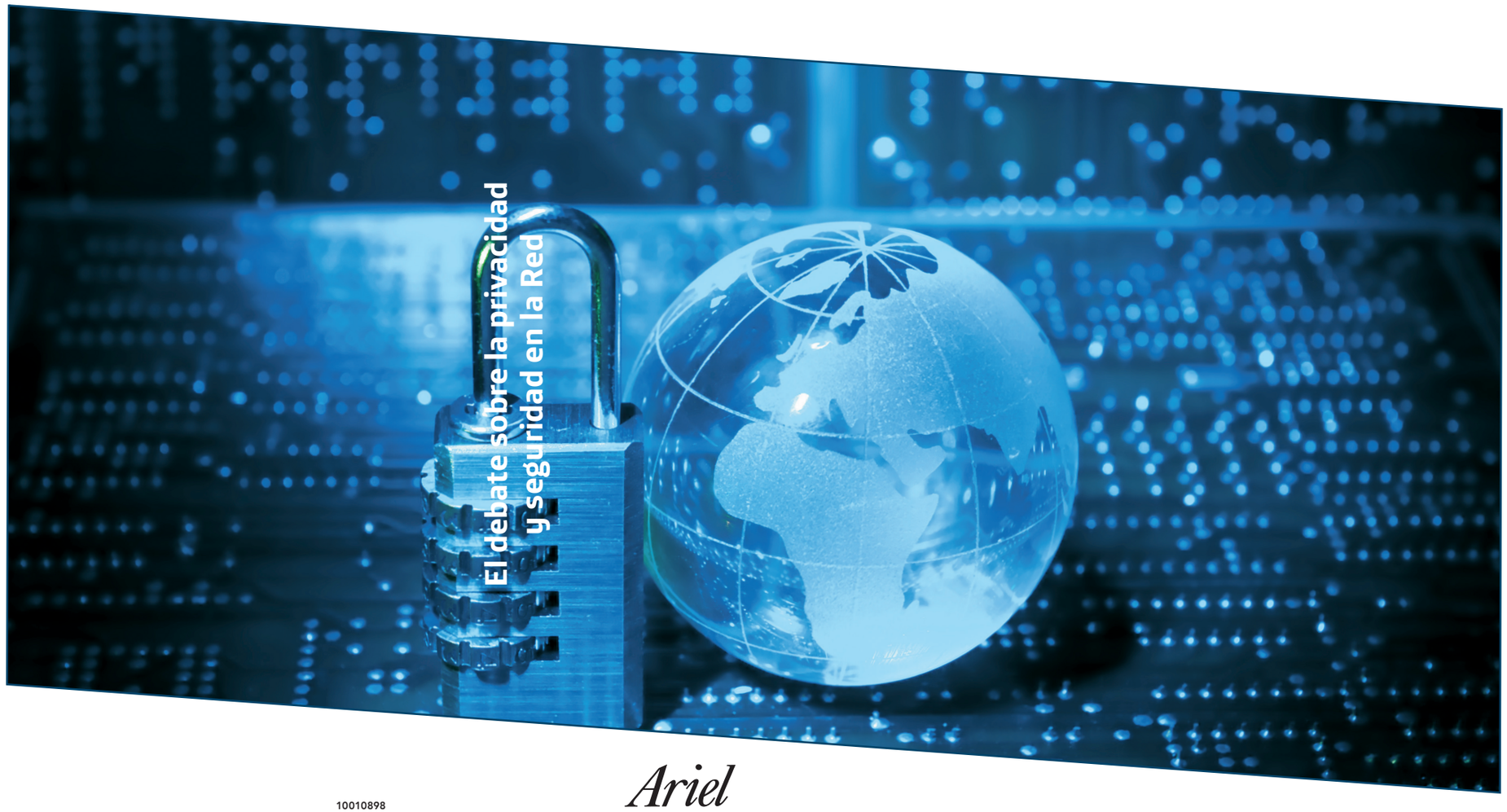
La evolución tecnológica de la última década ha incrementado la capacidad de recogida, uso y almacenamiento de datos personales en un entorno abierto y global, donde se difuminan las barreras territoriales y los sistemas legales que regulan la privacidad. Esto ha dado lugar a un importante debate sobre el desarrollo futuro del ecosistema Internet y la economía digital en el que urge una mayor armonización reguladora. Esta necesidad se materializa dentro de la UE en la propuesta de Reglamento de la Comisión Europea de 2012 y plantea nuevos retos en la relación con el resto de áreas geográfico-económicas en un mercado que se perfila del todo global.

A partir de las contribuciones de los expertos más relevantes del mundo académico y empresarial que han participado en este debate, tanto en EE. UU. como en Europa, se analizan sus orígenes, evolución y perspectivas.

Es, sin duda, un libro de gran interés que proporciona los distintos puntos de vista sobre un tema tan controvertido como es la privacidad en la Red.

Fundación Telefónica

El debate sobre la privacidad y seguridad en la Red: Regulación y mercados



Ariel

10010898
9 788408 034360
PVP. 15,00 €

Cuaderno 36

Fundación Telefónica

Telefónica

Fundación Telefónica

Telefónica

EL DEBATE SOBRE LA PRIVACIDAD Y SEGURIDAD EN LA RED: REGULACIÓN Y MERCADOS

Coordinadores:

Jorge Pérez y Enrique Badía

Ariel

COLECCIÓN
Fundación Telefónica

Esta obra ha sido editada por Ariel y Fundación Telefónica, en colaboración con Editorial Planeta, que no comparten necesariamente los contenidos expresados en ella. Dichos contenidos son responsabilidad exclusiva de sus autores.

Coordinación editorial de Fundación Telefónica: Rosa María Sáinz Peña
Primera edición: diciembre de 2012

ISBN: 978-84-08-03436-0

Depósito legal: B. 33.228-2012
Impresión y encuadernación: UNIGRAF, S.L.
Impreso en España – Printed in Spain

El papel utilizado para la impresión de este libro es cien por cien libre de cloro y está calificado como **papel ecológico**.

Índice

Prólogo

Todos somos conscientes de cómo las telecomunicaciones han penetrado de forma intensiva en la dinámica de la sociedad. Las posibilidades de intercomunicación y acceso se han multiplicado de forma exponencial en las dos últimas décadas y todo indica que el proceso está lejos de haber alcanzado su culminación. Los avances de la tecnología han *destruido* –en el sentido más schumpeteriano del término– barreras largo tiempo asentadas como la ubicación, la distancia y el acceso presencial, comprendiendo personas, datos e información. Hoy, prácticamente todo está al alcance en tiempo real y el futuro se perfila plagado de innovaciones que harán todo aún más accesible, a mayor velocidad y con creciente calidad.

Pero esa realidad ha planteado también nuevos retos, desafíos renovados y enfoques distintos que corresponde abordar. Uno de ellos atañe, sin duda, a la privacidad y, visto desde otro plano, a la seguridad. No es que sea una cuestión –en realidad un derecho– emergente, pero sí requiere de una nueva aproximación porque nuevos son los resquicios, si se prefiere retos, que empiezan a percibirse relacionados con la debida protección de los datos de índole personal.

Nuestras sociedades llevan más de un siglo dotadas de normas eficaces que garantizan la inviolabilidad de las comunicaciones postales y telefónicas, en muchos casos dotadas incluso de rango constitucional. De ello, probablemente, surge la demanda ciudadana de extender la salvaguardia al vasto y cada vez más extendido universo Internet, atendiendo a aspectos tan relevantes como qué datos se obtienen o facilitan y cómo se asegura que su utilización no exceda los límites de consentimiento otorgado de forma individual.

Europa viene abordando esta cuestión tomando como base aspectos muy asentados en nuestra idiosincrasia que, en general y a lo largo de la historia, han evidenciado preocupación y respeto por la preservación del derecho personal a la intimidad.

También, como en otros asuntos, el desafío europeo comporta dar adecuada respuesta a un reto esencial: diseñar un marco normativo que proteja eficazmente esos derechos sin cercenar las opciones de desarrollo e innovación de la industria ni, en consecuencia, limitar las opciones de competir en el escenario global. De ahí que la regulación, cuya necesaria puesta al día nadie discute, deba evitar considerar *aislado* el ámbito de aplicación comunitario, porque no lo está.

Consciente de todo ello, la industria de telecomunicaciones viene colaborando muy activamente en los trabajos que las distintas instituciones públicas realizan para poner al día el marco legal de privacidad y seguridad;

en particular, los abordados por la Comisión, el Consejo y el Parlamento europeos para la puesta al día de Reglamentos y Directivas acordes con la realidad.

En Fundación Telefónica, por otra parte, nos hemos impuesto hace tiempo la línea de contribuir al análisis y el contraste de posiciones frente a las realidades con que arranca el actual siglo XXI. Los libros que publicamos en nuestra colección *Fundación Telefónica-Ariel* abordan ese tipo de cuestiones, y convocan la participación de autores y expertos de reconocida solvencia, provenientes tanto del ámbito científico-académico como del mundo de la empresa y el resto de los agentes del sector. En esta oportunidad, en concreto, hemos decidido abordar un tema que en realidad entraña dos vertientes: privacidad y seguridad.

Desde Fundación Telefónica entendimos, en suma, que no debíamos dejar pasar la oportunidad de reunir en una nueva publicación las ideas y reflexiones de quienes, aunque con puntos de vista a menudo discrepantes, comparten el esfuerzo de analizar, estudiar y formular propuestas sobre el indicado binomio privacidad-seguridad. Como en libros anteriores, nuestra intención es aportar una herramienta que contribuya a que las decisiones se adopten con mayor conocimiento.

Desearía que el libro fuera recibido como una contribución relevante de pensamiento y reflexión a un debate en muchos aspectos trascendente que valdría la pena que se saldara con la implementación de soluciones capaces de aunar y equilibrar los objetivos, derechos y aspiraciones de todos. La experiencia y la historia son concluyentes: solo las reglas que logran ser formuladas *a favor de todos* perduran y contribuyen al desarrollo y al progreso de la sociedad.

César Alierta Izuel
Presidente ejecutivo de Telefónica
Presidente de Fundación Telefónica

Resumen ejecutivo

Durante la última década se han producido fenómenos tan relevantes como el crecimiento exponencial del número de usuarios de Internet, la proliferación de ordenadores, *smartphones* y otros dispositivos avanzados, la extensión de la banda ancha móvil, y la multiplicación de servicios como correo y comercio electrónicos, *cloud computing*, redes sociales y muchos otros directamente asociados a la web. Todo ello ha generado importantes beneficios económicos y sociales, al punto de haberse incorporado como parte fundamental de la vida diaria de los ciudadanos y permitido mayores posibilidades de comunicación, colaboración y compartición.

La evolución tecnológica ha incrementado, al mismo tiempo, la capacidad de recogida, uso y almacenamiento de datos personales, en gran medida por motivos de eficiencia, comerciales o de seguridad, por parte de múltiples agentes públicos y privados. Este proceso tiene lugar en un entorno abierto y global, donde se difuminan las barreras territoriales y los sistemas legales que regulan la privacidad y el intercambio de datos de índole personal.

Conforme el tratamiento de los datos personales se ha ido desplazando hacia posiciones de mayor relevancia para el desarrollo de nuevos servicios –sea para obtener ingresos a través de publicidad o generar servicios más eficientes y competitivos– la regulación asociada ha pasado de ser un elemento lateral, que era necesario cumplir, a constituir un factor fundamental, al menos en dos aspectos: para preservar el derecho individual a la intimidad bajo los nuevos parámetros de la realidad, y también como potencial obstáculo a la actividad de los agentes, imponiéndoles sobrecostes indebidos.

En ese contexto se está llevando a cabo la actualización del modelo regulador europeo, cuya norma fundamental, la Directiva de protección de datos de 1995, lleva sometida desde 2007 a un proceso de revisión y consulta. La reciente propuesta de Reglamento general de protección de datos, realizada a principios de 2012, supone el inicio del proceso legislativo ordinario por el que la Comisión, el Parlamento y el Consejo avanzarán hacia la configuración del nuevo marco europeo de protección de datos que se prevé entrará en vigor entre los años 2015 y 2016.

La trascendencia de tales cuestiones ha dado lugar a un importante debate sobre el desarrollo futuro del ecosistema Internet y la economía digital en el espacio europeo que, más allá de las discrepancias y enfoques contrapuestos, muestra cierta coincidencia en considerar que urge una mayor armonización reguladora; por descontado, entre los veintisiete Estados miembros de la Unión Europea (UE), pero no menos con el resto de las áreas

geográfico-económicas, en particular Estados Unidos (EE. UU.), en aras de propiciar una equidad competitiva en un mercado que –si cabe más que otros– se perfila del todo global.

Marco conceptual de privacidad y protección de datos

Privacidad es un concepto plural ligado al individuo. No existe una idea uniforme sobre ella ni, en consecuencia, una apreciación normativa y jurisprudencial compartida. Sí existe, en cambio, una generalizada sensibilidad social, individual y colectiva, que considera la privacidad como un derecho protegible y, en sentido inverso, se aprecia una notable preocupación por los ataques y violaciones que se puedan estar produciendo. Esto ha llevado a que, a lo largo del tiempo, la protección efectiva de ese derecho haya migrado desde la acción individual a la incorporación de distintos grados y formas de tutela a cargo de los poderes públicos; esto es, los Estados y sus mecanismos de intervención.

La extensión generalizada de acceso y uso de Internet ha variado los parámetros sobre los que se venía asentando la protección del derecho a la privacidad, tanto debido a la potenciación del efecto viral de la Red como a causa de la multiplicación de agentes, modelos de negocio, servicios, utilidades, herramientas, etcétera. Ello ha desembocado en una nueva ecuación entre prestadores de servicios y usuarios, planteando tres elementos fundamentales en relación con la privacidad:

- **Valor creciente de los datos.** Los datos se han convertido en una variable estratégica de las compañías, más allá de su mayor o menor presencia en la Red. Su utilización tendrá un impacto relevante en el desarrollo de modelos de negocio más eficientes y efectivos, por lo que el establecimiento de políticas de protección podría afectar a la capacidad de generar valor.

- **Globalización como elemento condicionante.** Más allá de la globalización imperante en la dinámica económica, la arquitectura propia de Internet facilita que el agente proveedor/prestador del servicio pueda –de hecho, así ocurre– estar radicado en territorios en absoluto coincidentes con el de ubicación del usuario. Esto provoca, en consecuencia, que uno y otro estén teórica y efectivamente sujetos a marcos jurídicos diferentes, no siempre con plena conciencia del sujeto del derecho a preservar su privacidad ni posibilidad material de hacerlo valer.

- **Publicidad en el centro de la mayor parte de modelos de negocio *online*.** La tendencia a migrar las inversiones publicitarias desde un planteamiento cuantitativo –*mass media*–, hacia otro más cualitativo –personalizado, basado en el comportamiento– incrementa el valor de los datos; entre ellos, los capturados en los distintos usos y modalidades de *navegación*. Esta evolución publicitaria es y seguirá siendo bastante determinante y deberá merecer atención específica en los renovados marcos de protección, al situarse la publicidad como uno de los principales motores de ingresos para los servicios prestados en Internet.

De esta forma, tanto Internet como la evolución del elemento tecnológico suponen factores muy relevantes que, por un lado, incrementan los riesgos a la invasión de la privacidad (captura, tratamiento, provisión, gestión de los datos privados...), pero resultan también y han de resultar todavía más determinantes para articular mecanismos de salvaguardia, protección, transparencia y control.

La respuesta normativa debería avanzar hacia marcos jurídicos *equilibrados* y jurisprudencias *comunes* que permitan solventar las problemáticas de privacidad y protección de

datos en Internet, pero obtener al mismo tiempo los beneficios potenciales de los nuevos negocios de economía digital ligados al procesado de datos. De cómo se articule el modelo regulador dependerá en buena medida el posicionamiento europeo en el contexto global y, en tal sentido, convendrá considerar algunas premisas:

- **Necesidad de cambio regulador y mayor armonización.** La necesidad de actualizar los marcos de regulación, asumiendo los nuevos parámetros y circunstancias que impone el carácter masivo de Internet, es común a todos, por lo que es el momento oportuno para establecer una convergencia reguladora, sin necesidad ni riesgo de situar una concepción o tradición históricas por encima de las demás.

- **Mantener el factor competitivo entre los distintos agentes.** Cualquier asimetría reguladora deviene en ventaja/desventaja competitiva, con un potencial altamente distorsionante para las oportunidades de presencia activa en los distintos negocios. Europa debe estar particularmente atenta, habida cuenta de los precedentes –poco favorables– ya consolidados en el mundo Internet.

- **Incrementar la seguridad jurídica.** Por una parte, parece ser necesario para las empresas con presencia activa en distintos mercados; por otra, para los propios usuarios, de forma que no vean limitada la capacidad de ejercitar su derecho a la protección.

- **Evitar la aparición de «paraísos» relativos a la privacidad y protección de datos.** Parece importante evitar cualquier posible situación de extraterritorialidad, sea física o sectorial, que propicie la consolidación de sitios con capacidad competitiva incrementada por quedar al margen de la norma.

- **Mejorar la transparencia y la seguridad.** La consecución de ambos efectos, sin duda precisos para que el usuario sienta eficaces las garantías, solo se antoja factible si existe un marco común de obligada observancia para todos los agentes, con independencia de cuál sea su ubicación.

- **Consentimiento transparente.** La falta de conciencia e incluso de conocimiento del usuario sobre los datos que está vertiendo en la Red se suele extender al alcance del consentimiento tácita o explícitamente otorgado. Parece, pues, preciso fijar estándares comunes de transparencia sobre la captura de datos y nuevas formas de otorgar consentimiento que sean lo más asequibles posible al usuario medio, sin obligarle a la realización de procedimientos o trámites complejos ni exigirle un conocimiento especializado, sea técnico o jurídico.

Modelos diferentes para proteger la privacidad en el escenario global

Causas de distinto tipo subyacen tras una realidad reguladora dispar y en cierta medida asimétrica, no solo entre la UE y EE. UU., sino igual o más apreciables entre los veintisiete estados comunitarios.

En la UE el derecho a la privacidad está mayoritariamente considerado como una parte integral del respeto a la vida privada, incorporando en él la protección de datos de carácter personal. El marco normativo comunitario comprende la Directiva de protección de datos de 1995, la Directiva sobre la privacidad y las comunicaciones electrónicas de 2002, enmendada en 2006 y 2009, así como leyes in-

tegrales y sectoriales nacionales. Asimismo, se han establecido en la UE agencias nacionales encargadas de la vigilancia y la defensa de los derechos sobre los datos, dotando a Europa de un sistema robusto de protección.

Sin embargo, la implementación del marco de 1995 no ha estado exenta de problemática y limitaciones en el proceso de armonización, con la aparición de numerosas barreras, en cierta medida conducentes al proceso de reforma iniciado en 2007 por la Comisión Europea. Dicho proceso alcanzó un punto clave a principios de 2012 con la publicación de la propuesta de un nuevo Reglamento general de protección de datos, que inicia el proceso legislativo ordinario entre Parlamento, Consejo y Comisión para configurar el nuevo marco europeo de protección de datos, que podría entrar en vigor entre 2015 y 2016.

En EE. UU., a diferencia de la UE, privacidad y protección de datos no son percibidas como derechos fundamentales, sino como problemática relacionada con la defensa de la competencia y los derechos de los consumidores, combinando actuaciones de los poderes judicial y legislativo. El marco estadounidense no se articula mediante leyes específicas de aplicación general, sino mediante leyes sectoriales, a nivel federal y estatal, ambas completadas por la actuación del organismo regulador de competencia –FTC, *Federal Trade Commission* –, con gran impacto sobre la problemática de privacidad.

Entre las principales iniciativas en materia de privacidad y protección de datos adoptadas en EE. UU. merecen destacarse el plan de revisión del marco normativo iniciado por la Administración Obama, la revisión de los principios empleados por la FTC para la supervisión de las políticas de autorregulación de privacidad, así como algunos ejemplos de códigos de autoconducta.

Las señaladas disparidades entre las principales áreas socioeconómicas del planeta deben animar, más que desincentivar, esfuerzos conducentes a propiciar una creciente armonización con vistas a alcanzar una regulación de la privacidad y la protección de los datos efectiva y compartida. En esa línea, es interesante observar el impacto y las reacciones más significativas suscitadas por la reciente propuesta de Reglamento lanzada por la Comisión Europea, en orden a los factores más relevantes: a) utilización de modelos de «uso y obligación», que se basan en una mayor flexibilidad y adaptación de las obligaciones a los riesgos y tipos de uso de los datos personales; b) utilización más constante del «principio de responsabilidad», por el que se requiere al propietario y al responsable de los datos personales el cumplimiento de las medidas de protección establecidas; y c), uso de modelos adecuados de transparencia y consentimiento.

Impacto de la regulación de la privacidad en servicios *online*

No menos importante habrá de ser el objetivo de articular una puesta al día del marco protector que no actúe en contra del desarrollo y la innovación de los servicios *online*, sino que haga compatible la salvaguardia de los derechos y la puesta de nuevos, mejores y más eficaces servicios al alcance de la sociedad. Como más significativos se pueden citar: *cloud computing,* publicidad *online* basada en el comportamiento, redes sociales y ecosistema de aplicaciones móviles.

En el caso de los servicios *cloud computing*, la principal problemática se centra en la distribución de responsabilidades y obligaciones entre cliente y proveedor, ya que el establecimiento de obligaciones muy restrictivas a este último podría desincentivar su desarrollo, particularmente en Europa. En este sentido, respecto a la propuesta de Reglamento de la Comisión se plantea la necesidad de una regulación homogénea y amistosa para poder alcanzar economías de escala que impulsen la innovación y promuevan la adopción masiva de nuevas aplicaciones y servicios.

En relación con la publicidad *online*, las principales cuestiones de privacidad derivan de la utilización de tecnologías de monitorización del comportamiento –habitualmente *cookies* de rastreo– para la elaboración de perfiles de usuario. El principal conflicto se basa en la regulación del consentimiento y la validez de las iniciativas de autorregulación surgidas en

la propia industria. En este sentido, la mayor concienciación de los usuarios, una mayor transparencia y la puesta a disposición de herramientas que permitan hacer efectiva la capacidad de elección de los consumidores son elementos clave para abordar la problemática descrita. Las principales incógnitas reguladoras se encuentran en el ámbito de la Directiva sobre la privacidad y las comunicaciones electrónicas, mientras que la propuesta de Reglamento introduce incertidumbres sobre la utilización de perfiles basados en el tratamiento automático de los datos.

La privacidad en el entorno de las redes sociales supone un elemento singular, ya que es probable que su propia naturaleza –compartición de información personal en diferentes ámbitos o círculos de relación– entrañe una concepción diferenciada de la privacidad. Las principales problemáticas son la recogida, el almacenamiento y la visibilidad de los datos, la integración de terceros en las plataformas de red social y las situaciones en las que los propios usuarios son responsables de los datos de otros –*terceros*–. Por su parte, la propuesta de Reglamento incide directamente sobre la provisión de servicios de red social al establecer el derecho al olvido y la portabilidad de los datos, así como establece el principio de privacidad por defecto.

También el crecimiento y la evolución del mercado de aplicaciones móviles –*apps*– plantea un conjunto de problemáticas relacionadas con la privacidad, específicamente en relación con la transparencia y el control sobre la información recogida en las aplicaciones –como ejemplo, la geolocalización–, la monitorización de la actividad del terminal, o la utilización de datos capturados para la inserción de publicidad. La fase inicial en que se encuentra este ámbito y su continua evolución hacen difícil anticipar el impacto que tendrá la revisión del marco regulador europeo de protección de datos. Sin embargo, será clave para el desarrollo económico y la generación de empleo que permita a los agentes europeos competir en el mercado global. En este sentido, la utilización de códigos de autorregulación puede resultar beneficiosa para disminuir las amenazas a la privacidad sin generar merma competitiva en la industria europea.

Viviane Reding

Viviane Reding es vicepresidenta primera de la Comisión Europea y comisaria de Justicia, Derechos Fundamentales y Ciudadanía desde 2010. Reding tiene una gran trayectoria en las instituciones europeas, donde ha sido comisaria de Sociedad de la Información entre 2004 y 2010, y comisaria de Educación y Cultura de 1999 a 2004. Anteriormente, entre 1989 y 1999, fue diputada del Parlamento Europeo por el Partido Popular Social Cristiano, del que fue su vicepresidenta entre 1995 y 1999. Reding es, asimismo, doctora en Humanidades por la Universidad de la Sorbona de París y ha recibido numerosas distinciones públicas y académicas.

Protección de la privacidad en un mundo conectado. Un marco europeo de protección de datos para el siglo XXI

Viviane Reding
Vicepresidenta primera de la Comisión Europea
Comisaria de Justicia, Derechos Fundamentales y Ciudadanía

Desafíos a los que se enfrenta la protección de datos

La globalización y los cambios tecnológicos han transformado en gran medida las formas de recopilación, acceso, uso y transmisión de nuestros datos personales. Los nuevos sistemas utilizados para compartir información, tales como las redes sociales, la conectividad a Internet a través del móvil y el almacenamiento de grandes cantidades de datos recopilados en infraestructuras del llamado *cloud computing*, forman parte de la vida de muchos de los 250 millones de europeos que navegan por Internet. Al mismo tiempo, los datos personales se han convertido en un gran activo para muchas empresas. Para algunas, la recopilación, agrupación y análisis de los datos sobre posibles clientes ya es una parte importante de sus actividades económicas, mientras que otras buscan con avidez otras formas de obtener beneficios a raíz de los datos personales que sus clientes les han confiado.

En este nuevo entorno digital, las autoridades públicas tienen la obligación de garantizar que los individuos puedan ejercer un control efectivo sobre su propia información personal. Los individuos deben disfrutar de los derechos y de la posibilidad real de hacerlos valer. La protección de datos es un derecho fundamental en Europa, consagrado por el Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea así como por el Artículo 16(1) del Tratado de Funcionamiento de la Unión Europea (TFUE), y merece por tanto el amparo correspondiente. Pero no se trata únicamente de una obligación jurídica. La protección de datos es una necesidad económica, en especial en el entorno económico actual. La economía digital presenta un potencial inmenso de crecimiento, aunque solamente si participan en ella los ciudadanos y los consumidores. La falta de confianza hace que los consumidores se muestren reacios a la hora de comprar *online* y de aceptar y usar nuevos servicios. Para poder confiar en los servicios *online*, exprimir el potencial de la economía digital y fomentar la competitividad de la industria europea, resulta elemental disponer de un alto grado de protección de datos.

La Directiva europea de 1995, el instrumento legislativo central para la protección de datos personales en Europa, marcó un hito en la historia de la protección de datos. Esta Directiva tiene dos objetivos, por un lado garantizar el funcionamiento de un Mercado Único, y por el otro, la protección efectiva de los derechos y libertades fundamentales de los individuos. El convencimiento de que sus datos personales estarían protegidos en el extranjero fue una condición previa para que los ciudadanos aceptaran la circulación libre de datos en toda la UE y para que los Estados miembros distendieran las restricciones sobre la transmisión de datos entre unos y otros. Se armonizaron las normas sobre protección de datos y se establecieron los principios para la transmisión de datos personales fuera de la UE teniendo en cuenta las infraestructuras de telecomunicaciones existentes. Dentro del nuevo y complicado entorno digital actual, estas normas ya no ofrecen el nivel de armonización requerido ni son lo suficientemente eficientes como para garantizar el derecho a la protección de los datos personales. Y ese es el motivo por el cual la Comisión Europea ha propuesto una reforma fundamental del marco europeo sobre la protección de datos.

Hoy día necesitamos normas modernas y coherentes que se apliquen a toda la UE y que permitan la libre circulación de datos entre los Estados miembros. Las empresas necesitan disponer de normas claras y uniformes que proporcionen una seguridad jurídica y minimicen la carga administrativa. Todo esto resulta esencial si queremos que funcione el Mercado Único y que crezca la economía, se creen nuevos empleos y se fomente la innovación. La modernización de la normativa europea sobre protección de datos reforzará el mercado interno, garantizará el elevado grado de protección de los datos de cada individuo y estimulará la seguridad, la claridad y la coherencia legales. La nueva normativa en materia de protección de datos desempeña, por tanto, un papel esencial en la estrategia de crecimiento de la UE.

La Comisión Europea ha entablado extensos debates con ciudadanos y empresas. La mayoría se inclinaba por que la Comisión Europea reformara la normativa sobre protección de datos. La Comisión analizó el posible impacto de las distintas opciones de políticas y decidió finalmente proponer un nuevo marco integral sobre protección de datos. Los nuevos instrumentos para la protección de datos se adoptarán dentro del marco del Tratado de Lisboa. Un Reglamento general sustituirá a la Directiva 95/46/CE en vigor y establecerá un nuevo marco europeo general sobre protección de datos que se aplicará al sector privado; asimismo, una nueva Directiva sustituirá la Decisión Marco 2008/977/JAI que contiene las normas de protección de datos actuales de aplicación al tratamiento de datos destinado a la prevención, detección, investigación o enjuiciamiento de delitos penales y las actividades judiciales relacionadas.

Otorgar a los individuos el control sobre sus propios datos personales

A partir de la Directiva 95/46/CE sobre protección de datos en vigor, se han desarrollado diferentes variaciones importantes en cuanto a la forma en que los individuos pueden ejercer su derecho a la protección de datos en los distintos Estados miembros. Lo mismo se aplica a las facultades de las autoridades nacionales responsables de la protección de datos. Como resultado de esta diversidad, les resulta mucho más difícil a los individuos de unos Estados que a los de otros poder ejercer sus derechos en materia de protección de datos.

A menudo, los usuarios no son completamente conscientes de que se están recopilando sus datos. Aunque muchos europeos consideran que la divulgación de datos personales forma una parte cada vez mayor de la vida

moderna, al 72 % de los usuarios de Internet en Europa todavía les preocupa que se les soliciten demasiados datos personales *online*. Creen que no controlan sus propios datos. No se les informa debidamente sobre lo que ocurre con su información personal, a quién se transmite y para qué fin. A menudo no saben cómo ejercer sus derechos *online*.

La reforma se ocupará de este problema consiguiendo que los derechos de los individuos sean más comprensibles y fáciles de ejercer. La Directiva actual garantiza, en principio, que los individuos puedan solicitar la eliminación de sus datos y que estos no sean procesados durante más tiempo del necesario para los objetivos legítimos para los que se requirieran. Para poder superar las dificultades a la hora de ejercer estos derechos, la nueva propuesta expresa los derechos de los individuos de manera más clara y mediante el membrete del «derecho al olvido».

La nueva legislación puede ilustrarse mediante muchos ejemplos concretos. Uno de ellos es el caso de un estudiante, miembro europeo de una red social *online*, que decide solicitar el acceso a todos los datos personales que la Red disponga de él y descubre que Internet recaba muchos más datos de los que él era consciente y que los datos cuya eliminación había solicitado todavía estaban almacenados.

La reforma de la normativa europea sobre protección de datos garantiza que esto no vuelva a ocurrir al introducir:

- un requisito explícito que obliga a las redes sociales *online* (y otros responsables del tratamiento de los datos, también conocidos como controladores de los datos) a minimizar el volumen de datos personales de los usuarios que recaben y procesen;
- la exigencia de que los parámetros por defecto garanticen que los datos no se hagan públicos;
- la obligación explícita de que los responsables del tratamiento eliminen los datos personales de un individuo si esa persona solicita expresamente la eliminación y cuando no exista motivo legítimo alguno para retenerlos.

Si el caso ejemplificado se hubiera tratado según la legislación nueva, el proveedor de la red social estaría obligado a eliminar los datos del estudiante de manera inmediata e íntegra.

Otro ejemplo de los problemas relativos a la forma en que se interpreta la normativa actual concierne a la implantación de las medidas de seguridad. Aunque las normas ya exigen claramente que los responsables del tratamiento de los datos garanticen la máxima seguridad técnica posible para dicho tratamiento, según sus condiciones económicas, los ciudadanos todavía siguen enfrentándose a casos notorios de infracciones en materia de seguridad por las que se pierden, roban o piratean enormes cantidades de datos personales. A menudo estas violaciones de datos revelan defectos en el sistema de seguridad del responsable en concreto, así como respuestas inadecuadas a los incidentes.

Ejemplos recientes incluyen un caso en que unos piratas informáticos atacaron un servicio de juego *online* que incluía a usuarios europeos. Los delincuentes consiguieron acceder a las bases de datos que contenían datos personales (incluyendo los nombres, direcciones y posiblemente datos de las tarjetas de crédito) de decenas de millones de usuarios del mundo entero. La empresa esperó una semana para notificar este hecho a los usuarios afectados.

La reforma de la normativa europea sobre protección de datos garantiza que esto no vuelva a ocurrir. Las nuevas normas obligarán a las empresas a:

- reforzar sus medidas de seguridad para prevenir posibles violaciones de los datos personales;

- comunicar la existencia de una violación de los datos personales a la autoridad nacional de protección de datos y a los individuos afectados sin demora injustificada (lo cual suele ser en un plazo de 24 horas) en cuanto se detecte la filtración.

El objetivo de la Comisión Europea consiste en reforzar los derechos, en aportar a las personas medios eficientes y operativos destinados a garantizar que se les mantenga completamente informadas sobre lo que ocurre con sus datos personales y en permitirles que ejerzan sus derechos con mayor efectividad.

La nueva normativa propuesta por la Comisión Europea protegerá a los individuos de manera más efectiva en lo que al tratamiento de sus datos personales se refiere.

La nueva normativa mejorará la capacidad de los individuos de controlar sus datos al:

- garantizar que, si se requiere el consentimiento, este se conceda de manera explícita, es decir, que se otorgue mediante declaración o mediante acción afirmativa por parte de la persona en cuestión, y que se conceda libremente;
- proveer a los usuarios de Internet de un derecho efectivo a ser olvidados en la Red; conceder el derecho a que se eliminen los datos si retiran dicho consentimiento y si no existen motivos legítimos para retener dichos datos;
- garantizar un acceso fácil a los datos propios y el derecho a la portabilidad de los datos; conceder el derecho a obtener una copia de los datos almacenados por el responsable del tratamiento y la libertad de desplazarlos de un proveedor de servicios a otro, sin obstáculos;
- reforzar el derecho a la información de manera que los individuos comprendan por completo cómo se manipulan sus datos personales, en especial cuando las actividades de tratamiento afecten a menores;
- mejorar los medios de que disponen los individuos para ejercer sus derechos mediante:
  – el refuerzo de la independencia y los poderes de las autoridades nacionales de protección de datos, con el fin de equiparlas adecuadamente para poder resolver las quejas de manera efectiva y dotarlas de las facultades para realizar investigaciones efectivas, tomar decisiones vinculantes e imponer sanciones efectivas y disuasivas;
  – el incremento de los recursos administrativos y judiciales correspondientes cuando se infrinjan los derechos de la protección de datos. En particular, las asociaciones cualificadas podrán emprender medidas legales en nombre del individuo.

Se reforzará la seguridad de los datos al:

- fomentar el uso de tecnologías impulsoras de la privacidad (tecnologías que protejan la privacidad de la información al minimizar el almacenamiento de datos personales), de parámetros por defecto que fomenten la privacidad y de programas de certificación de la privacidad;
- introducir una obligación general por la que los responsables del tratamiento de los datos deban notificar cualquier violación de estos tanto a los individuos perjudicados como a las autoridades de protección de datos sin demora injustificada (que suele ser, por norma, en un plazo de 24 horas).
- aumentar la responsabilidad de quienes procesen los datos, en concreto:
  – exigiendo a los responsables del tratamiento de los datos que designen a un encargado de protección de datos en empresas con más de 250 empleados y en las que lleven a cabo procesamientos arriesgados;
  – introduciendo el principio de la «privacidad desde el diseño» con el fin de garantizar que las medidas de protec-

ción de los datos se incluyen desde la etapa de planificación de sus procedimientos y sistemas; y
– creando la obligación de efectuar «Evaluación de Impacto sobre Protección de Datos» para las organizaciones que realicen procesamientos arriesgados.

Normativa sobre protección de datos adecuada al Mercado Único Digital

A pesar del objetivo de la Directiva actual por garantizar un nivel equivalente de protección de datos en la UE, todavía existe una divergencia considerable entre las normativas de los Estados miembros. En consecuencia, los responsables del tratamiento podrían tener que acatar veintisiete leyes y reglamentos nacionales distintos. El resultado es un entorno legal fragmentado que ha dado lugar a una incertidumbre jurídica y una protección desigual de los individuos. Todo ello ha acarreado gastos innecesarios y sobrecargas administrativas a las empresas, y constituye una traba para aquellas organizaciones que operan en el Mercado Único y que pudieran querer expandir sus operaciones más allá de sus fronteras.

Los recursos y las facultades de las distintas autoridades nacionales de protección de datos varían considerablemente de un Estado miembro a otro. En algunos casos, no son capaces de cumplir con sus tareas ejecutorias de manera apropiada. La cooperación entre estas autoridades a nivel europeo (a través del Grupo Asesor, denominado «Grupo de Trabajo» del Artículo 29) no siempre conduce a un cumplimiento sistemático y, por tanto, también debe mejorarse.

Dado que los servicios de redes pueden prestarse a nivel global desde una única plataforma, las diferencias entre las aplicaciones prácticas de las normas sobre protección de datos provocan unas divergencias que no tienen sentido, ni para los individuos ni para las empresas afectadas. Algunos casos recientes ejemplifican el resultado.

Una empresa multinacional con distintos establecimientos en la UE ha instaurado un sistema virtual de cartografía que recaba imágenes por toda Europa de edificios públicos y privados y que también puede hacer fotografías de personas en la calle. En uno de los Estados miembros, la inclusión de fotografías sin desenfocar de personas que no eran conscientes de que se les estaba fotografiando se consideró ilegal, mientras que en otro de los Estados miembros esta práctica no se consideró una infracción de la legislación sobre protección de datos. Por consiguiente, las autoridades de protección de datos no dieron una respuesta coherente para poner remedio a esta situación.

La reforma de la normativa europea sobre protección de datos garantizará que esto no vuelva a ocurrir en el futuro, puesto que:

- se establecerán los requisitos y garantías de preservación de la protección de datos mediante un Reglamento europeo que ejercerá un efecto directo sobre toda la Unión;
- tan solo la autoridad de protección de datos donde la sociedad cuente con su sede será la responsable de decidir si la sociedad obra de manera legítima;
- la coordinación inmediata y efectiva entre las autoridades de protección de datos nacionales (dado que el servicio está dirigido a los individuos de varios Estados miembros) ayudará a garantizar que la nueva normativa europea sobre protección de datos se aplique y cumpla de manera sistemática en todos los Estados miembros.

Las autoridades nacionales deben reforzarse y cooperar más para poder garantizar un cumplimiento sistemático y, en última instancia, una aplicación uniforme de la normativa en toda la UE.

Un marco legislativo sólido, claro y uniforme a nivel europeo contribuirá a impulsar el

potencial del Mercado Único Digital y promoverá el crecimiento económico, la innovación y la creación de empleo. El Reglamento acabará con la fragmentación de los ordenamientos legales de los veintisiete Estados miembros y derribará las barreras de acceso al mercado, un factor de especial importancia para las pequeñas y medianas empresas.

Las nuevas normas aportarán, además, a las empresas europeas una ventaja de cara a la competencia global. Según el marco regulador reformado, podrán asegurar a sus clientes que su valiosa información personal será tratada con el debido cuidado y diligencia. La confianza en un régimen regulador europeo coherente será un activo clave para los proveedores de servicios y un incentivo para los inversores a la hora de seleccionar la localización geográfica de sus servicios.

La nueva normativa ampliará la dimensión del Mercado Único en materia de protección de datos. Irá destinada a:

- establecer las normas sobre protección de datos a nivel europeo mediante un reglamento que entrará en vigor en todos los Estados miembros y que pondrá fin a la aplicación acumulativa y simultánea de las distintas leyes nacionales sobre protección de datos. Esta armonización, por sí misma, ayudará a las empresas a ahorrar unos 2.300 millones de euros al año en términos de carga administrativa;
- simplificar el entorno regulador al anular formalidades tales como los requisitos generales de notificación, lo cual contribuirá también al ahorro;
- reforzar todavía más la independencia y los poderes de las autoridades nacionales de protección de datos (APD) y obligar a los Estados miembros a equiparlas con los recursos necesarios para efectuar investigaciones, tomar decisiones vinculantes e imponer sanciones efectivas y disuasivas;
- instaurar un sistema de «ventanilla única» para la protección de datos en la UE que garantizará que los responsables de datos europeos solo tengan que tratar con una única APD, es decir, con la del Estado miembro donde esté situada su sede, eliminando cualquier problema burocrático;
- crear las condiciones de una colaboración rápida y eficiente entre las APD, incluyendo la obligación de que una APD inicie investigaciones e inspecciones si así se lo solicitara otra de ellas, y de reconocimiento mutuo de las decisiones, convirtiendo a cada APD en responsable último y representante máximo del cumplimiento de la legislación europea sobre protección de datos;
- instalar un mecanismo de coherencia a nivel europeo que garantice que las decisiones de las APD que ejerzan un impacto mayor en la UE tengan en cuenta el resto de las opiniones de otras APD implicadas y que cumplan por completo con la legislación europea;
- convertir al Grupo de Trabajo del Artículo 29 en un Consejo Europeo de Protección de Datos con el fin de mejorar su contribución a la aplicación sistemática de las leyes sobre protección de datos y de ofrecer una base sólida de cooperación entre las autoridades de protección de datos, incluyendo al supervisor europeo de Protección de Datos, lo cual fomentará las sinergias y la efectividad.

El nuevo Reglamento de la UE garantizará una protección firme de los datos personales en toda la UE y reforzará el funcionamiento del Mercado Único. Al mismo tiempo, asegurará que otros derechos fundamentales tales como la libertad de expresión y de información y el derecho a la defensa, así como el derecho a guardar secreto profesional (como en el caso de los abogados) sean respetados. La nueva normativa no afectará a la situación de las iglesias según la legislación de los Estados miembros.

Uso de los datos en cooperaciones policiales y de la justicia penal

La entrada en vigor del Tratado de Lisboa y en particular la introducción de una nueva base legal permitirá un marco de protección de datos integral que garantice tanto un elevado grado de protección de los datos personales en el campo policial como la colaboración judicial en materia penal. Todo ello conducirá, además, a un intercambio más fluido de la información entre las autoridades policiales y judiciales de los Estados miembros, mejorando la cooperación en la lucha contra los delitos graves en Europa.

El nuevo marco de protección de datos cubrirá, además, situaciones donde los datos del sector privado sean solicitados y procesados por las fuerzas y cuerpos de seguridad.

El tratamiento de los datos por parte de las autoridades policiales y judiciales en materia penal está contemplado en la actualidad por la Decisión Marco 2008/977/JAI, que precede a la entrada en vigor del Tratado de Lisboa. La Comisión no dispone de la facultad para aplicar sus normas, pues se trata de una Decisión Marco, y ello ha contribuido a una implementación muy desigual. Además, el ámbito de esta Decisión Marco queda limitado a las actividades transfronterizas de tratamiento. Esto significa que el tratamiento de los datos personales dentro de los Estados miembros no está cubierto en la actualidad por la normativa europea que rige dicho tratamiento y que protege el derecho fundamental a la protección de los datos. De esta forma se ha dado lugar a que las autoridades policiales, entre otras, se enfrenten a una dificultad práctica, pues puede no resultarles obvio si dicho tratamiento es meramente nacional o transfronterizo, y tampoco pueden prever si los datos «nacionales» podrían ser objeto de un posterior intercambio transfronterizo.

El Artículo 16 del TFUE proporciona la base jurídica en materia de tratamiento transfronterizo y nacional de datos personales. Una aplicación sistemática ayudaría además a hacer frente a las distintas «normas de origen» nacionales y otros estándares variables que afectan tanto al nivel de protección de los datos personales como a la eficiencia de la colaboración entre las fuerzas y cuerpos de seguridad.

El nuevo marco de protección de datos europeo está destinado, pues, a garantizar una protección de los datos sistemática y de alto nivel que mejore la confianza mutua entre las autoridades policiales y judiciales de los distintos Estados miembros, facilitando así la circulación libre de datos y la colaboración entre las autoridades policiales y judiciales.

Establecimiento de normas globales para la protección de datos

Muchas transacciones comerciales implican la transmisión de datos personales, y las empresas europeas han de beneficiarse de las oportunidades globales. Por ello es importante establecer las condiciones adecuadas de transmisión de datos personales desde la UE a otros países. Los derechos de los individuos deben seguir garantizándose al transferir sus datos personales. Lo mismo se aplica a los servicios prestados desde el exterior de la UE que están dirigidos a individuos dentro de los Estados miembros y que usan o analizan sus datos. Para poder tratar estos casos de manera adecuada, las normas europeas sobre protección de datos deben aplicarse independientemente de la ubicación geográfica de la empresa o de sus instalaciones de tratamiento.

En el mundo globalizado actual, los datos personales se transfieren a través de una cantidad cada vez mayor de fronteras virtuales y geográficas y se almacenan en servidores de múltiples países. Cada vez son más las empresas que ofrecen servicios de *cloud computing*,

que permiten a sus clientes acceder y almacenar sus datos en servidores remotos. Estos factores exigen que se mejore el mecanismo actual de transmisión de datos a países extracomunitarios. En éste se incluyen las decisiones sobre adecuación (es decir, las decisiones que certifiquen unas normas sobre protección de datos «adecuadas» en los países extracomunitarios) y los mecanismos de protección idóneos, tales como cláusulas contractuales estándares o «normas empresariales vinculantes», destinados a garantizar el alto grado de protección de datos en las operaciones internacionales de tratamiento y a facilitar la circulación de los datos más allá de las fronteras.

La reforma europea sobre protección de datos simplificará y estratificará el proceso de reconocimiento de las normas empresariales vinculantes, pues serán validadas únicamente por una Autoridad de Protección de Datos, y se contará con los mecanismos que aseguren una rápida implicación de otras Autoridades de Protección de Datos, de ser necesaria. Una vez que una autoridad haya aprobado un conjunto de normas vinculantes, se aplicará a toda la UE sin necesidad de otra autorización adicional a nivel nacional.

La reforma sobre protección de datos se ocupará de los retos de la globalización mediante herramientas y mecanismos flexibles que faciliten la operación de las empresas que trabajen a nivel mundial, garantizando al mismo tiempo la protección de los datos personales y sin dar cabida a lagunas jurídicas. Todo ello se conseguirá gracias a las siguientes medidas:

- normas claras que definan cuándo se aplica la legislación europea a los responsables de los tratamientos con sede en países externos, en concreto que especifiquen que siempre que las actividades de tratamiento estén dirigidas a ciudadanos de la UE se aplicarán las normas europeas;
- normas y procedimientos más claros para las decisiones sobre adecuación que tome la Comisión Europea bajándose en criterios explícitos y transparentes;
- se facilitará la circulación legítima de datos a países externos. La reforma de la protección de datos reforzará y simplificará las normas sobre transmisiones internacionales de datos a países no cubiertos por la decisión de adecuación. Se mejorará la eficacia del uso de las normas empresariales vinculantes y se ampliará de forma que se aplique a grupos de empresas. De este modo se ayudará a las cada vez más numerosas empresas que se ocupan de actividades de tratamiento, especialmente en la llamada *cloud computing*;
- se entablarán diálogos y, de ser necesario, negociaciones con países externos, especialmente con los socios estratégicos de la UE (y otras organizaciones de relevancia internacional tales como el Consejo Europeo, la Organización para la Cooperación y el Desarrollo Económico, las Naciones Unidas), con el fin de promover las estrictas normas de protección de datos y su interoperabilidad a nivel mundial.

Conclusión

La reforma sobre protección de datos de la UE creará un marco moderno, sólido e integral para la protección de los datos en la Unión Europea. El derecho fundamental de cada individuo a la protección de sus datos personales será mucho más efectivo y fácil de ejercer. Gracias a ello, se reforzarán otros derechos fundamentales que dependen a menudo de la privacidad y la confidencialidad, tales como la libertad de expresión e información, el derecho de reunión y el derecho a la defensa o al secreto profesional, por citar solo unos pocos.

Los individuos podrán beneficiarse de unos derechos en materia de protección de datos más sólidos, incrementando así su confianza en el entorno digital. La reforma simplificará de manera considerable el entorno legal de las empresas y del sector público. Asimismo, se estimulará el desarrollo de la economía digital en el Mercado Único europeo y fuera del mismo, en consonancia con los objetivos de la estrategia Europa 2020 y la Agenda Digital para Europa. Y lo que es más, la reforma fomentará la confianza entre las autoridades del orden público y facilitará los intercambios de datos entre las mismas.

La Comisión Europea podrá centrarse en colaborar estrechamente con el Parlamento Europeo y el Consejo para poder garantizar un proceso legislativo ágil y un acuerdo rápido en cuanto al nuevo marco europeo sobre protección de datos. A lo largo de este proceso de adopción y después del mismo, especialmente en el contexto de la implantación de nuevos instrumentos jurídicos, la Comisión seguirá manteniendo un diálogo constante y transparente con todas las partes interesadas.

En el entorno actual de constante desarrollo de las tecnologías de la información y de unas conductas sociales en evolución, dicho diálogo es de esencial importancia. Tan solo si nos comunicamos los unos con los otros podremos garantizar el alto grado de protección de los datos personales, la efectividad operativa del sector público (incluyendo la policía y el poder judicial), una carga administrativa mínima y, por último aunque no menos importante, el crecimiento y la competitividad de las industrias europeas.

Enrique Badía

Enrique Badía ejerce actualmente como consultor independiente, tras una dilatada trayectoria empresarial y periodística. Ha sido director general del regulador español de las telecomunicaciones (CMT), directivo de compañías como Airtel (Vodafone España), Acesa (Abertis) e Iberia, y medios como *El País*, *Cambio 16*, *Diario 16* y *Cinco Días.* Colaborador y analista económico en distintas publicaciones, es autor de *Rumasa* (Planeta, 1983) y *Zara y sus hermanas* (Lid, 2008).

1. Marco conceptual. Derecho ¿pendiente?

Enrique Badía
Consultor independiente

1.1 Introducción

Todo individuo alberga su propia concepción de privacidad. Dista de ser unívoca y por tanto compartida: antes bien, es distinta, privativa, personal..., al punto de formar parte de su propia parcela de intimidad. Es así a nivel de cada uno, pero también cuando se trata de aglutinar elementos comunes o compartidos en un colectivo aunado por factores de pertenencia, sean de índole cultural, territorial o simplemente grupal. Tampoco la concepción y, todavía menos, la *sensibilidad* o el deseo de preservación han sido estables a lo largo del tiempo, analizados grupo a grupo o, más extensamente, país a país.

Sí se ha mantenido, en cambio, la idea de que existe un derecho personal e inviolable a preservar aquellos aspectos de uno mismo considerados *privados*, es decir, protegidos por el deseo o la voluntad de mantenerlos al abrigo de todo o parte del entorno con capacidad de acceder a conocerlos. Por decirlo de otra manera: toda persona ostenta la potestad de *gestionar* aquellas partes de sí mismo y su comportamiento que libremente elija preservar.

A lo largo del tiempo, la protección efectiva de ese derecho ha migrado desde la acción individual a la incorporación de distintos grados y formas de tutela a cargo de los poderes públicos; esto es, los Estados y sus mecanismos de intervención. El tránsito, sin embargo, no ha sido paralelo ni constante, sino que ha discurrido jalonado de avances y retrocesos, en buena medida interferidos o condicionados por el impacto tecnológico y su incidencia en las formas de interrelación social.

Un primer episodio, en cierta medida paradójico, se produjo al designar al Estado responsable de proteger el derecho a la intimidad y al mismo tiempo potencial –a menudo efectivo– invasor y, por tanto, vulnerador de ese mismo derecho. Se puede considerar que en torno a ello surgió una primera contraposición relevante entre derechos considerados como esenciales: el señalado respecto a la intimidad personal y el atribuido al Estado como garante de la seguridad colectiva.

Sin retroceder demasiado en la historia, otro hito importante fue la implantación masiva de los medios de comunicación. La difusión –consumo– de periódicos, revistas, emisoras de radio y cadenas de televisión supuso un cambio sustancial que, entre otras cosas, trajo consigo una nueva contraposición, sería mejor decir colisión, a menudo frontal, con otro derecho tenido también por *fundamental*: información, en su doble vertiente de in-

formar (medio) y ser informado (sociedad). Algo que provocó, entre otras cosas, adherir al ya más o menos establecido derecho a la intimidad aspectos como la propia imagen o un históricamente *recuperado* honor personal. Ni la doctrina ni la jurisprudencia han acabado de acotar los límites entre ambos, dando lugar a una sucesión de controversias y contenciosos que sigue sin resolverse de una forma clara y determinante, tanto desde el lado de los medios en su desempeño profesional como de parte de la sociedad que reclama *protección* frente a cualquier *invasión.*

Ningún antecedente es comparable a lo que comporta la eclosión de Internet y el modo como facilita la consolidación de la globalidad. Cabe decir que la Red está obligando a definir nuevos límites y contornos que, al tiempo que abordan y garantizan el derecho a la privacidad, deben permitir el lanzamiento y la continuidad de los nuevos servicios digitales. Esto conlleva que, en cierta medida a su abrigo, hayan surgido nuevos modelos de negocio y se hayan desarrollado otros no tan nuevos que tienen en la posesión y manejo de datos personales todo o parte de su razón de ser. Han surgido, entre otros, renovadas formas de marketing[1]: personalizado, viral y, en algunas ocasiones, *no solicitado* que, sin ser siempre ni del todo nuevas, han adquirido dimensiones conducentes a reflexionar sobre nuevos modos de afrontar la privacidad.

Nunca resulta fácil determinar en qué medida la tecnología avanza y condiciona la práctica de sus usuarios o, en sentido inverso, los avances se producen como respuesta a las demandas y requerimientos de quienes se sirven de ella en su desempeño personal o profesional. Lo más probable es que la dinámica derive de una mezcla de ambas interpretaciones y acaso alguna más. Prueba de ello es que no todos los avances se comercializan ni los que se ponen a disposición del mercado acaban teniendo suficiente aceptación. Existe, en todo caso, un claro proceso de interacción.

Muchos son, por descontado, los *saltos* que la tecnología ha propiciado en las dos o tres últimas décadas. Pero, a los efectos que nos ocupan, es obligado circunscribir la cita a al menos tres: digitalización, movilidad e interactividad. No es momento ni espacio para desbrozar lo que cada uno de esos factores, unidos a muchos otros, ha contribuido al *estado de la cuestión* –privacidad–, pero cabe citarlos por su aportación al desarrollo de nuevos mercados y fórmulas que tratan de satisfacer la demanda de servicios innovadores de los usuarios. En el ámbito de la privacidad, estos servicios exigen redefinir parámetros, conceptos y mecanismos que preserven garantías del derecho fundamental a la privacidad, sin dificultar su lanzamiento e implantación.

Contraponiendo el presente al pasado más o menos reciente, quizá el cambio más relevante radique en que la capacidad de gestionar los propios datos se ha tornado en gran medida tarea más difícil, desde el punto y hora en que la mayoría de las personas ignora cuál va a ser el manejo de los datos que vierte en la Red por terceros agentes que intervienen en el mundo Internet. A título de ejemplo de las dudas que se plantean: ¿quién y qué está haciendo el *capturador* con sus datos personales? Y, lo que es tanto o más importante, ¿cómo, dónde y ante quién puede requerir de modo efectivo –asequible y eficiente– la protección que desea preservar?

Las previsiones coincidentes de la prospectiva sitúan en la actual y próximas décadas una multiplicación de realidades ya presentes como marketing viral, publicidad personalizada, servicios de geolocalización, *cloud compu-*

1. Aunque la Real Academia de la Lengua Española (RAE) recomienda el uso del vocablo «mercadotecnia», se mantendrá el habitual («marketing») dada su general comprensión.

ting, *streaming*, redes sociales... sin que ello deba conducir a considerar que el nuevo escenario ha alcanzado ningún tipo de cénit: antes al contrario, existe cierto consenso en que el camino no ha hecho más que empezar. Huelga decir que en todas ellas desempeñan un papel notable la posesión y el manejo de datos personales y, por ende, la privacidad.

Frente a ese cúmulo de realidades no sería oportuno ceder a la tentación frecuente de concluir que solo cabe resignarse y asumir mayores o menores grados de pérdida o erosión de la privacidad como una especie de *precio* irremediable. Por el contrario, hay que utilizar los recursos, herramientas y posibilidades que ofrece el propio estado de la tecnología, orientándolos y poniéndolos al servicio de una mejor y más efectiva salvaguardia de lo íntimo y personal, sin tener que renunciar a ninguna de las facilidades que proporciona la innovación y muy en particular Internet.

De ahí que sea tiempo –oportunidad– de promover un replanteamiento actualizado del marco garantista de la privacidad. Aunque no de cualquier forma. Por citar solo los aspectos más cruciales, deberá ser lo suficientemente equilibrado entre la protección efectiva y la prudencia precisa para evitar que un exceso normativo evite o incluso yugule el desarrollo de nuevos servicios, herramientas y aplicaciones –negocios– asociados al mundo digital en progresiva eclosión. Expresado gráficamente: proteger la intimidad no tiene ni debe por qué comportar nada parecido al estancamiento o la defunción del desarrollo de Internet.

La perseguida y deseable eficacia no será tal a menos que se alumbren e implementen normas con plena conciencia de que abordan un fenómeno globalizado. No han de valer, por tanto, enfoques de índole básicamente estatal o territorializado. No servirían –no sirven– desde la constatación palmaria de que muy a menudo no coinciden los ámbitos territoriales respectivos del cliente de un servicio y su prestador. Como tampoco se puede ignorar que un distinto enfoque regulador puede desembocar en desventaja competitiva de una parte de la industria, por el mero hecho de estar radicada en un territorio, frente a agentes ubicados en otra demarcación normativa.

Esa última particularidad, desventaja a fin de cuentas, se está ya manifestando en al menos dos supuestos para las empresas europeas. Por una parte, la falta de armonización en la aplicación práctica de la normativa europea de privacidad en cada uno de los veintisiete Estados miembros, con lo que conlleva de desventaja para los agentes económicos cuya actividad abarca distintos mercados comunitarios. Otro supuesto deriva de las limitaciones competitivas que deben afrontar respecto de prestadores radicados fuera del perímetro de la UE[2], por tanto, no sujetos a la normativa europea en materia de privacidad y protección de datos personales.

Y corresponde citar, en último término, otro tipo de asimetría: la dispar presión reguladora sobre distintos agentes concurrentes en el mismo mercado. Es el caso, en concreto, de unas operadoras de telecomunicaciones *intensamente* sometidas a obligaciones, y otros que, pese a prestar servicios similares o conexos, actúan del todo librados de someterse a tutela reguladora alguna.

1.2 Algo de historia

La «privacidad» dista de ser un concepto compartido a escala universal. Ni siquiera ha sido constante a lo largo del tiempo, en ningún lugar ni ámbito cultural. Probablemente por eso, su consideración jurídico-normativa ha ido evolucionando y lo ha hecho de forma dispersa, al punto que ahora

2. Las diferencias y particularidades de los respectivos marcos reguladores se tratan extensa y detalladamente en el capítulo 2.

mismo no se puede considerar que exista una visión compartida, sin ir más lejos a una y otra orilla del Atlántico. De todo ello también deriva la persistente dificultad de reglamentar y tutelar su protección. Y es que, por más que sea difícil de acotar, la intimidad personal –una acepción bastante extendida– se ha tendido a considerar *bien* susceptible de ser protegido, aunque con limitaciones decididas desde una mezcla de intereses políticos y sociales.

Huelga decir que el derecho a la salvaguardia personal, en sus distintas formas, solo ha emergido en contextos avanzados de organización social. En buena medida, su consideración ha discurrido asociada al reconocimiento y la protección, en realidad la primacía de la libertad individual. Otras formas de organización social –en esencia, política– la excluyen en sí misma o, cuando es el caso, la consideran excepción de una forma tan amplia que acaban por subvertirla hasta un punto en que deja de existir en realidad.

Yendo a lo concreto, cualquiera de las acepciones de privacidad surge asociada a la emergencia del Estado moderno, tras un dilatado devenir histórico de permanecer ignorada en las sucesivas etapas de absolutismo, feudalismo y demás formas de control social. Se trata, pues, de un *bien* históricamente reciente, excluido en todos y cada uno de los sucesivos sistemas autoritarios, dictatoriales o cercenadores de las libertades que se han ido sucediendo... hasta hoy.

Pero no solo el contexto político o la cultura sociales han determinado cuál ha sido la evolución del concepto: el ingrediente tecnológico ha desempeñado y sobre todo está desempeñando un papel primordial; y lo hará todavía más. Es en función de ello que está empezando a germinar un intenso debate sobre cómo acotar debidamente la preservación del derecho –privacidad, intimidad o como se elija llamarlo– sin perjudicar ni limitar el potencial que los avances tecnológicos mantienen para contribuir al desarrollo económico y social. Debate nada fácil desde la constatación de que la línea divisoria es, o suele ser, extremadamente delgada.

De siempre, la controversia se ha centrado en el papel del Estado: por una parte, a los poderes públicos les debe corresponder la protección de los derechos individuales; por otra, es frecuente que en nombre de esa misma protección se planteen formas de intrusión *legalizada*, dotando a las administraciones de facultades para invadir la intimidad. El equilibrio no es fácil y en estos tiempos discurre, además, complicado por el imperativo de la globalidad, que añade al poder público la responsabilidad de aunar y equilibrar dos tipos de protección: privacidad y estímulo –al menos no desincentivo– al desarrollo económico y la innovación.

Como anticipo de un tratamiento más extendido[3], cabe apuntar tres hechos –reales– de importancia sustancial. Uno es la progresiva implantación de modelos de negocio cuasi estrictamente centrados en el uso y la explotación de datos susceptibles de ser considerados *privativos* de cada sujeto. Otro se refiere a que son varias las formas en las que un individuo está suministrando información personal, por el simple hecho de servirse de las facilidades, herramientas y servicios asociados a Internet. Y, para acabar de complicarlo, es cada vez más frecuente que el ámbito privado que se pretende proteger y el potencial subvertidor de esa protección se encuentren en ámbitos geográficos, y normativos, distintos o, dicho de otra forma, que los organismos legitimados para proteger tales derechos carezcan de potestad jurisdiccional allí donde se almacena, gestiona y, en último término, comercializa el uso de los datos acumulados.

3. La casuística y descripción de los nuevos negocios se aborda en el Capítulo 3.

1.2.1 Concepto vago

Valga en lo que valga la óptica estrictamente semántica del término, la Real Academia de la Lengua Española (RAE) define «privacidad»: «Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión». No acoge, curiosamente, la esencia que fundamenta el vocablo inglés *privacy*, del que a todas luces deriva, dado que este descansa en gran medida sobre el concepto intimidad, a su vez definido por la RAE: «Zona espiritual íntima y reservada de una persona o un grupo, especialmente una familia». Y, retrotrayendo un poco más el recorrido semántico del término, cabe acudir al latino *privatus*, referido al mantenimiento de algo separado del resto, a resguardo de la visión, el conocimiento o la influencia externos.

Desbrozar la raíz de los distintos significados e interpretaciones, acogidos a cada momento, circunstancia y tradición histórico-culturales, excedería con mucho las pretensiones de espacio y dimensión de este libro, pero vale la pena significarlo como precursor de las dificultades que aún hoy se oponen a la, por otra parte cada vez más necesaria, casi se podría decir ineludible, armonización del concepto mismo y su protección, en una realidad que puede y debe ser rotulada tanto deslocalizada como irreversiblemente global.

Un camino que desbrozar puede partir de la evidencia de que buena parte de las significadas disparidades son más de matiz que de concepto mismo, al punto de permitir establecer un probable consenso compartido que subyace en todas ellas: el reconocimiento del derecho de cada quien a marcar los límites de lo que desea sea conocido de sí mismo, lo que no y, en todo caso, su potestad indelegable de decidir quién o quiénes pueden compartir ese conocimiento y para qué.

Es cierto que la intimidad suele ser confundida, cuando no asimilada, a la voluntad o el deseo de mantener el anonimato, permaneciendo total o parcialmente desconocido, inadvertido o no identificado por el gran público y, en la mayoría de los casos, por los diferentes estamentos del poder; sea este estatal o de otra índole, por ejemplo empresarial. Anonimato que, por extensión, se entiende comprensivo de datos, usos, costumbres, hábitos y prácticas de carácter personal. En el entendido de que el derecho individual a preservarlos niega el de otros para acceder a su conocimiento –y uso– sin mediar la voluntad –consentimiento– de su titular.

1.2.2 Factor cultural y tradición

Existen pocas dudas de que la globalidad impone alguna forma de armonización. Ya se ha señalado la persistente tendencia a que usuarios y prestadores de servicios radiquen en ámbitos diferenciados y, en consecuencia, estén teóricamente sujetos a marcos normativos diversos, de tal forma que el titular de la privacidad protegible ignore, total o parcialmente, la legislación a la que está sujeto el prestador del servicio o intermediador que está capturando sus datos.

No cabe ignorar, sin embargo, que la armonización, en realidad unificación de criterios y reglas, no será fácil. La disparidad normativa preexistente, de la que dará cumplida referencia la segunda parte de este libro, constituye un obstáculo que se debe tener en cuenta, tras el que subyacen, como es imaginable, un sustrato cultural y un acervo de tradiciones que están justamente en el origen de cada legislación y, lo que es más importante, su aplicación.

Como más o menos se ha ido exponiendo, no solo el concepto en sí mismo, sino sobre todo su alcance, han sido interpretados y valorados de forma lo suficientemente dispar como para que todos ellos se deban tomar en consideración a la hora de alumbrar propuestas de armonización suficientemente universalizadas.

Tradicionalmente, las disparidades más remarcadas son las referidas o *detectadas* entre una y otra orilla del Atlántico, también en lo

referido a la privacidad. Puestos a destacar solo un aspecto susceptible de marcar una diferencia clara entre la doctrina estadounidense y la predominante europea –no carente de *matices*–, cabe señalar que aquella tiende a considerar lícita la difusión de datos personales siempre que sean veraces, en tanto que la imperante en buena parte de los países comunitarios tiende a sostener que el consentimiento debe añadirse a la veracidad.

Puede, en todo caso, que seguir circunscribiendo el debate a las disparidades entre EE. UU. y la UE, por relevantes y condicionantes que resulten, constituya una suerte de enfoque *nostálgico* que pasa por alto el alcance real de la globalidad. A nadie escapa que radicación física, localización, frontera y un largo etcétera de cuestiones, en otro tiempo determinantes, han dejado de tener valor. Trae como consecuencia, entre otras, que sea preciso avanzar en la exploración de renovadas pautas y tradiciones, a la hora de buscar un marco armonizado verdaderamente susceptible de ser compartido y ostentar efectivamente el pretendido –muy preciso– alcance global.

También se aprecian diferencias de índole cultural en las actitudes y percepciones de parte del consumidor. El hecho en sí mismo –consumo– tiene distintas lecturas dependiendo del entorno y, asociado a ello, son marcadas las disparidades en actitud y percepción frente al hecho publicitario, cuyo papel es sin duda central en cualquier aproximación que se realice al ámbito privacidad/intimidad.

1.2.3 Los datos, herramienta estratégica

De siempre, los datos han constituido una herramienta estratégica en la aproximación al consumidor, pero es indudable que la evolución de las técnicas de marketing, fruto en gran medida de la creciente presión competitiva en los distintos mercados, ha propiciado una progresiva puesta en valor de los de índole personal. Probablemente por ello, las bases de datos comprensivos del perfil demográfico, conductual y consumidor se han erigido en una modalidad de negocio en sí misma.

Anticipar las necesidades de los clientes es una de las principales preocupaciones de toda industria, para lo que históricamente se ha desarrollado un sinnúmero de técnicas y procesos de desigual efectividad. Una fuente habitual de conocimiento ha sido la propia relación con los consumidores, computando y analizando sus hábitos de compra, incluidos los observables cerca de la competencia, amén de distintas modalidades de prospección.

Lógicamente, localizar y obtener datos fiables ha sido siempre requisito previo a su explotación. Durante mucho tiempo, la principal fuente radicaba en organismos estatales o paraestatales, siendo los censos uno de los viveros más utilizados.

1.3 Privacidad, seguridad, información... y más

Toca señalar una obviedad: la privacidad no constituye un derecho absoluto –¿cuál lo es? –, sino que debe contextualizarse en relación con otros de igual o parecida consideración. Tanto es así que, en lo concreto que domina estas páginas, son frecuentes las *colisiones*, no siempre resueltas con identidad de criterio, no ya entre distintos países y ordenamientos, sino incluso en uno mismo, mediando apenas un leve desfase temporal o ni siquiera eso. Las dos confrontaciones más habituales atañen a información y seguridad.

Comenzando por este último, el desempeño del Estado ha incurrido a menudo en franca contradicción. Por un lado, se ha erigido como protector esencial del derecho personal a la privacidad/intimidad. Por otro, se ha considerado legitimado a invadirla en nombre de la defensa del interés más colectivo de la seguridad. De hecho, una parte de la producción normativa del último siglo y medio ha basculado entre la potestad gubernativa

–policial y judicial– de investigar y almacenar datos personales de sus ciudadanos, y límites impuestos a ello por la propia legislación. Una dicotomía que ha dado lugar incluso a cierta *alergia* social al avance tecnológico, partiendo de una lectura *orwelliana* de los instrumentos que proporcionaba al Estado para introducirse en la intimidad de los miembros de la comunidad.

Vale la pena recordar que una de las primigenias incorporaciones del derecho a la intimidad en el ordenamiento ha sido declarar la inviolabilidad de la correspondencia y las comunicaciones telefónicas; en no pocos casos, incluso dotada de rango constitucional. Protección, cuya tutela queda por lo general asignada a órganos judiciales, siendo los únicos habilitados y legitimados para «excepcionarla», en los casos o supuestos de presunta comisión delictiva y solo para los posibles autores de una transgresión de la ley.

Tanto o más controvertida ha sido y sigue siendo la contraposición entre el derecho a la privacidad/intimidad y el también constitucionalmente sancionado a la libertad de información y expresión. La profusión de litigios procesales para sentar los límites y *rozamientos* entre ambos derechos ha discurrido de forma proporcional a los avances y a la multiplicación de los medios de difusión, con una jurisprudencia a menudo oscilante entre la prevalencia de uno u otro, no solo atendiendo a una comparativa en tiempo real entre distintos países, culturas y tradiciones, sino dentro de un mismo ámbito y con exigua cadencia temporal.

La prevalencia de la información ha tenido, por lo general, la doble acepción de proteger la potestad profesional de difundir datos y el derecho de la sociedad a ser informada. Hasta fechas relativamente recientes, los litigios han discurrido casi siempre acotados al ámbito de los medios de comunicación: prensa, radio y televisión. Y, del lado de la jurisprudencia, los criterios dominantes se han centrado en apreciar, por un lado, la veracidad o falsedad de lo difundido y, por otro, valorar el carácter público o privado de la persona afectada. No siempre, conviene reiterarlo, con una unidad apreciable de resolución. No hace falta decir que la irrupción de Internet está cambiando parámetros, también en este ámbito, entre otras cosas por la proliferación de *medios* y la incursión de emisores individuales de información, al punto de estar generándose una especie de irresponsabilidad impune en el vertido a la Red de toda clase de rumores, falsedades e incluso calumnias/injurias de aparentemente difícil o imposible reparación.

Ciertamente, la aparición de *libelos* no constituye ninguna novedad, pero sí lo es el potencial que otorga el carácter viral de Internet. Remontados a otro momento histórico, son conocidos numerosos episodios de difusión de panfletos, pasquines, murales de contenido calumnioso, veraz o no, pero por lo general en ámbitos muy concretos, lo que limitaba su conocimiento a colectivos determinados, a veces ampliando su espectro mediante el siempre un tanto sorprendente *boca a boca*. La novedad está en que hoy bastan unos pocos minutos para que la *noticia* llegue a cualquier confín del planeta.

Resta referir otra vertiente del concepto seguridad: la que corresponde al uso de la propia Red. Aunque lo esencial es el flujo o si se prefiere la relación entre el usuario que vierte datos y el prestador de servicio que los captura, toca considerar la presencia de un imprevisible tercero capaz de interferir ese flujo, horadar los lugares de almacenamiento e incluso alterar uno y otro, con o sin percepción directa de los afectados por la intromisión.

La seguridad efectiva, y todavía más la percepción social que de ella domine, constituyen un factor crítico y probablemente determinante del desarrollo futuro de Internet. Lo está siendo, por ejemplo, en lo que se refiere al comercio electrónico de los particulares, donde la reticencia a facilitar datos bancarios –cuentas, tarjetas, pins...– está revelándose muy superior a la percibida respecto al uso de los cajeros electrónicos o de las mismas tarje-

tas –crédito o débito– cuando la compra es presencial.

La captura y posesión de datos, por tanto, deberá observar también requisitos de custodia y protección frente a amenazas externas, con asunción de responsabilidad en caso de violación, añadidas a las que puedan corresponder por cualquier otro uso u obtención indebidos. Mención particular merecen los distintos casos de *suplantación* que se producen en la Red: envío fraudulento de mensajes de correo electrónico, propagación de virus y amenazas y, en fechas recientes, la relativa proliferación de identidades falsas en Twitter.

1.4 Internet lo cambia... ¿todo?

Sería ocioso tratar de relatar toda la panoplia –extensa– de cambios que ha comportado Internet. A grandes rasgos, podría decirse que ha masificado y en cierta medida magnificado fenómenos que hasta su aparición habían permanecido poco menos que circunscritos a ámbitos muy minoritarios de la sociedad. Uno de los ejemplos más socorridos –aunque ajeno a lo tratado en este espacio– es, sin duda, la protección de la propiedad intelectual o, por expresarlo en sentido inverso, la difusión masiva de obras sin sujeción al derecho de autoría protegido por las leyes.

Algo parecido está ocurriendo con la salvaguardia de la intimidad o, en una consideración contrapuesta, el potencial de intromisión en el ámbito privado de las personas. Con una *innovación* muy relevante, como es no conocer por lo general el riesgo incurrido e incluso la falta de conciencia de haber prestado conformidad a la utilización de datos capturados *al otro lado* de la Red.

La eclosión de Internet ha generado nuevas pautas de comportamiento cuyo alcance resulta todavía complicado determinar. La supresión de barreras de acceso e intercomunicación abarca tantos aspectos que sería excesivo repasarlos, ahora y aquí. Pero, al tiempo, ha abierto no pocos interrogantes, buena parte de los cuales se están revelando enormemente difíciles de despejar y, todavía más, resolver.

Internet afronta, en buena medida fruto de todo ello, importantes desafíos, entre los que probablemente sobresalga la confianza en su uso por parte de la sociedad. Su desarrollo, por avanzado e irreversible que se antoje, dependerá en gran medida de su capacidad de superar los puntos de desconfianza que, por distintas razones, se han instalado en su derredor. Recelo que, en no pocos casos y aspectos, sigue actuando como barrera de entrada o factor disuasorio; no solo, aunque también, en los estratos de población que han accedido en fases avanzadas de su recorrido vital, experiencia y formación.

La arquitectura de Internet permite capturar de forma automática los datos vertidos por su uso. Algo en gran medida ignorado, si no como hecho en sí, básicamente en su alcance; es decir, aun existiendo conciencia de esa capacidad de captura, resulta poco menos que un arcano tener una idea clara de qué información está migrando del propio y acaso exclusivo conocimiento a los servidores que vehiculan la Red. Ello, como es deducible, marcando una clara diferenciación respecto a formas precedentes de intercomunicación en las que la privacidad más se ha fijado: telecomunicaciones y correo postal.

La señalada inviolabilidad de las comunicaciones postales y telefónicas, además de protegida incluso constitucionalmente, se ha entendido y de hecho ha discurrido garantizada por los prestadores del respectivo servicio. Pero ¿alguien protege o garantiza lo mismo en Internet?

Los compromisos de encriptación y custodia, siempre suscritos o asumidos de forma voluntaria por los agentes, supuesto su cumplimiento estricto, no entrañan la *no captura*, sino el simple compromiso de no utilizar los datos de forma distinta o no autorizada por quienes los suministran. En modo alguno se compromete a no almacenarlos: todo lo con-

trario. Sucede, además, que solo los usuarios más experimentados poseen los conocimientos y la experiencia suficientes para adquirir una mínima conciencia de qué datos están facilitando y, en su caso, qué herramientas tienen a su alcance para aumentar su nivel de protección. Un claro ejemplo son las llamadas *cookies*. Todos los navegadores y sistemas operativos del mercado facilitan un medio sencillo de desactivación, pero lo cierto es que solo una minoría de internautas opta por bloquearlas y muchos ni siquiera son conscientes de su existencia y significación. Existen, por otra parte, aplicaciones y servicios que simplemente niegan el acceso o el uso a quienes han utilizado esa posibilidad.

Más generalizado aún es el caso de sedes web que exigen como condición que el usuario acepte la utilización con fines comerciales de sus datos de carácter personal, tanto los capturados de forma opaca como los que obligadamente debe consignar en el cuestionario facilitado ad hoc.

1.4.1 La rendija del correo electrónico

La inviolabilidad del correo postal, dotada incluso de rango constitucional, fue históricamente pionera en la protección del derecho a la intimidad personal. Su *sucesor,* el correo electrónico, pareció merecer en principio idéntica consideración, pero la realidad no discurre estrictamente así.

Para muchos, el flujo de mensajes a través de la Red constituye la parte más vulnerable de su seguridad. Afecta a los sistemas de correo más extendidos y, tanto o más, a los de mensajería instantánea, lo que no ha impedido, por paradójico que resulte, su extensión masiva: a fecha de hoy, cualquiera dispone de una o varias cuentas de correo electrónico y una apreciable mayoría está adherida a un servicio de conversación –chat–. Contrasta, por descontado, con la idea de que no ofrecen la debida privacidad.

Probablemente no venga a cuento desarrollar aquí todos los cambios que han comportado el correo electrónico, la mensajería instantánea y su relativo *pariente*, los mensajes *Short Message Service* (SMS) y *Multimedia Messaging System* (MMS), en los hábitos, comportamientos y formas –consumos– de comunicarse. Pero sí al menos mencionarlo para tener en cuenta su importancia relativa y la trascendencia social de cómo evolucione la protección efectiva del derecho a la intimidad.

Recuperando el antecedente del correo postal, la versión electrónica se ha revelado mucho más vulnerable, incluyendo aspectos que en absoluto lo eran en su predecesor. A la intrusión estricta en el texto de los mensajes se han agregado otras, como la suplantación de la dirección remitente, la captura de la agenda de contactos y hasta la réplica íntegra de las bases conteniendo todo o parte de los datos de envío a los adheridos al servicio.

La derivación más extendida es, por descontado, la masiva distribución de correo *spam*, que ha tenido como respuesta la puesta a disposición de los suscriptores de herramientas de filtro y desvío de mensajes. Otra, harto frecuente, es la difusión de *virus* de efecto nocivo, con capacidades tales que copiar todos los contenidos del disco duro, con o sin borrado previo o posterior, reenviar el mensaje *infectado* a todos los incluidos en la lista de correo del destinatario, etcétera.

Acaso más llamativo resulta que la doctrina y práctica normativas se estén produciendo de forma sustancialmente distinta en lo relativo al correo electrónico respecto de la doctrina largo tiempo asentada en lo referido a la comunicación postal. Aunque la jurisprudencia no acaba de ponerse de acuerdo en dotar de validez probatoria a los mensajes de correo electrónico –antes ocurrió otro tanto con el fax–, son ya varios los casos en los que un tribunal español –también de otros países– ha sentado dos principios relevantes, uno de ellos directamente relacionado con la privacidad.

En síntesis, se viene considerando que el curso de mensajes de correo electrónico a través de los sistemas corporativos o empresariales no está sujeto a plena privacidad, puesto que los directivos tienen pleno derecho a conocerlos y, en su caso, emplearlos en vía disciplinaria. Así se ha admitido en más de un caso de sanción a un empleado, llegando incluso a considerar procedente el despido, a partir de haber considerado prueba válida el texto de un mail. En algún caso –menos– se ha extendido esa consideración a cualquier comunicación enviada o recibida desde el ordenador puesto a disposición por la empresa, en horario laboral, fuera cual fuese el servicio de correo utilizado; es decir, aunque fuese distinto al corporativo.

Cabe mencionar, por otra parte, la admitida existencia de mecanismos de rastreo en manos de servicios de inteligencia, capaces de localizar en tiempo real determinadas palabras, frases o conceptos en cualquiera de los millones de mensajes que diariamente se intercambian a través de todos los sistemas de correo y mensajería que pueblan Internet. De nuevo, como es obvio, surge la correlación entre seguridad y privacidad, en este caso bajo el teórico *paraguas* de la lucha global contra el terrorismo y el crimen organizado.

1.4.2 Modelos de negocio emergentes

La Red ha traído consigo la emergencia de no pocos negocios hasta entonces inexistentes, pero en conjunto sigue pendiente de establecer un modelo de negocio específico o, por expresarlo de otro modo, construir una configuración estable de cadena de valor, con los consecuentes repartos entre todos y cada uno de los participantes y prestadores del universo Internet.

Esta carencia de modelo estable ha propiciado precisamente la configuración de distintas e incluso variopintas formas de capturar valor, partiendo de la premisa –de momento difícilmente eludible– que otorga carácter gratuito o semigratuito al uso de Internet.

Sin ánimo de caer en un recorrido exhaustivo, cabe apuntar que lo anterior ha condicionado, o está condicionando en gran medida, lo que pudiera ser rotulado como quebrantamiento del derecho a la privacidad.

A nadie se oculta que, hoy por hoy, la publicidad es el único medio de aportación de ingresos verdaderamente extendido en Internet. Distintos intentos de fijar precio y percibirlo por el acceso a contenidos se han saldado en fracaso, al punto de haber *retrocedido* sus prestadores a la gratuidad. No es momento de ahondar en las implicaciones de esa realidad, pero baste citar la aparente incoherencia entre la demanda de contenidos de mayor calidad por parte del mercado y la refracción que se debe pagar por ellos, poco menos que despreciando la evidencia de que el coste efectivo de los contenidos es directamente proporcional a su calidad.

Internet, no obstante –se ha mencionado antes–, ha conseguido captar únicamente una pequeña porción, aunque creciente, del total de inversión publicitaria o, lo que es más importante, un volumen de recursos a todas luces insuficiente para que todos los que se incorporan a la Red alcancen situaciones de rentabilidad. Sucede además que, aun siendo relevante la progresión interanual de esos ingresos, su tasa o ritmo de crecimiento es varias veces inferior a la multiplicación de sitios incorporados a la Red.

Tiene fundamento, por tanto, que el uso y explotación de los datos se haya erigido en una fuente de generación de recursos, a veces complementarios, a veces sustitutivos de los obtenidos a partir de publicidad. De hecho, han surgido modelos de negocio[4] cuya viabilidad se asienta única y exclusivamente en el uso y la eventual rentabilización de los datos obtenidos del usuario final. Pero también los hay de

4. Tratado extensamente en el capítulo 3.

carácter mixto: entre otros, los que complementan el cobro de una comisión por la prestación de un servicio, casi siempre de intermediación, con la explotación comercial de la información capturada en el correspondiente acto. Un ejemplo pueden ser los sitios especializados en *facilitar* reservas en hoteles, restaurantes, espectáculos, etcétera, cuya actividad se extiende a vehicular ofertas y promociones atendiendo a las preferencias y hábitos *detectados* en la prestación del servicio.

1.4.3 El papel de los buscadores

Los motores de búsqueda o buscadores han adquirido un papel central en Internet. Su peso determinante ha ido creciendo conforme se multiplicaba y diversificaba la oferta de sitios disponible en la Red. Los hay de distintos tipos: desde generalistas a especializados, con o sin prestaciones de *gestión*, perceptores de un precio –comisión– por el servicio o completamente gratuitos. Su modelo de negocio, en consecuencia, es dispar.

Contrariamente a la tónica de atomización imperante en muchos aspectos, en este apartado es casi obligado mencionar a Google como paradigmático en el ámbito de las búsquedas. No solo, aunque también, por ser el utilizado mayoritariamente, con los demás a enorme distancia, cuanto por su condición de precursor en la articulación de fórmulas de obtención de ingresos y la ramificación de actividades –productos– que ha ido desarrollando.

No se trata, lógicamente, de analizar el fenómeno Google en su totalidad, pero sí de aproximar su papel en cierta medida central en lo que se refiere a la privacidad.

Otro aspecto que se debe tener en cuenta, referido al papel de los buscadores, es su carácter de facilitadores de acceso a depósitos de datos e información ya existentes, pero de difícil o complicado acceso para el público en general. No pocos ejemplos constatan que muchas veces la privacidad se consideraba suficientemente salvaguardada con esa suerte de *barrera*, pero la intervención de los motores de búsqueda la ha eliminado, ayudados por herramientas de software complementarias al alcance de cualquier usuario. Una muestra ilustrativa son las publicaciones oficiales que contienen datos relativos a la situación personal: providencias, edictos, adjudicaciones, etcétera. Es verdad que de siempre han resultado accesibles, pero su manejo resultaba engorroso y la localización del dato concreto precisaba emplear un tiempo apreciable de consulta y, en muchos casos, cierta especialización. Hoy día, en cambio, la búsqueda se puede producir prácticamente en tiempo real, desde cualquier ubicación que permita acceder a la Red, con suma facilidad y al alcance de cualquiera dotado de conexión.

También resulta notable que los buscadores constituyan probablemente el aporte –*captura*– más rico y extenso de datos en Internet. La frecuencia y multiplicación de uso –para muchos constituye el medio exclusivo de acceso–, junto con el carácter multidisciplinar de las búsquedas, propicia establecer un perfil enormemente completo del usuario asociado o asociable al punto de conexión. Seguramente por ello suelen ser el principal generador de susceptibilidad a la hora de abordar el derecho a la privacidad.

Ayuda, sin duda, que su evolución –Google a la cabeza– haya discurrido hacia la implantación de búsquedas patrocinadas y otros mecanismos generadores de ingresos, como puede ser primar la ubicación de un sitio web en la lista de localizaciones cuando aquel satisface una determinada cuota en concepto de alguna de las modalidades ofertadas de publicidad. Un mejor posicionamiento facilita, a su vez, la captación de ingresos publicitarios para el sitio en cuestión.

No menos controvertida ha resultado alguna de las aplicaciones desarrolladas colateralmente, como es el caso de *Google Earth* o *Street View*, en las que, al tiempo que se facilitaba la localización real o solicitada, se proporcionaban imágenes consideradas privati-

vas de terceros, dando lugar incluso a la prohibición en sede judicial del servicio en algún país, como por ejemplo Alemania.

1.4.4 Del equipo a la *nube*... ¿vulnerable?

El desarrollo futuro de Internet parece orientado a una transformación relevante en la relación hasta ahora dominante desde y para los usuarios. En síntesis, se presume una sustitución más o menos acelerada desde el uso *local* a formas más *remotas* de utilización. Las derivaciones son bastante amplias, pero centrados en el campo de la privacidad conviene destacar la tendencia al almacenamiento, por un lado, y la compartición, por otro. De ambas van a surgir, están surgiendo, nuevos modelos de negocio y modalidades de prestación[5], en las que la mayor o menor garantía de protección a la privacidad va a desempeñar un papel esencial.

Sería prolijo diseccionar cómo y por qué la práctica de radicar información y contenidos en el propio equipo ha ido decayendo como preferencia, lo importante es que ha ocurrido, tanto en el ámbito personal como en el medio empresarial o profesional. Una razón esencial puede haber sido la limitación de capacidad que, antes o después, puede presentar cualquier ordenador. Lo que, en el caso de profesionales y empresas, acaba traducido en necesidades de mayores desembolsos e inversiones para cubrir las necesidades de almacenamiento, proceso y gestión.

Al abrigo de esas tendencias se están desarrollando, con cálculos de enorme potencial, nuevos modelos de prestación, entre los que interesa destacar distintas formas de *cloud computing*, crecientemente ofertadas a todos los niveles: desde las grandes y pequeñas compañías al usuario de carácter personal. Ofrecen, en términos generales, capacidades de almacenamiento y proceso a costes netamente inferiores a los que deberían asumirse para obtener individualmente idéntica prestación.

Es imaginable que será clave en su desarrollo la fiabilidad. Esto es, habrá de proporcionar garantías y obtener crédito en orden a la conservación de los datos vertidos en la *nube*, pero al propio tiempo asegurar que permanecerán suficientemente protegidos, a salvo tanto de incursiones o violaciones externas –*hackers*– como de uso indebido por los responsables de gestionar el servicio.

No es de extrañar, por tanto, que *cloud computing* parezca llamado a ser objeto de particular dedicación a la hora de pergeñar un marco normativo que proteja y garantice la preservación del derecho a la privacidad. En realidad, ya lo está siendo, aunque de momento con claras asimetrías, lo mismo en el interior de áreas como la UE que entre esta y EE. UU., por citar únicamente la comparación favorita de una mayoría de observadores, analistas y la propia industria relacionada con la sociedad de la información.

No hace falta resaltar que la propia concepción de la *nube* desvincula por completo las respectivas ubicaciones del *propietario* de los datos y los servidores encargados de su almacenamiento, proceso y, en su caso, gestión. De ahí que se antoje condición ineludible un planteamiento común –armonizado– a escala global para que la perseguida protección sea efectiva.

En tanto que segmento de negocio con enorme potencial, convendrá valorar también las implicaciones que una eventual asimetría podría acabar acarreando en el aspecto competitivo y de posicionamiento de los agentes.

1.4.5 Especificidad de las redes sociales

La emergencia y la extensión de las redes sociales han introducido nuevas consideracio-

5. La amplia y creciente disposición de nuevas prestaciones se aborda en el capítulo 3.

nes en el ámbito de la privacidad. Han constatado, entre otras cosas, un nuevo enfoque del concepto mismo o, si se prefiere, la percepción que de él alberga una parte sustancial de la población; en especial, los segmentos más jóvenes y, en consecuencia, imbricados preferentemente en la era digital.

Sin tener del todo claras las causas, lo cierto es que las generaciones más jóvenes evidencian una propensión a divulgar y compartir aspectos que para la mayoría forman todavía parte de la intimidad que entiende tener derecho a preservar y para la que se reclama un modelo efectivo de protección. Una posibilidad quizá tenga que ver con el hecho de su incorporación al uso de Internet desde los contornos de la propia infancia, asimilando como *natural* su esencia: esto es, la libertad de interconexión y acceso superando tradicionales barreras de tiempo, espacio, distancia, ubicación y demás. Acaso de ello parta la poca o ninguna reticencia a verter en la Red datos, vivencias, opiniones, experiencias e incluso estados anímicos, por descontado los propios y, con relativa frecuencia, hasta de los demás. Lo que abre, sin duda, un frente que cabe tener en cuenta: que una presumida renuncia al derecho de salvaguardar la intimidad propia no puede ni debe derivar en considerarse liberado de mantener el respeto al derecho de otros.

De alguna manera, cabe entender que la adhesión a las redes sociales comporta una suerte de renuncia, respecto a la protección y defensa de la privacidad. Pero no está tan claro. No se puede ni debe pasar por alto que se aprecia cierta tendencia a una mayor utilización de las opciones de limitar el acceso que incorpora la mayor parte de ellas, lo que, desde una óptica sociológica, puede inducir a considerar el fenómeno como una forma de respuesta al aislamiento que en muchos sentidos imponen determinados aspectos de la configuración social dominante. Se habría producido, así, un efecto del todo contrario al en su momento profetizado respecto del avance tecnológico: Internet no habría conducido a la *producción* de seres aislados, individualistas y más o menos fronterizos con el autismo, sino que estaría contribuyendo a la superación de lo que, en ese sentido, deriva de la urbanización, los horarios, las distancias y cuanto ha distorsionado viejos hábitos de relación social, añadiendo dificultades a la relación personal directa.

La propia e inequívoca esencia de las redes sociales descansa en la compartición. Algunos analistas las han descrito como sustitutivo poco menos que obligado a las formas tradicionales de interrelación comunitaria, surgido por imperativo directo de un teórico aislamiento personal impuesto por las nuevas formas de vida y organización poblacional. Pero no queda del todo claro que sea así. Aun admitiendo que algo de eso pueda estar en el motor de su emergencia, es innegable que concurren otros factores que, en suma, constituyen un cambio sustancial en la actitud personal de relación.

La aproximación e inclusión en esta nueva modalidad de interrelación denota ingredientes algo distintos, en realidad renovados, respecto de lo considerado tradicional, siquiera en la segunda mitad del pasado siglo XX. Se percibe, sobre todo, una consideración distinta de la intimidad. Es frecuente, incluso, apreciar una suerte de desinhibición al comunicar y difundir aspectos de la personalidad, el comportamiento y la experiencia vitales muy distintos, en realidad más amplios, que los admitidos y practicados en la relación directa, cara a cara, presencial.

Cabe percibir también un deseo de ampliar notoriamente el entorno, el círculo y alcance de las relaciones, no solo, aunque también, superando las proverbiales limitaciones físicas: tiempo, espacio, ubicación, disponibilidad... Hay que admitir que recorrer espacios como Facebook, Twitter o hasta Linkedin provoca no pocas sorpresas, incluso en personas que uno podía jactarse de conocer con relativa profundidad.

No es este un espacio que deba dedicarse a horadar y profundizar en el fenómeno de las

redes sociales, pero sí puede resultar oportuno preguntarse si pueden o deben requerir una consideración específica y diferenciada a la hora de abordar la necesidad de un marco de regulación orientado a proteger o salvaguardar el derecho a la intimidad.

No es, en absoluto, que en ellas no quepa ni proceda tener en cuenta tal derecho, pero sí incluir en su tratamiento específico el hecho incuestionable que adherirse a ellas comporta un deseo más que manifiesto de verter precisamente lo íntimo: todo lo contrario al deseo de permanecer anónimo y desconocido que en cierta medida algunas jurisdicciones y jurisprudencias han asimilado a la privacidad, y que se revela muy presente en el resto de los usos asociados a la Red.

Cuestión distinta es que, igual que ocurre en términos generales con el uso de Internet, todos y cada uno de los integrados en las redes sociales sean plenamente conscientes del alcance de su adhesión y el uso que hacen de ellas. Ocurre, entre otras razones, porque no es precisamente amplia la transparencia que ofrecen en los dos puntos cruciales varias veces señalados: ¿qué datos e información se está capturando?, ¿qué uso les están dando los gestores de esas redes?

Además de otros factores, es incuestionable que las nuevas generaciones no han sentido los condicionantes que, en forma de *barrera de entrada,* han sentido y en buena medida siguen sintiendo quienes se han ido incorporando, potencial o efectivamente, al uso de las nuevas tecnologías en fases más avanzadas de su recorrido vital y profesional, y muy en particular a la utilización cotidiana y regular de Internet. Cabe constatar la enorme diferenciación en las percepciones y, en consecuencia, actitudes y hábitos entre segmentos de la sociedad, por lo general referidos a los distintos estratos de edad, tanto o más que el grado de formación, el nivel de renta o incluso la mayor o menor inserción en las áreas urbanizadas de cada territorio.

En definitiva, cabe apuntar la probabilidad de que el fenómeno de las redes sociales haya comportado una relativamente sorpresiva mutación en la idea de privacidad, al menos en las generaciones más recientemente incorporadas al uso cotidiano de la Red.

1.4.6 Operadores de telecomunicaciones

El escrupuloso respeto a la privacidad –datos de sus clientes– no constituye para las operadoras de telecomunicaciones ninguna novedad: forma parte en gran medida de su cultura empresarial. Que haya tenido o no que ver con la reglamentación específica, derivada de la estricta consideración protectora que las leyes han otorgado a la privacidad de las comunicaciones es opinable, pero la realidad es que su ejecutoria ha sido raramente generadora de desconfianza, sin *incidentes* que, por ejemplo, hayan inducido el reforzamiento de las reglas sectoriales de custodia y manejo de la información obtenida.

Es una evidencia que, además de los datos correspondientes a la estricta correlación entre proveedor y cliente, las operadoras han dispuesto –disponen– de amplia información relativa a consumos, tráficos, hábitos, tendencias, etcétera, pero la *doctrina* sectorial dominante ha sido siempre restringir su utilización, prioritariamente a la planificación del despliegue de sus infraestructuras y recursos de red, y como añadido a acciones de índole comercial orientadas a sus clientes, adición de nuevos servicios y mejora de prestaciones.

Cabe hablar, en consecuencia, de una cierta tradición de sensibilidad respecto a lo que se suele considerar como derecho a la privacidad, probablemente superadora del imperativo que haya comportado las reglas establecidas para el sector de las telecomunicaciones. Algo que, sin ir más allá en la consideración, necesariamente contrasta con el tratamiento más *ambiguo* que se ha podido observar en otras ramas de actividad, sobre las que hasta ahora no se ha fijado un marco normativo específico, más allá del establecido con carácter

genérico para el tratamiento de los datos personales.

Es importante señalar que la política seguida no ha supuesto un freno a la capacidad innovadora de las compañías ni, todavía menos, ha comportado una sobrecarga de acciones o procedimientos por parte de los suscriptores. Su práctica ha discurrido, pues, de una forma que se puede considerar equilibrada y en gran medida satisfactoria para ambas partes. Por decirlo de forma más expresiva, ninguna medición demoscópica ha revelado desconfianza o susceptibilidad social, sí manifestada en otros ámbitos respecto a los que se presupone –con razón o sin ella– una ejecutoria más *laxa.*

Dicho de otra manera, cabe preguntarse si, aunque no sean las únicas facultadas, las operadoras de telecomunicaciones no están en posición relativamente aventajada para cuando menos enriquecer un modelo protector de la privacidad que conjugue la efectiva salvaguarda de los derechos del usuario de la Red con la capacidad innovadora para añadir nuevas prestaciones –servicios, aplicaciones, herramientas...–, en un marco suficientemente armonizado para que no se produzcan menoscabos competitivos ni garantías diferenciadas en una realidad global.

No en vano, y por encima de todo, las operadoras de telecomunicaciones son y van a seguir siendo parte sustancial del universo Internet, cuya extensión masiva, tanto cuantitativa –usuarios– como cualitativa –prestaciones–, fundamenta la necesidad de reorientar y adecuar la protección del derecho individual y colectivo a la privacidad.

1.5 El papel central de la publicidad

Una preocupación básica de la actividad publicitaria es ajustar el mensaje –inversión– al impacto efectivo y su contribución a las ventas del producto anunciado. Se han sucedido para ello diversas técnicas que, en síntesis, tratan de focalizar como destinatario central del mensaje al consumidor potencial, tenido como público objetivo al que orientar la estrategia comercial.

Hasta fechas recientes, sin embargo, ha predominando el factor cuantitativo sobre el cualitativo a la hora de determinar los planes de inversión en publicidad. Así, el grueso de recursos dedicado se ha orientado a medios de comunicación considerados de masas –prensa, radio y televisión–, con métodos de cómputo de audiencia basados en la cifra de difusión –ventas– en el caso de los medios impresos, y encuestas o mediciones de muestra para los audiovisuales. Los planes de medios, en consecuencia, se han construido por lo general a partir de la posición relativa de cada medio, mucho más que atendiendo al análisis más pormenorizado de los perfiles y características del *receptor*: lector, oyente o espectador. Es verdad, en todo caso, que tal regla ha mantenido excepciones, centradas en publicaciones o programas muy especializados, entre cuyos adeptos se presumían hábitos o preferencias de consumo hacia productos determinados. Han captado, no obstante, porciones minoritarias de la inversión publicitaria total.

Fuera del universo de los *mass media*, han proliferado estrategias de alguna manera más personalizadas, con acciones de marketing directo, telefónico, postal e incluso presencial-domiciliario, pero su participación en el conjunto ha estado siempre a distancia de la inversión conjunta en los *media*.

Se puede mencionar aquí la proliferación de acuerdos comerciales entre empresas y grupos o colectivos específicos para la difusión preferencial entre sus miembros de ofertas por lo general diseñadas ad hoc, con o sin cesión íntegra de las correspondientes bases de datos. Ha sido el caso de entidades financieras, compañías de seguros y cadenas comerciales que suscriben pactos de ese tipo con clubes deportivos, asociaciones culturales o empresas para *beneficio* de sus miembros.

Cabe decir, por tanto, que la inversión publicitaria ha discurrido mayoritariamente concebida *a bulto*, con una presunción de que, a mayor número de destinatarios, mayor probabilidad de captar una porción relevante del público objetivo que interesa *convencer.*

El *sueño* de una publicidad personalizada, aunque apenas materializado, viene no obstante de atrás. Intentos previos se han saldado con eficacia más bien limitada, sin la debida correspondencia entre el esfuerzo requerido y los frutos cosechados... hasta que el avance tecnológico ha abierto la puerta a su consecución. Dos canales se han habilitado de forma muy clara: Internet, por un lado, y la interactividad de los medios audiovisuales, por otro. En ambos casos, huelga decirlo, la provisión de datos ejerce un papel fundamental para producir una comunicación comercial *a medida*, dando lugar a una posible nueva problemática en relación con la privacidad.

Aunque todavía minoritaria en términos de participación sobre el total (15 %), la publicidad a través de Internet presenta, año tras año, tasas de crecimiento del orden del 7-8 %, en tanto se reducen las cantidades absolutas destinadas a los medios masivos de comunicación. Ello acompañado de avances bastante notorios de nuevas modalidades directamente vinculadas a innovaciones rápidamente asentadas como la movilidad.

Las razones son variadas, pero pueden resumirse en una progresiva puesta en cuestión de lo anteriormente apuntado: efectividad del criterio cuantitativo frente al cualitativo a la hora de abordar el público objetivo –deseado– para cada inversión. Con el complemento, nada despreciable, del cambio de determinados hábitos de consumo en buena parte de la sociedad, en líneas generales tendentes a una acelerada segmentación.

La televisión, hasta ahora soporte publicitario por excelencia, es buen ejemplo de cómo la segmentación de las audiencias está dificultando la efectividad de una estrategia cuantitativa, a lo que toca agregar otra inclinación que empieza a percibirse: el tránsito desde la aceptación de las cadenas de índole generalista y programación estructurada hacia un deseo de consumo más personalizado, con elección de contenido, momento y cadencia por parte del espectador. Algo sin duda apoyado por la existencia de dispositivos asequibles para la organización doméstica del consumo televisivo, el acceso a contenidos a través de la Red o la creciente disposición de servicios de *streaming* que, como se está haciendo cada vez más evidente, incluso cambian la relación del usuario con el propio Internet[6].

Es notorio que el grueso del potencial está por aprovechar. La publicidad en la Red sigue mayoritariamente sujeta a pautas unidireccionales, lejos de la personalización o el mensaje a medida que se citan como tendencia de futuro. Y lo mismo cabe decir de la inversión publicitaria en televisión, cuya digitalización no ha comportado, por ahora, lo en su momento presentado como *salto* cualitativo más relevante respecto de su predecesora analógica: interactividad. Una carencia que muchos asocian a la idea de que la televisión vive actualmente una fase de transición que desembocará en un escenario dominado por la difusión personalizada, a medida, verdaderamente interactiva y bajo demanda directa a través de Internet.

También en fase de desarrollo inicial, pero con un potencial atribuido nada despreciable, se suele situar una evolución de fórmulas publicitarias basadas en la movilidad y, derivada de ella, la localización[7]. Un exponente pueden ser las búsquedas patrocinadas, de modo que dirijan la provisión del producto o servicio soli-

6. Se refiere a la progresiva tendencia a sustituir posesión de contenidos y descargas por el acceso a sitios en los que se pueden visualizar sin necesidad de usar las capacidades de memoria de los dispositivos propios.
7. Ejemplos de esta innovación se detallan y describen en el capítulo 3.

citados al prestador más cercano a la ubicación, con la correspondiente contraprestación por compraventa unitaria.

Sin duda, como contrapartida de todo ello, reverso si se prefiere, toca citar la profusión de ofertas comerciales y publicidad no solicitadas ni deseadas, como variantes específicas del fenómeno más amplio que constituye el *spam.* Dejando de lado aquellas que constituyen una violación flagrante de la privacidad, por estar basadas en datos obtenidos, comercializados o utilizados subrepticiamente, existen otras derivadas de formas de consentimiento prestado por el usuario.

Está ya bastante extendida la práctica de ofertar servicios y contenidos gratuitos a través de la Red, previa exigencia del compromiso de *permitir* el envío de mensajes publicitarios y ofertas comerciales. Estimula, sin duda, acogerse a este tipo de transacciones el carácter de *gratis total* que permanece adherido a Internet. No es seguro, en cambio, que exista debida conciencia de cuáles son las verdaderas implicaciones para el usuario que se aviene al *pacto* ni sea cierta en sentido estricto la consideración de gratuidad. Lo primero deriva del carácter genérico con que se propone el otorgamiento del *permiso*. Lo segundo, la pretendida gratuidad es engañosa porque, si bien el prestador del sitio no está recibiendo una contraprestación dineraria, no significa que el usuario no esté *pagando* por el uso: en realidad, está realizando una aportación, puesto que entrega datos personales de los que aquel puede decidir obtener un rédito económico.

A modo de conclusión, se puede afirmar que Internet tiene en parte pendiente encontrar su propia forma de expresión publicitaria, optimizando el aprovechamiento de sus características diferenciales respecto a otros medios y soportes. Algunos han recordado que algo parecido ocurrió con los primeros pasos de la televisión. Las primitivas inserciones publicitarias a través de la pantalla fueron poco más allá de replicar las *guías comerciales* en aquellos tiempos características de las emisiones radiofónicas, con el solo añadido de una cámara y la visualización de la imagen del o los encargados de su locución. Tiempo después apareció el *spot* que permitió dar el salto en anuncios, tarifas e ingresos... hasta hoy. Y, acaso curiosamente, ello forzó a buscar nuevas formas de expresión publicitaria en las emisiones de radio, fruto de lo cual la *cuña* sustituyó a la mencionada *guía.*

¿Serán personalización y localización la base del *hallazgo* que precisa Internet como el *spot* lo fue para la televisión? Son cada vez más los convencidos de que puede ocurrir... compatible con la debida protección de la privacidad.

1.6 Camino del futuro: tecnología, transparencia, armonización...

El papel central de la tecnología no se puede discutir. Sin los avances hoy accesibles y sobre todo comercializados, el enfoque clásico posiblemente podría aspirar a persistir. Su implosión lo ha cambiado todo y es por ello que corresponde buscar nuevas formas y renovados marcos de regulación. Ahora bien, la innovación tecnológica, ¿juega en contra o a favor de la protección?

La respuesta puede sonar ambigua, puesto que en realidad juega y sobre todo puede jugar en ambos sentidos.

No es momento ni espacio para enfatizar lo que el avance tecnológico ha aportado y puede seguir aportando al desarrollo económico y el bienestar individual y colectivo de la sociedad. Lo que no significa ni puede significar que la erosión de la privacidad debiera aceptarse como una suerte de precio que satisfacer por disfrutar de los beneficios aportados. Dicho de otra forma, la potencial o real pérdida de intimidad asociada al uso de Internet no tiene por qué abocar a ninguna suerte de resignación.

Un ejemplo reseñable –en absoluto único– es la respuesta tecnológica que se viene procurando frente a la actitud reticente detecta-

da respecto de distintas formas de comercio total o parcialmente *online*.

A nadie se oculta que el recelo a verter a la Red los datos bancarios o de los medios más extendidos de pago –tarjetas de crédito o débito– se ha erigido como uno de los principales obstáculos al desarrollo del comercio electrónico, aunque bien es verdad que con diferencias sustanciales de actitud en los distintos países y mercados. Esto se ha visto, sin duda, periódicamente estimulado por la difusión de casos de fraude muy señalados, con mayor intensidad que en episodios en gran medida paralelos, tal que la clonación física de tarjetas o la captura de las claves de utilización.

No es equiparable el efecto desincentivador producido a raíz de los casos de fraude producidos –conocidos– en la Red, con el mucho menor que ha derivado en la utilización presencial de medios de pago o el uso de cajeros electrónicos en las operaciones bancarias. Es más: el aumento del uso de Internet como plataforma de relación con el banco se ha visto mucho menos penalizado que las distintas formas de comercio *online* por los particulares, pero la realidad es que, entre unos y otros, han aumentado las reticencias en relación con el uso de medios de pago electrónicos y a ello ha debido hacer frente el sector.

En fases sucesivas, la tecnología ha aportado ingredientes para mejorar la seguridad de las transacciones y, tanto o más que eso, la percepción de los usuarios.

1.6.1 El consentimiento libre e informado, clave para la innovación en nuevos servicios

El carácter personal del derecho a la privacidad puede sugerir, de hecho señala, el consentimiento como elemento capital para fijar la frontera entre el uso debido o indebido de la información –datos– de índole privada.

Hay que partir de lo ya apuntado: no existe plena conciencia, mucho menos constancia fehaciente de qué datos e informaciones resultan *capturados* en cada *navegación* a través de la Red. La hay, eso sí, cuando el uso o la prestación de un servicio requieren cumplimentar un cuestionario, facilitar determinados datos o, en ciertos casos, mantener activado el registro de *cookies* como condición exigida por la propia web. Aunque tampoco en estos casos está del todo garantizado que los únicos datos *capturados* sean los derivados del referido cuestionario ni, en consecuencia, sea posible conocer todo el alcance de una eventual conformidad prestada a la solicitud de utilización.

A todo ello cabe añadir la inseguridad jurídica que planea, tanto respecto al eventual uso sin mediar consentimiento como cuando aquel no se ajusta a lo expresa o tácitamente consentido. ¿Cómo saber cuál ha sido ese uso? Y, caso de lograr constancia –difícil– de la transgresión, ¿a qué instancia acudir? Y, suponiendo superado todo lo anterior, ¿cuál es el resarcimiento posible?

La realidad es que el usuario no tiene demasiadas posibilidades de ejercer un efectivo control sobre sus datos en Internet. Afronta, además, prácticas dispares y heterogéneas en materia de protección y salvaguardia de su privacidad. Es así porque, entre otras realidades, cada sitio dispone de margen de libertad para elegir o diseñar sus *compromisos*, a los que en ocasiones el internauta debe prestar conformidad antes de usar la aplicación, herramienta o servicio, sin que siempre el texto ofrecido sea suficientemente comprensible. La casuística es muy extensa y, por ende, susceptible de un sinfín de disparidades imposible de concretar.

Tampoco resulta siempre sencillo abordar el ejercicio del derecho de protección. Arranca de la práctica imposibilidad, en muchos casos, de requerir la rectificación y todavía más la cancelación de una eventual conformidad prestada o la simple rectificación de datos prestados conscientemente. Y culmina, en todo caso, en la enorme dificultad de ejercerlo cuando media constatación o simple sospecha de transgre-

sión, sea en instancia administrativa o judicial. Es notoria, además, la práctica inviabilidad de un resarcimiento pleno, por ejemplo en el caso de que se haya producido una difusión indebida, dada la imposibilidad de retrotraerla desde todos y cada uno de los destinatarios. Y, por sumar un ingrediente añadido: ¿es mensurable económicamente el daño causado?

Conviene señalar, en todo caso, que cualquier fórmula adoptada para un otorgamiento informado, efectivo y consciente de conformidad habrá de preservar el debido equilibrio para que no acabe por constituir un obstáculo al desarrollo y la innovación.

Ya se ha visto que determinados servicios, herramientas, aplicaciones y utilidades exigen en sí mismos la captura y gestión de datos de los usuarios susceptibles de ser considerados de índole privativa, privada o personal. De hecho, muchas veces lo son. De ahí que establecer un exceso de complejidad o una sobrecarga de limitaciones podría devenir en hacer inviable la puesta a disposición del mercado de innovaciones potencialmente contributivas al progreso económico y el bienestar.

Puntos clave que considerar podrían ser ajustar la captura de datos a lo esencialmente necesario para la prestación óptima del servicio –uso– y, por otra parte, reforzar las garantías de tratamiento y custodia por parte del prestador. Todo, con una mejora apreciable del grado de conocimiento y conciencia del usuario; esto es, con la mayor transparencia posible de información en cada operación.

1.6.2 Transparencia: sí, pero...

Ciertamente, la transparencia surge como un elemento imprescindible, acaso en teoría idóneo e insuperable, para permitir al usuario el libre albedrío sobre sus datos personales.

El argumento de partida suena impecable: en tanto que propietario de los datos que afectan a su intimidad, nadie mejor que la propia persona para determinar y decidir quién, cómo, cuándo y para qué pueda utilizarlos, difundirlos o, en su caso, comercializarlos... incluso a cambio de... Pero la realidad, en parte de nuevo por imperativo del avance tecnológico, muestra que semejante lectura anda excedida de sencillez.

Hay que decir, en primer término, que ningún marco se puede considerar idóneo si su esencia descansa en una suerte de sobrecarga sobre el usuario. No solo, aunque también, por la señalada disparidad de concepciones, por lo general reflejadas en la literatura normativa, cuanto por aspectos más operativos, como es la falta de comprensión jurídica o, desde otro punto de vista, que los compromisos asumidos por el prestador del servicio figuren en zonas poco visibles del correspondiente sitio de Internet.

Diversos estudios demoscópicos constatan que una mayoría de usuarios de Internet carece de la debida conciencia de cuáles son sus derechos, qué grado de protección han asumido –o renunciado– y, lo que es todavía más relevante, cómo y ante quién deberían reclamar la protección de sus derechos y, en caso de violación, cuáles son las instancias y los procedimientos que tienen a su alcance para reclamar ser resarcidos.

1.6.3 Armonización, equilibrio y competitividad

Un corolario determinante es abordar y, subsiguientemente, resolver la problemática desde un objetivo claro de armonización y equilibrio.

Está suficientemente constatado que Internet ha desvirtuado los límites territoriales; en realidad, han dejado de existir en todo lo referido a la Red. Pero no es lo único: tanto o más ha invalidado diferenciaciones tradicionales en materia sectorial. Parece, en consecuencia, llegada la hora de descartar diferencias normativas entre estados y entre sectores como vía de solución a los problemas y la casuística relacionados con la privacidad.

El avance tecnológico, por otra parte, ha constatado la obsolescencia de concepcio-

nes y marcos normativos previos a la extensión, práctica universalización de fenómenos como la digitalización, la movilidad y la interactividad. La persistencia de muchos de esos requisitos y cautelas legales *pre* ha devenido en al menos dos fenómenos nocivos: por una parte, la emergencia de *negocios* desarrollados al margen o en los contornos de la legalidad establecida, con la consecuente inseguridad para los usuarios, pero también para los propios titulares de esos negocios, y, derivado de ello, una situación de asimetría competitiva entre los voluntaria u obligadamente sometidos a marcos desactualizados y los demás.

La regulación que necesariamente viene es, por tanto, clave sustancial para al menos tres aspectos: afrontar la nueva realidad que supone la extensión masiva del uso y el acceso a Internet; establecer un equilibrio entre obligaciones, requisitos y *costes* –del lado de agentes y usuarios– y capacidad efectiva de desarrollar nuevos negocios, herramientas, aplicaciones, servicios y utilidades que favorezcan el desarrollo económico y el bienestar; y, en tercer lugar, establecer un marco armonizado, libre de asimetrías, garante de la seguridad jurídica de todos y libre de actuar como ingrediente anticompetitivo que distorsione el posicionamiento de unos u otros en el concierto global.

Los pormenores más destacados del proceso europeo de revisión normativa, así como las asimetrías *heredadas* de marcos precedentes respecto a EE. UU., constituyen la materia abordada en el capítulo 2.

Jorge Pérez Martínez

Doctor ingeniero de Telecomunicación por la Universidad Politécnica de Madrid y licenciado en Ciencias Políticas y Sociología por la Universidad Complutense. Es catedrático de la ETSI de Telecomunicación de la UPM desde 1990, donde imparte docencia e investigación en materias relacionadas con los aspectos socioeconómicos de las tecnologías de la información y las comunicaciones, y política y regulación de las telecomunicaciones. De junio de 1990 a febrero de 1999 fue decano del Colegio Oficial de Ingenieros de Telecomunicación. En la actualidad es miembro de su Consejo de Colegio. De septiembre de 2003 a junio de 2004 fue director general para el desarrollo de la Sociedad de la Información en el Ministerio de Ciencia y Tecnología y consejero de los Consejos de Administración del CDTI y de la Entidad Pública Empresarial RED.ES. Actualmente es director de la Cátedra Red.es en la Universidad Politécnica de Madrid, donde coordina el Grupo de Análisis y Prospectiva del sector de las Telecomunicaciones (GAPTEL). Es asesor del secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, y coordinador del Grupo de Alto Nivel de la Agenda Digital para España. Es, asimismo, coordinador del Foro de Gobernanza de Internet en España (IGF España).

Arturo Vergara Pardillo

Doctor ingeniero de Telecomunicación por la Universidad Politécnica de Madrid en 2011, ingeniero de Telecomunicación por la UPM en el año 2006 y especialista universitario de Economía de las Telecomunicaciones por la UNED en el año 2008. Desde el año 2007 al año 2011 disfrutó de una beca de Personal Investigador en la UPM para el desarrollo de su tesis doctoral centrada en la problemática del despliegue de las redes de acceso de próxima generación (NGA). Durante su etapa de investigación ha formado parte del equipo de trabajo del *think-tank* GAPTEL (Grupo de Análisis y Prospectiva del sector de las Telecomunicaciones), ha participado en la elaboración de diferentes informes para la Administración pública, así como en la elaboración de diversos libros, artículos y ponencias científico-técnicas. Desde 2012 es consultor para la Cátedra Red.es y se incorpora al equipo de trabajo de la Agenda Digital para España en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Asimismo, es miembro del Grupo de Regulación y de Políticas Públicas del Colegio Oficial de Ingenieros de Telecomunicación y del Foro de Gobernanza de Internet en España, donde colabora activamente.

2. Modelos reguladores de protección de datos para una era global

Jorge Pérez Martínez
Catedrático de la Universidad Politécnica de Madrid (UPM)

Arturo Vergara Pardillo
Investigador y consultor

2.1 Introducción

En la última década el número de usuarios de Internet, la proliferación de ordenadores y *smartphones*, la extensión de la banda ancha móvil, así como el uso de servicios de *cloud computing*, comercio electrónico, redes sociales y otros servicios web ha experimentado un crecimiento exponencial. Estos elementos han generado importantes beneficios económicos y sociales, incorporándose como parte fundamental de la vida diaria de los ciudadanos y permitiendo una mayor capacidad de comunicación, colaboración y compartición.

Al mismo tiempo, la evolución tecnológica ha incrementado la capacidad de recogida, uso y almacenamiento de datos personales por motivos de eficiencia, comerciales o de seguridad por parte de múltiples agentes públicos y privados. Este proceso tiene lugar en un entorno abierto y global, donde se difuminan las barreras territoriales y los sistemas legales que regulan la privacidad y el intercambio de los datos personales. Si bien la legislación vigente en Europa permite manejar ciertas problemáticas derivadas del tratamiento de datos personales, los avances tecnológicos y el mayor impacto de una Internet global generan incertidumbres en los consumidores y empresas sobre sus derechos, obligaciones y protecciones legales.

Desde una perspectiva de negocio, el libre intercambio de información resulta esencial para la economía digital actual. Cada vez más, las empresas emplean el tratamiento de datos personales como fuente de su inteligencia corporativa, fomentando la innovación empresarial, técnica y de servicios. Si estas nuevas prácticas no se realizan bajo un marco legislativo robusto y flexible que permita garantizar los derechos de los usuarios y la innovación, la confianza de los consumidores se podrá ver resentida, impactando negativamente en la adopción de nuevos servicios. El desarrollo del Mercado Único Digital, y el potencial impulso a la innovación, el emprendimiento y la creación de empleo, requerirán del firme compromiso de las empresas, los reguladores y los usuarios, situando la protección de la privacidad y los datos personales como un elemento clave.

Este capítulo presenta la situación actual de los marcos reguladores en la UE y EE. UU., y analiza la evolución de los debates, iniciativas y revisiones de la regulación en ambas regiones. Posteriormente se plantea, desde un enfoque global, diferentes mecanismos globalizados para alcanzar una regulación de privacidad y de protección de datos efectiva, así como el impacto de la propuesta de la Comisión Europea realizada a principios de 2012. El capítulo se completa con un conjunto de contribuciones de académicos y expertos al debate de la privacidad.

2.2 El modelo de protección de datos en Europa

Una de las primeras referencias modernas al derecho a la privacidad puede hallarse específicamente en el Artículo 12 de la Declaración de Derechos Humanos de 1948, referido a la privacidad territorial y de las comunicaciones de los individuos. Otros tratados internacionales posteriores, como el Pacto Internacional de Derechos Civiles y Políticos de 1966, la Convención de los Derechos del Niño de 1990, o la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familias de 1990, reconocen específicamente el derecho a la privacidad en términos similares.

Algunos de los derechos mencionados fueron legalmente exigibles a través de tratados a nivel regional, como el Artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950, o posteriormente en los Artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea del año 2000, que con la entrada en vigor del Tratado de Lisboa en 2009 hizo legalmente vinculante la Carta para todos los países, excepto Polonia y el Reino Unido.

De esta forma, el derecho a la privacidad está considerado en Europa como una parte integral del derecho al respeto de la vida privada, incorporando, asimismo, el derecho a la protección de datos de carácter personal[8]. Este derecho no solo se refiere a la protección de los individuos frente a intrusiones a la privacidad de sus vidas, sino que establece que los datos concernientes a una persona deben necesariamente ser procesados de manera leal, y sobre la base del consentimiento o de otro fundamento legítimo previsto por ley, que toda persona tiene derecho a acceder y rectificar los datos recogidos que la conciernan, y que el cumplimiento de estas normas debe estar sujeto al control de una autoridad independiente.

Asimismo, este derecho se menciona en las constituciones de varios Estados miembros, como es el caso de España, y que se presentará con mayor detalle en la contribución del profesor Ricard Martínez, o reconocido a través de sentencias de tribunales constitucionales, como en el caso de Alemania[9]. De esta forma, la defensa de la privacidad y la protección de los datos de carácter personal es percibida como un derecho fundamental que el gobierno debe proveer a los ciudadanos.

La sólida percepción europea del derecho a la privacidad se ha cimentado mediante el desarrollo de un marco legislativo en varios niveles, encabezado por la Directiva de protección de datos de 1995, y la Directiva sobre la privacidad y las comunicaciones electrónicas, así como leyes integrales y sectoriales nacionales. Asimismo, se han establecido en Europa las agencias nacionales de protección de datos, encargadas de la vigilancia y la defensa de los derechos de protección de datos. Este marco legislativo, junto con la consideración del dere-

8. Se entiende por «datos de carácter personal» toda información referente a su persona que le pueda identificar directa o indirectamente, por ejemplo su nombre, número de teléfono, correo electrónico, lugar y fecha de nacimiento, etcétera.
9. En 1983, el Tribunal Constitucional Federal alemán reconoció el derecho individual a la autodeterminación de la información, según el cual, los individuos deben tener garantizada la capacidad para determinar el grado de apertura y el uso de sus datos personales.

cho a la privacidad y a la protección de datos como derecho fundamental, han situado a Europa como líder en derecho a la privacidad.

Sin embargo, la implementación del marco de 1995 no ha estado exenta de problemáticas y limitaciones en el proceso de armonización europea. Dichas limitaciones y la necesidad de adaptar el marco a los nuevos retos planteados por el avance tecnológico y la globalización llevaron a Europa a iniciar, en 2007, un profundo debate sobre la revisión de la legislación en materia de protección de datos. A principios de 2012 el proceso de revisión alcanzó un punto clave, con la publicación de la propuesta por parte de la Comisión de un nuevo marco legislativo, cuyo posterior debate y aprobación permitirán a Europa avanzar en la protección de la privacidad y de los datos personales.

2.2.1 Marco legislativo

El modelo legislativo de protección de datos personales en Europa se basa principalmente en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (denominada Directiva de protección de datos), que armoniza las legislaciones nacionales que exigen unas prácticas de gestión de datos de alta calidad a los responsables del tratamiento de datos, y la garantía de una serie de derechos a las personas físicas. Este marco regula el tratamiento de los datos personales dentro de los Estados miembros, excluyendo las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y a las actividades del Estado en materia penal. A modo de referencia, se ha incluido en los anexos un resumen de las principales disposiciones en términos de derechos y obligaciones existentes en la Directiva de protección de datos.

Esta directiva, de carácter general, se completa con la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, de 12 de julio de 2002, que garantiza el tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas. Esta directiva fue actualizada en 2009 para incluir, entre otros aspectos, el concepto de brecha de datos o violación de los datos personales. En su contribución, Alexander Alvaro, vicepresidente del Parlamento Europeo, realiza una descripción más amplia del efecto de dicha revisión. Además, se ha incluido en los anexos un breve resumen de las principales disposiciones introducidas por la directiva sobre la privacidad y las comunicaciones electrónicas.

Asimismo, el marco general europeo incluye el Reglamento 45/2001 de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios, y la Decisión Marco 2008/977/JAI del Consejo de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Las directivas, reglamentos y decisiones anteriores conforman el marco jurídico general a nivel comunitario que los distintos Estados miembros tienen obligación de incorporar en sus legislaciones nacionales mediante la transposición de aquellas. Asimismo, en virtud de lo dispuesto en la Directiva de protección de datos, se exige a los Estados miembros el establecimiento de autoridades nacionales independientes, dotadas de poderes de investigación y de intervención, para que vigilen la aplicación de sus disposiciones.

2.2.2 La revisión del modelo regulador de protección de datos

La revisión formal del marco legislativo de protección de datos, iniciada en 2007, responde a la necesidad de alcanzar una verdadera armonización de la normativa de protección de datos en Europa, así como de afrontar las problemáticas de privacidad generadas por la aparición y uso de nuevas tecnologías, en especial a

través de Internet. El proceso ha ido evolucionando a lo largo de varios años, y ha necesitado de varias etapas de consulta pública hasta alcanzar una propuesta formal de la Comisión, que continuará siendo debatida por el Parlamento y el Consejo en el marco del proceso legislativo ordinario de la Unión Europea.

La falta de armonización de las leyes nacionales

El proceso de transposición al Derecho nacional de la Directiva de protección de datos fue supervisado por la Comisión Europea mediante informes de seguimiento en 2003[10] y en 2007[11]. Estos informes pusieron de manifiesto la falta de armonización entre las implementaciones realizadas por los diferentes Estados miembros. Pese a que todos ellos habían realizado la transposición de la Directiva, algunos no habían incorporado todas las provisiones, mientras que en otros casos las legislaciones nacionales no se había realizado con arreglo a aquella.

Asimismo, como reconoció el propio supervisor europeo de Protección de Datos[12], la Directiva contiene provisiones formuladas genéricamente, dejando cuestiones abiertas que dan lugar a implementaciones divergentes, elemento que ha facilitado la actual falta de armonización en Europa. Un informe encargado por la Comisión Europea en 2008[13] analizó las divergencias generadas en el derecho nacional de protección de datos señalando discrepancias considerables en la aplicación de las leyes, que podían generar un impacto muy serio en términos de mercado interior.

Esta circunstancia ha dificultado y limitado procesos de simplificación, autorregulación o normas empresariales que pudiesen derivar en una mayor agilidad y reducción de los costes para las empresas, lo que ha impedido en gran medida el desarrollo de un verdadero mercado interior. Esto ha resultado crítico para aquellas empresas que operan en varios Estados, al incurrir en mayores costes y retraso en las operaciones derivados del cumplimiento de las diferentes obligaciones legales (en muchos casos divergentes) propias de cada país. Además, esta situación dificulta la transferencia de datos personales entre distintas sedes europeas, y puede generar conflictos de validez y supremacía entre leyes nacionales y europeas.

Asimismo, las profundas divergencias en la normativa de protección de datos en el mercado internacional suponen una desventaja competitiva para las empresas europeas, especialmente en lo referido al entorno del ecosistema de Internet, donde existe una fuerte competencia con empresas de regiones como EE. UU., cuyos marcos normativos son menos restrictivos que el europeo.

De esta forma, la mejora en la armonización europea se situó como uno de los principales objetivos de la revisión del marco legislativo de protección de datos. Este deberá permitir alcanzar unas reglas de juego homogéneas para todos los agentes involucrados,

10. European Commission. Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/EC). COM(2003) 265 final.
11. European Commission. Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. COM(2007) 87 final.
12. Ver párrafo 52 de European Data Protection Supervisor. Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - «A comprehensive approach on personal data protection in the European Union». Disponible en: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf
13. Es destacable el informe European Commission. Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, desarrollado entre octubre de 2008 y agosto de 2009, en el que se identifican los principales retos a la protección de datos generados por los nuevos fenómenos tecnológicos y sociales. El informe realiza, asimismo, un análisis comparado de las respuestas que ofrecen distintos sistemas basados o no en marcos reguladores (dentro y fuera de la UE) a dichos retos. El informe está disponible en: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

independientemente de su localización geográfica o del sector económico donde desarrollen su actividad, incluyendo a los agentes que prestan servicios *online* en la UE, estén o no localizados en territorio europeo. Solo mediante dicha armonización y tratamiento equivalente para todos los responsables de los tratamientos de los datos personales se podrán reforzar los derechos y la confianza de los individuos sin que se produzca un impacto negativo en la competitividad de las empresas y negocios europeos.

El proceso de revisión del Marco 2007-2010

Si bien la Comisión consideró en 2007 que la Directiva de protección de datos constituía un marco jurídico general que cumplía con sus objetivos originales, asegurando un alto nivel de protección, también reconoció que la evolución tecnológica y el creciente uso e importancia de los datos personales en Internet requerirían de iniciativas, legislativas o no legislativas, para hacer frente a los nuevos retos. Asimismo, había quedado patente la necesidad de una mayor armonización para la construcción de un verdadero mercado interior.

De esta forma, la Comisión Europea inició un proceso de debate sobre la necesidad de revisar el marco general de protección de datos para hacer frente a los nuevos retos derivados del avance tecnológico y la globalización, para reforzar los derechos individuales, disminuir la carga administrativa, así como mejorar la claridad y coherencia de las medidas implementadas. Este debate incluyó la realización de informes específicos para identificar los nuevos retos[14], conferencias de alto nivel para debatir las distintas posiciones, y la publicación de una Comunicación de la Comisión en 2009[15]. Las diferentes iniciativas ponían de manifiesto que, si bien la protección de datos en la UE podía y debía continuar basada en los principios y criterios planteados por la Directiva de protección de datos, la aplicación de dichos principios necesitaba ser clarificada y mejorada en relación con los nuevos retos.

La entrada en vigor del Tratado de Lisboa en el 2009 supuso el fin de la división del espacio europeo en tres pilares, dotando a la UE de personalidad legal propia. Asimismo, supuso la vinculación legal de la Carta de Derechos Fundamentales, cuyos Artículos 7 y 8 reconocen el derecho a la privacidad y a la protección de datos. Estas dos circunstancias impulsaron la realización de una consulta pública en el 2009[16] sobre la capacidad del marco legislativo para hacer frente a los nuevos retos y, en su caso, la necesidad de realizar reformas en las Directivas o de implementar nuevos sistemas o procedimientos.

El resultado de la consulta[17] puso de manifiesto la existencia de diferentes problemáticas y retos percibidos por ciudadanos, empresas, organizaciones y administraciones. Muchas respuestas manifestaron la necesidad de actualizar o delimitar los distintos roles y definiciones dispuestos en las Directivas para su aplicación a los nuevos casos de uso, tales como el *cloud computing*, la identificación biométrica, las tecnologías de identificación por radiofrecuencia (RFID, del inglés *Radio Frecuency IDentification*), las tecnologías de vigi-

14. Ver nota 6.
15. En European Commission. Communication from the Commission to the European Parliament and the Council. An area of freedom, security and justice serving the citizen. COM (2009) 262; se presentan, entre otros elementos, las líneas principales de la actuación futura de la Comisión Europea en términos de Protección de datos. Dichas líneas están centradas en: el desarrollo de tecnologías para preservar la protección de datos, la introducción de mecanismos de certificación europea de tecnologías, los productos y servicios respetuosos con la privacidad, la realización de campañas de información y sensibilización, y el papel central de Europa en la promoción de normas internacionales en materia de protección de datos personales.
16. Disponible en: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm
17. Disponible en: http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf

lancia o las redes sociales. En relación con el coste de cumplimiento de las Directivas, las empresas manifestaron el impacto negativo sobre la competitividad generado por la sobreprescripción de aquellas, solicitando un mayor equilibrio entre el derecho a la protección de datos con otros principios como el derecho a la propiedad o a la libertad de actividades económicas, una disminución de las cargas relacionadas con las obligaciones de notificación y de comprobación previa, la agilización de los trámites para los casos en los que se produzca la subcontratación del tratamiento de datos, así como una mayor homogenización del mercado interior.

Asimismo, en relación con los retos asociados a la globalización y a las transferencias transfronterizas, destacaron la necesidad de armonizar el marco europeo al entorno global e implementar mecanismos más ágiles como códigos de buenas prácticas, estándares, cadenas de responsabilidad o autorregulación, mitigando la necesidad de disponer de una decisión favorable de la Comisión que involucre a sectores o países enteros. Por su parte, los agentes afectados por la Directiva sobre la privacidad y las comunicaciones electrónicas solicitaron que en aquellos casos en que solo se realicen funciones de transporte, y no de tratamiento de datos personales, únicamente estén obligados a cumplir con los requisitos de seguridad y confidencialidad.

El debate iniciado sobre la revisión del marco legislativo de privacidad y protección de datos continuó con la realización de reuniones de consulta entre la Comisión Europea y agentes públicos (Agencias Nacionales de Protección de Datos) y privados[18] en julio de 2010, llevando a la publicación, en noviembre del mismo año, de una nueva Comunicación.

La consulta pública de 2010

La Comunicación de 2010[19] «Un enfoque global de la protección de los datos personales en la Unión Europea» planteó las cinco líneas maestras[20] que impulsarían la revisión del Marco regulador. Estas líneas maestras se utilizaron como base para una consulta pública[21] que dio lugar a una amplia respuesta por parte de empresas, asociaciones, administraciones públicas y ciudadanos. El proceso de consulta pública permitió definir mejor los elementos de consenso y disenso en relación con la revisión de la normativa de protección de datos.

La necesidad de una mayor armonización del mercado interior, limitando las diferencias entre los distintos Estados miembros, se situó como uno de los principales consensos alcanzados. En este sentido, las principales demandas se centraron en: a) la clarificación sobre las leyes aplicables en los casos de transferencia de datos entre varios países de la Unión Europea; b) la clarificación en el caso de empresas no establecidas en Europa que prestan servicios dentro de su territorio, y c) la reducción de los costes y trabas administrativas asociadas a los procesos de transferencia de datos personales y de notificación.

El consenso alcanzado en estos aspectos respaldaba la opinión del Grupo de Trabajo del Artículo 29 (GT29)[22] que establece un criterio

18. Consulta disponible en: http://ec.europa.eu/justice/news/events/data_protection_regulatory_framework/background_paper_en.pdf
19. European Commission. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union. COM(2010) 609 final.
20. Las cinco líneas en las que la Comisión organizó la revisión fueron: a) refuerzo de los derechos de los usuarios, incluyendo la adaptación de las normas al contexto del avance tecnológico, una mayor transparencia y un mayor control de los datos por parte de los usuarios; b) la mejora del mercado interior, centrada en la disminución de las divergencias, fomentar menores cargas administrativas, clarificación del derecho aplicable, el refuerzo de la responsabilidad de los agentes y un mayor papel de los mecanismos de autorregulación; c) la ampliación de las normas generales de protección de datos a los ámbitos de la cooperación policial y judicial en materia penal dada la supresión de la estructura de pilares de la UE; d) la simplificación de los criterios para la transferencia de datos personales en el ámbito internacional, y e) la mejora del marco institucional.
21. Información disponible en: http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm
22. Dictamen 8/2010 del Grupo del Artículo 29.

de «país de origen» para aquellas empresas con base en Europa, de forma que una empresa que opere en diversos mercados nacionales deberá estar sometida únicamente a la legislación del país donde esté establecida, en lugar de a todas las legislaciones de los mercados donde opera. Mientras, en el caso de empresas no establecidas en Europa, el consenso alcanzado solicitaba la aplicación de la legislación de aquellos Estados miembros a los que dirijan específicamente sus servicios, ofreciendo a todos los ciudadanos europeos los mismos niveles de protección independientemente de la localización de su proveedor de servicios.

Asimismo, varias de las respuestas a la consulta incidieron sobre la necesidad de reducir la divergencia de obligaciones y protecciones dispuestas en función de los sectores específicos. Concretamente, la Directiva sobre la privacidad y las comunicaciones electrónicas impone mayores requisitos y salvaguardas a los datos personales empleados por el sector de las telecomunicaciones, así como sobre los datos de tráfico y localización. Dichas respuestas[23] pusieron de manifiesto la necesidad de avanzar hacia una armonización sectorial. Asimismo, se alcanzó un amplio consenso sobre la necesidad de mantener el carácter de neutralidad tecnológica en la Directiva de protección de datos, ya que de lo contrario no se podría asegurar que la norma será lo suficientemente flexible para adaptarse a futuros avances tecnológicos.

Por otra parte, la consulta pública puso de manifiesto la existencia de posiciones más diferenciadas en cuanto a la aplicación de mecanismos de flexibilización de la regulación, como el paso de un modelo prescriptivo a uno más pragmático y orientado a objetivos, la orientación de la regulación hacia un modelo basado en la responsabilidad, o la aplicación más flexible de las obligaciones de transparencia y de los mecanismos de consentimiento. Estos elementos han sido planteados en el entorno internacional como posibles vías para la convergencia de los distintos marcos normativos, y se presentan con más detalle en el apartado 2.4.

Finalmente, otros elementos más concretos que generaron posiciones diferenciadas son la aplicación de mecanismos de autorregulación, que si bien son ampliamente aceptados, generan posiciones diferenciadas sobre la necesidad de que tengan un carácter vinculante o no[24]; así como el «derecho al olvido» propuesto por la Comisión, que ha sido considerado por múltiples agentes[25] como un derecho ya implícito en los derechos de supresión, rectificación y cancelación, y cuya principal problemática para la puesta en funcionamiento es la necesidad de una mayor armonización y la persecución de su cumplimiento. La problemática del derecho al olvido se trata de forma exhaustiva en la contribución realizada por Hans Graux, Jef Ausloos y Peggy Valcke.

Actuaciones posteriores

A partir de las respuestas a la consulta pública de 2010 y de los consensos alcanzados entre los distintos agentes, la Comisión Europea comenzó el largo proceso de preparación de la propuesta de nuevo marco que no finalizaría hasta principios de 2012.

Durante ese proceso, la Comisión Europea realizó otras dos consultas públicas sobre las problemáticas de privacidad en el ámbito de

23. ETNO, Telefónica, Nokia, GSMA Europe y FTC, entre otros.
24. En este sentido, las principales empresas como Nokia, Microsoft o consorcios de empresas se han manifestado a favor de una autorregulación y de la introducción de certificaciones no vinculantes de base voluntaria, otras empresas como HP, e instituciones o asociaciones como la AEPD o la European Privacy Association han manifestado la necesidad de que la autorregulación sea vinculante y pueda estar sometida a sistemas de control de cumplimiento.
25. Por ejemplo, Telefónica, ETNO, Nokia, GSMA Europe, la AEPD, la European-American Business Council o Ebay.

las comunicaciones electrónicas y del *cloud computing*. La primera de ellas relacionada con el desarrollo del *cloud computing* en Europa[26], en la que se preguntó a los agentes interesados sobre las problemáticas y barreras relacionadas con la protección de datos y la privacidad. Mientras, en segundo lugar, la realizada en julio de 2011 para revisar las circunstancias, los procedimientos y los formatos de las notificaciones requeridas por la Directiva sobre la privacidad y las comunicaciones electrónicas en el caso de brechas de seguridad[27].

2.2.3 La propuesta de la Comisión Europea

Finalmente, la nueva propuesta de marco regulador que plantea sustituir a la Directiva de protección de datos de 1995 fue publicada por la Comisión Europea el 25 de enero de 2012. Dicha propuesta inicia el proceso legislativo ordinario por el que el Parlamento, el Consejo y la Comisión avanzarán hacia la configuración del nuevo marco europeo de protección de datos que entrará en vigor entre 2015 y 2016. Es ahora cuando Europa se enfrenta al desafío de alcanzar un marco lo suficientemente robusto como para garantizar de una forma eficaz el derecho a la privacidad en las próximas décadas y lo suficientemente flexible como para hacerlo minimizando las trabas y las cargas a la innovación y el desarrollo.

El marco planteado por la Comisión, presentado en detalle en la contribución de la comisaria Reding que abre este libro, se compone de un reglamento para la protección de los individuos en relación con el tratamiento de sus datos personales y el libre movimiento de dichos datos (conocido como Reglamento general de protección de datos), y que reemplazaba a la Directiva 95/46/EC, y de una directiva de protección de datos en los ámbitos de la cooperación policial y judicial en materia penal, que reemplazaba la Decisión Marco 2008/977/JHA. Este nuevo marco para la protección de datos introduce dos cambios significativos de manera inmediata.

En primer lugar, la utilización de un reglamento en lugar de una directiva como instrumento legal para definir las reglas relativas a la protección de datos. A diferencia de las directivas, cuya función prescriptiva debe ser transpuesta en cada uno de los Estados miembros a su propia legislación nacional, dando por tanto lugar a posibles divergencias entre la implementación realizada por distintos países, el reglamento supone la forma más directa de Ley en la UE, al ser directamente vinculante en los distintos Estados miembros. Una vez que un reglamento es aprobado, pasa a ser parte de los sistemas legales de los distintos países, asegurando la armonización del marco regulador de la privacidad y la protección de datos.

En segundo lugar, la existencia de una directiva que permite armonizar el tratamiento de los datos personales en materia de investigación policial y judicial por primera vez tras el cambio generado por la entrada en vigor del Artículo 16 del Tratado de Lisboa, facilitando así el trabajo policial y la lucha contra el crimen.

Las principales modificaciones que plantea la Comisión Europea han sido presentadas en la contribución de la comisaria Reding. Asimismo, la contribución de la europarlamentaria Pilar del Castillo, y de los académicos Hans Graux, Jef Ausloos y Peggy Valcke, amplían el análisis de la propuesta de la Comisión. Finalmente, se ha incluido en los anexos un resumen de los principales elementos que incorpora la propuesta de la Comisión, así como el

26. Consulta realizada sobre las líneas presentadas por la comisaria Neelie Kroes el 27 de enero de 2011 titulado «Towards a European Cloud Computing Strategy». Disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50
27. European Commission. ePrivacy Directive: circumstances, procedures and formats for personal data breach notifications. Public consultations. Disponible en: http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/data_breach/index_en.htm

texto legislativo de la propuesta de Artículo 17, que regula el derecho al olvido.

2.3 El modelo de protección de datos en Estados Unidos

La privacidad y la protección de datos en EE. UU. no son percibidas como un derecho fundamental, como en el caso de la Unión Europea, sino como una problemática de defensa de la competencia y de defensa de los derechos de los consumidores. A diferencia de la UE, donde el derecho a la privacidad es recogido en diversos tratados, manifiestos y las constituciones de algunos Estados miembros, en EE. UU. dichos conceptos no están presentes directamente en la constitución, sino que se ha seguido un enfoque *laissez faire*, más reactivo, con el que se ha dado prioridad al rol de los actores privados y de las fuerzas de mercado.

El derecho a la privacidad se ha desarrollado en EE. UU. mediante una combinación de la actuación del poder judicial y el legislativo. En unos casos los tribunales son los que interpretan y definen nuevos derechos de privacidad, mientras que en otros casos la iniciativa parte del poder legislativo. Algunos ejemplos de casos judiciales que han supuesto avances relevantes del derecho a la privacidad son: el caso Griswold vs. Connecticut en 1965, en el que el Tribunal Supremo reconoció una «zona de privacidad» generada por la conjunción de la Primera, Cuarta[28], Quinta y Novena Enmiendas; o el caso Whalen vs. Roe en 1977, que reconoció el derecho constitucional a la privacidad de la información.

A nivel federal, la privacidad y la protección de datos en EE. UU. están recogidas mediante legislación sectorial. Existen diferentes estatutos que regulan las prácticas públicas y privadas sin que exista una ley específica sobre protección de datos. Por su parte, la Comisión Federal de Comercio (FTC)[29], órgano regulador de competencia, impulsa la autorregulación y las tecnologías de protección de la privacidad como principal vía de actuación.

Mientras que, a nivel estatal[30], se desarrolla la regulación de protección al consumidor, segundo pilar en el que descansa la legislación sobre privacidad en EE. UU. Estos, al igual que el gobierno federal, tratan la problemática desde una perspectiva sectorial en lugar de mediante leyes integrales. Las disposiciones federales representan las protecciones mínimas que los Estados pueden reforzar, dando lugar a divergencias significativas entre Estados en algunos casos, así como a situaciones en las que sectores industriales han acudido al Congreso para tratar de limitar leyes estatales más restrictivas.

La diversidad de agentes implicados (a nivel federal intervienen los poderes legislativo, judicial y ejecutivo, así como la intervención a nivel estatal), junto con las divergencias generadas por el modelo sectorial, dificultan que el marco legislativo estadounidense encaje en el paradigma de protección de datos europeo, así como la existencia de un enfoque cohesionado para las leyes sobre privacidad. El modelo de privacidad en EE. UU. es analizado en profundidad por el doctor Paul M. Schwartz y por Alan Charles Raul en las contribuciones realizadas a este monográfico. Para el primero, el modelo resulta «limitado y a veces incoherente», al existir elementos o sectores no cubiertos que requieren la intervención de la FTC, mientras que para el segundo, la existen-

28. La Cuarta Enmienda protege a los individuos que tienen unas expectativas razonables de privacidad. El Tribunal Supremo ha interpretado que dicha regla no proporciona protección cuando los individuos comparten información con terceras partes. Ver Stephen Henderson, «Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search» (2010) 55 Catholic University Law Review, disponible en: http://works.bepress.com/cgi/viewcontent.cgi?article=1002&context=stephen_henderson

29. Autoridad reguladora de competencia en EE. UU.

30. «... the protection of a person's general right to privacy – his right to be let alone by other people – is like the protection of his property and of his very life, left largely to the law of the individual States.» Katz v. United States, 389 U.S. 347 (1967).

cia de múltiples agentes genera mayores equilibrios y garantías de protección. En ambos casos coinciden en que el enfoque de EE. UU. es, en general, menos prescriptivo que el modelo europeo, generando menores cargas y trabas a las empresas para el tratamiento de datos personales y siendo más permisivo con la innovación.

2.3.1 Marco legislativo

Como se ha puesto de manifiesto, en EE. UU. se tienen diferentes nociones de derecho a la privacidad, que incluyen desde el aislamiento físico, la privacidad de las decisiones y la privacidad de la información. Este amplio rango de intereses, combinado con el enfoque sectorial, genera que las cuestiones sobre privacidad se basen en leyes constitucionales, leyes estatales, derecho común, agencias reguladoras, principios de autorregulación y normas sociales, sin que exista una definición coherente de los derechos de privacidad[31].

A continuación se presentan brevemente las principales leyes federales y estatales relacionadas con la privacidad, así como los mecanismos de privacidad desarrollados por la Comisión Federal de Comercio, que en su conjunto conforman el marco legislativo aplicable en EE. UU.[32]

Legislación federal

En la legislación federal los derechos de privacidad y de protección de datos se encuentran repartidos en el código criminal, código civil, en el derecho probatorio, el derecho de familia, el derecho real, los contratos y la regulación de la administración. No se ha desarrollado ninguna ley que trate de unificar los distintos intereses en los diversos contextos en los que se utiliza el concepto de privacidad.

Si bien la Constitución no reconoce explícitamente el derecho a la privacidad, las distintas enmiendas reconocen elementos parciales. Los más relevantes son: a) el derecho a hablar anónimamente recogido en la Primera Enmienda; b) el derecho a la libre asociación reconocido en la Primera Enmienda; c) la prohibición del alojamiento de soldados en casas privadas sin el consentimiento del propietario en tiempos de paz, reconocido en la Tercera Enmienda; d) la razonable expectación de privacidad de la Cuarta Enmienda; y e), el privilegio contra la autoinculpación de la Quinta Enmienda. La interpretación de dichos derechos ha derivado en el reconocimiento del derecho a la privacidad y a la privacidad de la información.

Por su parte, el Congreso ha creado diversas leyes relativas a la recopilación, el tratamiento y la publicación de información y de datos personales. La principal ley que regula la recogida, el uso y la publicación de datos personales es la Privacy Act de 1974, que implementó varios de los elementos de las Directivas de la Organización para la Cooperación y el Desarrollo Económicos (OCDE). Asimismo, se han desarrollado leyes sectoriales relacionadas con la privacidad de datos financieros, registros médicos, privacidad de las comunicaciones, o de datos relacionados con el entorno laboral. Una revisión de la legislación federal puede encontrarse en el artículo realizado por Alan Charles Raul, disponible en el apartado 3.3.

Legislación estatal

Gran parte de la legislación sobre privacidad se ha desarrollado a nivel estatal, ya sea mediante reconocimiento en las constituciones estatales, como por ejemplo ocurre en el estado de California; mediante derecho de res-

31. Ver Daniel J. Solove, «Conceptualizing Privacy» (2002) 90 California Law Review 1087, y Daniel J. Solove, «A Taxonomy of Privacy» (2006) 154 U. Penn. L. Rev 477.

32. Como guía de referencia para la consulta de la legislación estadounidense se recomienda consultar Daniel J. Solove and Paul M. Schwartz, Privacy Law Fundamentals (International Association of Privacy Professionals 2011).

ponsabilidad civil, que reconoce en algunos estados las problemáticas de invasión de la privacidad o las violaciones de la confidencialidad[33], o mediante leyes específicas.

La legislación estatal puede diferir de los requisitos de la legislación federal, y en ocasiones es más restrictiva que esta. En general, la legislación federal reemplaza a la estatal en aquellos puntos en los que la estatal es contraria a la federal. Cualquier disposición que no sea contraria a la regla federal permanece vigente y debe ser aplicada en dicho estado.

Este enfoque permite la divergencia legislativa entre diferentes estados. Un ejemplo claro de esta situación es el estado de California, donde se han aprobado múltiples leyes relativas a la protección de datos, motivadas en muchos casos por la reacción pública ante prácticas específicas de empresas o administraciones.

Algunos ejemplos son: a) la obligación de los sitios web de presentar las políticas de privacidad empleadas; b) la restricción sobre los datos personales publicados de empleados públicos; c) restricciones a determinadas prácticas comerciales o de marketing, tales como la solicitud de documentación para inscribirse en promociones comerciales o el requisito de consentimiento escrito para publicar los datos telefónicos en las guías telefónicas; d) mayores derechos para las víctimas de robo de identidad; e) mayores derechos en relación con la protección de datos financieros que los garantizados por las disposiciones federales, permitiendo por ejemplo bloquear el acceso de nuevos proveedores de crédito a la información fiscal de un consumidor; f) requisitos de eliminación de registros de datos personales en diversos contextos; o g) el desarrollo de leyes anti-*paparazzi* prohibiendo la invasión de la privacidad y el uso de tecnologías para obtener imágenes o sonidos que no podrían ser capturados sin un traspaso físico.

Regulación de competencia

El tercer elemento que cabe considerar en la regulación sobre privacidad y protección de datos es la Comisión Federal de Comercio, que ha desarrollado un papel relevante en la aplicación de las leyes y disposiciones sobre privacidad. A través de la autoridad que le confiere la sección 5 del FTC Act, la Comisión ha desarrollado labores de autoridad para el cumplimiento de diferentes leyes federales, de defensa de la competencia y de los consumidores, así como estudios y labores de divulgación y formación sobre la implicación de distintas tecnologías y prácticas empresariales en la privacidad y la protección de datos.

La Comisión ha empleado principalmente dos enfoques complementarios para tratar las cuestiones sobre privacidad.

En primer lugar, la Comisión impulsó desde mediados de la década de los noventa un conjunto de iniciativas de autorregulación para fomentar la implantación de principios para una justa información de las prácticas realizadas relativas a la privacidad de los datos personales[34]. Dichas iniciativas se basan en la aplicación de los conceptos de transparencia, responsabilidad y de autonomía de los consumidores. Una descripción en profundidad de los *Fair Information Practice Principles* puede encontrarse en el artículo de Paul M. Schwartz en el apartado 3.2.

La efectividad de las medidas de autorregulación fue evaluada en el año 2000[35], y mostró que únicamente una de cada cuatro políticas de privacidad analizadas implemen-

33. Por ejemplo, 46 estados, el Distrito de Columbia, Puerto Rico y las Islas Virginias han implementado legislación que obliga a las empresas o a las agencias estatales a notificar a los consumidores la existencia de brechas de seguridad que involucren datos personales.
34. Propuestas denominadas Fair Information Practice Principles.
35. Ver FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace 12-13 (2000), disponible en: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf

taba las prácticas propuestas. Esta situación motivó una propuesta de la Comisión al Congreso para hacer obligatoria la implementación de estas medidas, propuesta que no fue aceptada por la Cámara.

Como segundo enfoque, la FTC ha llevado a cabo investigaciones *ex post* en casos de perjuicio a los derechos de los consumidores o de violación de los derechos de privacidad. Algunos ejemplos de estas investigaciones son el caso de Google Buzz o de Facebook, ambas presentadas en la contribución de Paul M. Schwartz. En general los casos involucraban prácticas que fallaban[36] en: a) cumplir con las políticas de privacidad publicadas; b) tomar las medidas necesarias para defenderse de vulnerabilidades comunes; c) la eliminación de los datos personales; d) tomar las medidas necesarias para asegurar que los datos no son compartidos con terceras partes no autorizadas.

2.3.2 Revisión del modelo regulador

Problemáticas actuales

El marco regulador de privacidad y protección de datos en EE. UU. se enfrenta a diferentes problemáticas derivadas de la estructura sectorial y territorial del mismo. Las principales problemáticas son[37]:

- Infrainclusión: La posibilidad de que determinadas prácticas empresariales eviten cumplir con los requisitos de privacidad al encontrar determinados huecos en el sistema sectorial. Esto se puede producir por una interpretación forzada de las leyes o por la aparición de nuevas tecnologías que, no estando consideradas en el actual marco regulador, permiten realizar los mismos servicios y aplicaciones que otras sí incluidas en el marco.
- Sobreinclusión: Problemática que se produce cuando empresas que operan en múltiples sectores están sometidas a distintas leyes y restricciones. Asimismo, los cambios en el uso de las tecnologías pueden generar esta problemática.
- Diversidad territorial: La existencia de diferencias en el tratamiento de los datos personales entre los diferentes estados genera mayores complicaciones y costes para empresas que desarrollan su actividad económica en múltiples estados.

Asimismo, la política llevada a cabo por la FTC de autorregulación, aplicación de las leyes e investigaciones *ex post*, también presenta un conjunto de limitaciones y problemáticas:

- En relación con los principios para una justa información de las prácticas realizadas establecidos por la FTC, un informe de la propia Comisión[38] pone de manifiesto que su aplicación está sirviendo más para limitar la responsabilidad de las empresas que para informar a los usuarios. Estos se enfrentan a la dificultad de leer y entender unas políticas de privacidad cada vez más largas y complejas, teniendo que ejercer un control muy limitado de opciones sobre privacidad, muchas veces insuficientemente explicado.
- En relación con el enfoque basado en los casos de perjuicio y daño a los usuarios,

36. Consultar FTC, Protecting Consumer Privacy in an Era of Rapid Change (2010), disponible en: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf
37. European Commission, Comparative Study on different approaches to new privacy challenges, in particular in the light of technological developments. Country studies, B.1 – United States of America. (2010). Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B1_usa.pdf
38. FTC, Protecting Consumer Privacy in an Era of Rapid Change, (2010), disponible en: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

el mismo informe reconoce que las investigaciones se han centrado principalmente en situaciones en las que se ha producido un daño físico o económico, no prestando suficiente atención a otro tipo de perjuicios, como el daño al honor u otro tipo de sensibilidades.

El avance de las actividades desarrolladas a través de Internet en un entorno globalizado supone otro de los retos para el modelo de privacidad de EE. UU., ya que no existe un marco homogéneo, sino que cada empresa se ve regulada por las leyes específicas de su área de aplicación. Asimismo, la adaptación del marco regulador para cumplir con los requisitos de privacidad de las transacciones con otras regiones internacionales supone otro de los retos para el modelo estadounidense.

Revisión del marco de privacidad

La Administración del presidente Obama ha analizado el conjunto de problemáticas relacionadas con la regulación de privacidad, y publicó el pasado 23 de febrero un documento que recoge la estrategia de revisión del marco de privacidad[39]. Este documento, analizado en profundidad por Alan Charles Raul en su contribución, reafirma el compromiso del Gobierno con el modelo legislativo actual y con la capacidad del mismo para afrontar los distintos retos identificados.

Para ello propone un conjunto de líneas de actuación entre las que se incluyen el desarrollo de una carta de derechos de los consumidores, el desarrollo de códigos de autoconducta, el impulso del cumplimiento de los códigos, o la necesidad del reconocimiento mutuo de los marcos de privacidad en el contexto internacional.

2.3.3 Iniciativas actuales

Propuestas legislativas

Durante el año 2011 se han introducido en las cámaras legislativas de EE. UU. más de diez propuestas de ley relacionadas con la privacidad *online*, los derechos de los consumidores, la seguridad de los datos personales y la obtención de datos de localización, lo que indica el incremento de la preocupación política despertado por la problemática de privacidad. La siguiente tabla presenta algunas de las principales iniciativas introducidas en las Cámaras.

Entre las iniciativas planteadas destaca la denominada *Do-Not-Track Online*, propuesta por el senador del partido demócrata, Jay Rockefeller. En esta iniciativa se propone el desarrollo, por parte de la FTC, de una regulación que establezca un mecanismo estándar para permitir a los usuarios de servicios *online* (incluyendo servicios y aplicaciones móviles) indicar cuándo estos aceptan que los proveedores de dichos servicios recopilen información personal, prohibiendo dicha recopilación en caso de no ser permitida por los usuarios. La mayoría de las asociaciones defensoras de los derechos de privacidad[40] agradecieron la propuesta planteando que permite un equilibrio entre la protección de la privacidad de los usuarios de servicios *online* y las necesidades de recogida de información de las distintas empresas, facilitando la monetización de los datos personales en caso de ser este el interés de los usuarios.

Esta iniciativa fue acompañada por otra centrada específicamente en la protección de los menores. La propuesta de ley *Do Not Track Kids Act of 2011* obliga a los proveedores de servicios web, páginas web, o servicios y apli-

39. The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Disponible en: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

40. American Civil Liberties Union, Consumer Federation of America, Consumers Union, Electronic Frontier Foundation, Privacy Rights Clearinghouse, Consumer Watchdog, Consumer Action, y the Center for Digital Democracy. Información obtenida de: http://www.physorg.com/news/2011-05-privacy-groups-track-bill.html

caciones móviles, a disponer de la aprobación paterna para poder recopilar datos personales de menores de diecisiete años, y prohíbe el uso de estos datos para su cesión a terceros o para propósitos de marketing. La propuesta también plantea el desarrollo de una regulación por la FTC para que los citados proveedores permitan a los usuarios y padres el borrado de los datos personales almacenados.

Revisión de los principios empleados por la FTC

Por otra parte, la FTC ha planteado una propuesta para renovar los principios empleados en las políticas de autorregulación de privacidad, orientándola más hacia los usuarios y mejorando los aspectos negativos de las actuales directrices a partir de tres componentes principales.

- En primer lugar, la adopción de mecanismos de privacidad desde el diseño, de forma que se incorporen protecciones para una mayor privacidad en los diferentes procesos y fases del ciclo de vida del producto.
- En segundo lugar, simplificar las elecciones sobre privacidad planteadas a los usuarios a aquellas prácticas que no respondan a prácticas comúnmente aceptadas, de forma que se clarifiquen adecuadamente aquellas situaciones donde los usuarios deben tomar una decisión sobre la gestión de sus datos personales. Para facilitar la elección de los usuarios la información deberá proporcionarse de forma comprensible y uniforme.
- En tercer lugar, la Comisión insta a un incremento de la transparencia sobre las prácticas de privacidad y de protección de datos personales. Las notificaciones deberán ser claras, precisas y tener un formato estandarizado que permita su comparación, de forma que los usuarios puedan tomar decisiones correctamente informados.

Estas medidas se completan mediante un mayor impulso a las iniciativas de educación y concienciación de los usuarios sobre las prácticas comerciales de recogida y uso de datos personales, facilitando la existencia de una mayor competencia entre empresas relativa a la implementación de medidas de privacidad.

Códigos de autoconducta

Asimismo, desde el lado de la autorregulación, destaca el acuerdo[41] alcanzado entre el Fiscal General de California con Amazon, Apple, Google, Hewlett-Packard, Microsoft y Research In Motion, para mejorar las condiciones de privacidad en el entorno de las aplicaciones para *smartphones*, tabletas y otros dispositivos móviles. El acuerdo, que no impone obligaciones legales vinculantes, establece un conjunto de estándares en la industria de aplicaciones móviles con el objetivo de promover una mayor transparencia, reforzar el control de los usuarios sobre sus propios datos, así como cumplir con la legislación de California de privacidad.

Para promover la transparencia, los firmantes han acordado un principio según el cual se deberá establecer y publicar cuál es la política de privacidad de las aplicaciones que acceden a datos personales, proporcionando una información clara y completa, en aquellos casos en los que la ley lo requiera. Además, se incluirá en los procesos de envío de aplicaciones a las tiendas de aplicaciones una categoría opcional destinada a describir las prácticas relativas a la privacidad. Cuando esta información esté disponible se pondrá a disposición de los usuarios antes de descargar e instalar las aplicaciones.

El acuerdo impulsa la existencia de mecanismos en las tiendas de aplicaciones de los

41. Nota de prensa disponible en: http://oag.ca.gov/news/press_release?id=2630

Área	Nombre de la propuesta	Fecha de introducción
Privacidad *online*	S. 913: Do-Not-Track Online Act of 2011	Mayo de 2011
	H.R. 654: Do Not Track Me Online Act	Febrero de 2011
	H.R. 1895: Do Not Track Kids Act of 2011	Mayo de 2011
Derechos de los consumidores	S. 799: Commercial Privacy Bill of Rights Act of 2011	Abril de 2011
	H.R. 1528: Consumer Privacy Protection Act of 2011	Abril de 2011
Seguridad de los datos personales	S. 1207: Data Security and Breach Notification Act of 2011	Junio de 2011
	S. 1151: Personal Data Privacy and Security Act of 2011	Junio de 2011
	H.R. 1707: Data Accountability and Trust Act	Mayo de 2011
	S. 1434: Data Security Act of 2011	Julio de 2011
Geolocalización	H.R. 2168: Geolocational Privacy and Surveillance Act	Junio de 2011
	S. 1212: Geolocational Privacy and Surveillance Act	Junio de 2011

firmantes para que los usuarios puedan informar del no cumplimiento con los términos del servicio o leyes aplicables. Asimismo, se implementarán los procesos adecuados para responder a estos casos detectados, facilitando un enfoque autorregulado.

Finalmente, los firmantes se comprometen a seguir colaborando con el fiscal general del Estado de California en la mejora de las prácticas de privacidad en el entorno móvil, elemento que evaluarán tras seis meses de firmar el acuerdo.

2.4 Iniciativas globales de privacidad y protección de datos personales

La protección de los datos personales y el establecimiento de políticas de privacidad respetuosas con los individuos se han situado como elementos críticos para el negocio de múltiples corporaciones, algunas de las cuales basan una gran parte de su actividad en el uso, la explotación y la compartición

de determinada información personal. Una adecuada gestión de los datos personales no solo es necesaria para asegurar la seguridad y la protección de estos, sino para garantizar la competitividad de las empresas, la imagen de marca y la confianza de los consumidores.

Dado el carácter globalizado y descentralizado de Internet, que facilita la ubicuidad en la recogida y el tratamiento de los datos personales, resulta necesario adoptar un enfoque global en el tratamiento de las problemáticas reguladoras que afectan a las cuestiones de privacidad y protección de datos. El uso de normas globales permitirá contribuir a incrementar la confianza de los consumidores, facilitará la actividad de las empresas al enfrentarse a marcos reguladores homogéneos, además de reducir la existencia de asimetrías en la regulación que generan impactos negativos en la competitividad y la innovación[42].

El debate de cómo alcanzar modelos globales de privacidad y protección de datos ha sido adoptado en diferentes foros y conferencias globales, como el *European Data Protection Day* (EDPD), organizado anualmente por el Consejo de Europa[43]; *el Asia-Pacific Economic Cooperation* (APEC), que configura una red de 21 países en la región de Asia-Pacífico incluyendo a EE. UU.[44] y que en 2011 permitió alcanzar un acuerdo para armonizar la transferencia de datos personales entre sus miembros[45]; o la *International Conference of Data Protection and Privacy Commissioners* (ICDPPC), que en 2012 celebra su conferencia número 33 y que ha alcanzado acuerdos relevantes como la Resolución de Madrid de 2009.

A través de dichos foros se discuten modelos de protección de datos más flexibles que puedan ser la base para acuerdos de carácter global que limiten las diferencias normativas en las distintas regiones. Las principales medidas propuestas en los diversos foros para avanzar hacia estándares globales[46], y que serán objeto del presente apartado, se basan en la aplicación de modelos de uso y obligación, el principio de responsabilidad, y la flexibilización de los mecanismos de transparencia y de consentimiento.

Los procesos de revisión y reforma de la legislación en EE. UU. y en Europa se presentan como una oportunidad clara para incluir medidas de carácter global, y para avanzar hacia un mayor reconocimiento de elementos comunes, como propone en su contribución Paul M. Schwartz. Esto resulta de especial importancia en el caso europeo, cuyo modelo supone un elemento de referencia internacional. La Comisión Europea ha incluido en su propuesta de Reglamento algunos de los enfoques globales planteados a continuación, sin embargo, se enfrenta al reto de afrontar las problemáticas de privacidad y de protección de datos mediante una visión global durante el proceso de modificaciones de la propuesta realizada.

---

42. Ver, ETNO, ETNO views on the issue of innovation and competitiveness of EU-based companies with a view to the review of the Data Protection Directive, (2011); Catherine Tucker, «Internet Privacy: The Impact and Burden of EU Regulation» (2011), Testimony to the Committee on Energy and Commerce, U.S. House of Representatives; Paula J. Bruening, «Internet Privacy: The Impact and Burden of EU Regulation» (2011), Testimony to the Committee on Energy and Commerce, U.S. House of Representatives; Avv. Felix Hofer, «Privacy Challenges in Marketing Practices. European (over)ruling of the use of personal data?» (2011), audience the Advertising Law & Public Policy Conference 2011 organized by the Association of National Advertisers; Avi Goldfarb and Catherine Tucke, «Privacy Regulation and Online Advertising» (2011), Management Science, 57(1), 57-71.
43. Ver http://www.coe.int/t/dghl/standardsetting/dataprotection/Data_protection_day_en.asp
44. Ver http://www.ftc.gov/opa/2010/07/apec.shtm
45. La información completa sobre el APEC Cross-border Privacy Enforcement Arrangement (CPEA) puede consultarse en http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Cross-border-Privacy-Enforcement-Arrangement.aspx
46. Ver Paula J. Bruening and Waterman K. Krasnow. «Data Tagging for New Information Governance Models.» (2010), IEEE Security & Privacy Magazine, 8(5), 64-68.

2.4.1 Modelo de uso y obligación

El modelo de notificación y elección, eminentemente prescriptivo, se basa en la obligación de los responsables del tratamiento (también conocidos como controladores de los datos) de notificar a los consumidores el mecanismo según el cual la organización recogerá, usará y compartirá datos sobre ellos, y en el cumplimiento de un conjunto de obligaciones de protección en caso de existir un consentimiento explícito de los consumidores. La notificación, la posterior solicitud de consentimiento y las obligaciones adquiridas bajo este modelo dependen únicamente del tipo de datos recogidos (datos personales o sensibles), de cómo fueron recogidos y de a qué sector pertenece el responsable de ellos (diferenciación de obligaciones en el caso del sector de las telecomunicaciones).

Este enfoque puede generar la saturación de los usuarios al recibir demasiadas notificaciones, que en ocasiones resultarán demasiado largas, y complejas, lo que dificultará la toma de decisiones informadas. Esto puede desembocar en la aceptación sistemática de las condiciones de privacidad, sin que los usuarios presten atención suficiente a aquellas situaciones de mayor riesgo. Asimismo, esta obligación genera en los responsables de dichos datos costes relevantes que pueden afectar a su competitividad y su capacidad de innovación.

Como alternativa al modelo anterior se ha planteado el uso de modelos de «uso y obligación»[47], que se basan en una mayor flexibilidad y adaptación de las obligaciones a los riesgos y los tipos de uso de los datos personales. Este modelo no reemplaza la necesidad de la participación de los consumidores mediante políticas de notificación y elección, sino que permite disminuir la actual sobredependencia en los consumidores en la gestión de sus datos personales. Los responsables de los datos seguirán teniendo que proporcionar notificaciones adecuadas, pero la naturaleza de estas y de las obligaciones en cuanto a información, obtención del consentimiento y derechos de los propietarios de los datos variarán en función del uso de los datos, reduciendo la dependencia en el consentimiento individual de los consumidores en situaciones en las que los usos y niveles de riesgo no lo requieran.

Por ejemplo, bajo un modelo de uso y obligación, la aparición del nombre de un individuo en un listado de empleados en la intranet de su empresa requerirá de menores protecciones y obligaciones que la aparición del mismo nombre en una «lista negra» relacionada con impagos de crédito. Este enfoque difiere del modelo actual de notificación y elección implementado en la UE, ya que todos los datos personales –salvo los datos caracterizados como sensibles– disfrutan de las mismas protecciones y obligaciones independientemente del contexto en el que se usan[48].

Este modelo supone una mejora frente al de notificación y elección, al permitir responsabilizar de una forma más directa a las entidades responsables del tratamiento de los datos de la regulación y vigilancia del mismo, mientras que mantiene la capacidad de participación de los individuos en los casos necesarios[49]. Este enfoque se encuentra estrechamente relacionado con el principio de responsabilidad.

---

47. The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy. Disponible en: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
48. Algunos Estados miembros han adoptado medidas en las que se distingue el contexto en el que se usan los datos. Por ejemplo, en Austria los datos codificados están sometidos a menores requisitos si son procesados por entidades que no disponen de los códigos. Datenschutzgesetz 2000 – DSG 2000, Bundesgesetzblatt, 17 August 1999, as amended, Article 2, §4(1). Disponible en: www.dsk.gv.at/DocView.axd?CobId=41936
49. Ver Fred H. Cate «The Failure of Fair Information Practice Principles» in Consumer Protection in the Age of the Information Economy (2006). Disponible en SSRN: http://ssrn.com/abstract=1156972

2.4.2 Principio de responsabilidad

El principio de responsabilidad ha sido incluido en diversos acuerdos internacionales, como las directrices de privacidad de la OCDE de 1980[50], el marco de privacidad de la APEC en 2005[51] o el estándar internacional sobre protección de datos personales y privacidad de 2009[52], conocida como la resolución de Madrid. En los distintos casos el principio de responsabilidad requiere al propietario y al responsable de los datos personales la responsabilidad para cumplir con las medidas de protección de datos establecidas, estando estos obligados a dotarse de los mecanismos y medidas necesarias para ello y para demostrar su cumplimiento si dicha verificación fuese requerida.

Este principio ha sido planteado por el Grupo de Trabajo del Artículo 29 y el Grupo de Trabajo sobre Política y Justicia[53] como una oportunidad para innovar en el marco legislativo de protección de datos, permitiendo que los responsables del tratamiento de los datos estén en posición para asegurar y demostrar su cumplimiento en la práctica con los principios de protección de datos. En una opinión posterior[54], el GT29 consideraba necesario el uso del principio de responsabilidad para «requerir explícitamente a los responsables del tratamiento la implementación de las medidas apropiadas y efectivas para poner en efecto los principios y obligaciones de la Directiva, así como para demostrarlo en caso de ser solicitado». Asimismo, la utilización de este principio como elemento principal para la revisión de la Directiva de protección de datos ha sido solicitada por diversos organismos[55].

El alcance del principio de responsabilidad, las condiciones que las organizaciones deben demostrar y el tipo de verificación que los reguladores deben hacer para certificar la responsabilidad están siendo analizados por reguladores, responsables públicos y expertos[56]. Una organización responsable puede ser descrita como aquella que dispone sus objetivos de protección de la privacidad y los datos personales según criterios externos establecidos por ley, autorregulación y códigos de buenas prácticas, dotando a la propia organización de la capacidad y la responsabilidad para determinar e implementar las medidas efectivas y apropiadas para alcanzar dichos objetivos.

Los elementos esenciales para el cumplimiento del principio de responsabilidad son: a) el compromiso de la organización de diseñar específicamente políticas internas que permitan desarrollar los principios de privacidad y protección de datos; b) mecanismos para desarrollar y poner en práctica dichas

50. OECD. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). Disponible en: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
51. Disponible en: http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(03995EABC73F94816C2AF4AA2645824B)~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf
52. International Standards on the Protection of Personal Data and Privacy: The Madrid Resolution. Disponible en: http://www.gov.im/lib/docs/odps//madridresolutionnov09.pdf
53. Article 29 Data Protection Working Party, The Future of Privacy: Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (2009), WP 168. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf
54. Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (2010), WP 173. Disponible en: http://www.cbpweb.nl/downloads_int/wp173_en.pdf
55. Entre ellos el GT29, GSMA Europe, Microsoft, eBAy o Hewlett-Packard.
56. Como ejemplo de dichas discusiones se pueden destacar los informes The Galway Accountability Project, Data Protection Accountability: The Essential Elements, a Document for Discussion (2009), disponible en http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf; The Centre for Information Policy Leadership, Demonstrating and Measuring Accountability. A Discussion Document. Accountability Phase II – The Paris Project (2010), disponible en http://www.ftc.gov/os/comments/privacyreportframework/00360-57967.pdf; y The Centre for Information Policy Leadership, Accountability: A Compendium for Stakeholders (2011), disponible en http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Centre_Accountability_Compendium.pdf.

políticas, incluyendo procedimientos, tecnologías, formación y educación; c) sistemas que permitan una supervisión interna continua, la elaboración de revisiones de impacto y la verificación externa; d) situar el foco en los riesgos y en los resultados de las políticas implementadas; e) transparencia, y f) disponibilidad para demostrar el cumplimiento de los compromisos adquiridos.

La aplicación del principio de responsabilidad no implica el reemplazo de las salvaguardas y obligaciones existentes, pero supone el giro del foco regulador hacia la capacidad de las organizaciones para demostrar el compromiso y la ejecución de las medidas necesarias para alcanzar objetivos específicos de privacidad, reforzando la protección ofrecida por la legislación. Este enfoque proporciona una mayor flexibilidad y adaptabilidad del modelo regulador frente a nuevas prácticas y tecnologías.

La implementación de tecnologías de protección del derecho a la intimidad[57] y la inclusión del principio de privacidad desde el diseño[58] se han planteado en el debate como mecanismos asociados al desarrollo del principio de responsabilidad. Si bien la mayoría de los agentes[59] están a favor de la introducción de este tipo de tecnologías y consideran favorable que se incluyan las protecciones a la privacidad desde el diseño de los productos y servicios, advierten de los problemas que puede generar una excesiva prescripción en la codificación de la legislación sobre este aspecto. El principio de privacidad desde el diseño es considerado como un proceso de innovación e ingeniería más que como un requisito obligatorio, por lo que es necesario que su aplicación sea flexible, progresiva y que respete la neutralidad tecnológica.

2.4.3 Transparencia y consentimiento de los usuarios

Una adecuada transparencia de las políticas y condiciones de privacidad es condición fundamental e indispensable para permitir a las personas efectuar un control sobre sus propios datos y para garantizar la protección efectiva de los datos personales. Esta necesidad de alcanzar una mayor transparencia efectiva, con un acceso fácil a la información, mediante un lenguaje claro, sencillo y fácil de entender, ha sido reconocida por la mayoría de los agentes y forma parte de acuerdos internacionales, como la Resolución de Madrid.

La existencia de una transparencia adecuada que permita a los usuarios la toma de decisiones informadas facilita que el usuario se sitúe en el centro del modelo, haciendo que el tratamiento de los datos personales y la información a los usuarios supongan elementos determinantes en la competencia entre empresas, impulsando su desarrollo.

No obstante, algunos agentes[60] han advertido que el derecho de protección de datos no puede garantizarse suficientemente si el foco de dicha defensa descansa demasiado en las

57. Conocidas más a menudo por su término en inglés Privacy Enhancing Technologies (PETs). Para una mayor información sobre estas tecnologías se recomienda la consulta del informe European Commission, Study on the economic benefits of privacy-enhancing technologies (PETs). Final Report to The European Commission (2010). Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf
58. Según la Comisión Europea COM (2010) 609, «El principio de «privacidad a través del diseño» significa que la protección de la intimidad y los datos personales se tiene en cuenta a lo largo de todo el ciclo de vida de las tecnologías, desde su concepción hasta su despliegue, utilización y eliminación final.»
59. En las respuestas a la consulta de la Comisión Europea sobre la Comunicación Un enfoque global de la protección de los datos personales en la Unión Europea, se han manifestado en esta línea Telefónica, ETNO, Nokia y Microsoft, entre otros.
60. Carta del 14 de enero de 2011 del Grupo de Trabajo del Artículo 29 a la vicepresidenta Viviane Reding sobre la Comunicación Un enfoque global de la protección de los datos personales en la Unión Europea. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/others/2011_01_14_letter_artwp_vp_reding_commission_communication_approach_dp_en.pdfdocs/odps//madridresolution-nov09.pdf

acciones tomadas por los individuos, y por el uso que estos hacen de sus derechos. La creciente complejidad del tratamiento de datos personales ha generado el uso de largas y complejas notificaciones, que en muchas ocasiones los usuarios no leen, y la solicitud del consentimiento de los usuarios de forma habitual. Esto puede derivar en que un número significativo de usuarios se acostumbren a dar su consentimiento a las prácticas de protección de datos por defecto, sin que necesariamente hayan comprendido la situación y los riesgos para su privacidad.

El objetivo de la transparencia y la capacidad de elección no debe ser, por tanto, el traslado de una carga excesiva de responsabilidad a los usuarios a través del ejercicio de sus derechos, ya que esto puede ser contraproducente. Por el contrario, la transparencia debe formar parte fundamental de un marco de responsabilidad colectivo que involucre a usuarios, responsables del tratamiento y reguladores, permitiendo una flexibilidad suficiente. Este escenario planteado se relaciona estrechamente con los modelos de uso y obligación y con el principio de responsabilidad presentados anteriormente.

Para mejorar la eficacia de la transparencia y la capacidad de elección se han planteado[61] modelos más flexibles que el implementado actualmente por la UE, basados en: a) que la prioridad legislativa se centre en la transparencia y la publicación de información en aquellos casos que excedan las expectativas razonables y legítimas de los consumidores, sin necesidad de la publicación explícita de información obvia; b) que el consentimiento no sea necesario en todos los casos, sino principalmente en situaciones inusuales, que involucren datos de naturaleza sensible, o durante el alta del usuario con nuevos servicios; c) que exista una suficiente flexibilidad en cuanto a la forma y el contenido de las notificaciones, sin imposición de estándares, y permitiendo su adaptación a los casos de uso concretos, y d), la implementación de mecanismos por los que los individuos puedan expresar su elección y preferencias sobre el uso de la información personal en distintos casos, en lugar de depender de un modelo restrictivo de solicitud de consentimiento para cualquier tipo de tratamiento.

Por ejemplo, bajo el modelo anterior, una persona que solicite un servicio de información basado en la posición para conocer la localización del taller mecánico más cercano, estará solicitando activamente ser localizado, y no debería ser necesaria la negociación de los términos de uso mediante complejas notificaciones y procesos de consentimiento. Sin embargo, si el proveedor de servicios quisiera usar esa información posteriormente para proporcionar ofertas personalizadas, deberá notificarlo de forma breve y clara, garantizando que el usuario es capaz de expresar su elección y preferencias. Otros ejemplos significativos son las iniciativas tipo *do-not-track* planteadas en EE. UU., y cuya estandarización técnica está llevando a cabo el W3C[62], que permiten la instalación de un interruptor en los principales navegadores web indicando si el usuario acepta o no el uso de sus datos personales en los distintos sitios que va visitando.

2.4.4 Impacto y reacciones ante la propuesta de la Comisión Europea

El marco europeo de protección de datos se ha situado como un elemento de referencia internacional, tanto por el papel de liderazgo ejercido por Europa en la defensa de la privacidad y la protección de los datos personales, como por la relevancia económica del mercado europeo para agentes de dentro y fuera de

61. Véanse, por ejemplo, las respuestas de GSMA Europe o de Hunton & Williams LLP - Centre for Information Policy Leadership a la Consulta de la Comisión sobre la Comunicación Un enfoque global de la protección de los datos personales en la Unión Europea.
62. http://www.w3.org/2011/tracking-protection/

la UE. La revisión de la Directiva de protección de datos en forma de propuesta de reglamento y el posterior debate enmarcado en el proceso legislativo definirán las reglas de protección de datos que se apliquen en Europa a partir del 2015, teniendo un impacto significativo sobre la evolución de las distintas normativas y acuerdos de cooperación internacionales, así como sobre la viabilidad de los nuevos modelos de negocio.

Reacciones iniciales en el ámbito europeo

Las reacciones iniciales[63] reconocen el impacto positivo en la armonización del marco regulador que proporcionará el nuevo enfoque, el tratamiento equivalente para servicios equivalentes prestados en la UE independientemente de la localización de las empresas prestadoras de servicios, la introducción de mecanismos de cooperación interna, así como la introducción de las reglas vinculantes corporativas como mecanismo de transferencia de datos personales a terceros países.

Sin embargo, también señalan que la nueva propuesta incluye disposiciones que podrían limitar y obstaculizar de forma innecesaria la actividad empresarial y los nuevos modelos de negocio, generando pérdidas económicas (principalmente entre la pequeña y mediana empresa), limitando las oportunidades a nuevos entrantes, frenando la competencia y la expansión de los negocios globales.

Sin el objetivo de realizar un análisis exhaustivo de las problemáticas que presenta la propuesta de Reglamento realizada por la Comisión, algunos de los principales elementos negativos identificados por agentes de la industria en las distintas opiniones publicadas incluyen:

- Un aumento de las obligaciones de documentación, análisis de impacto, oficina de protección de datos, etcétera. que genera un incremento de los costes y cargas administrativas, así como la extensión de algunas de dichas obligaciones a los agentes encargados del tratamiento de datos, dificultando el desarrollo de servicios *cloud* en Europa.
- Una definición muy estricta del requisito de consentimiento que puede limitar tanto su efectividad como el desarrollo de nuevos planteamientos comerciales.
- La magnitud de las sanciones planteadas, que pueden alcanzar hasta el 2 % de la facturación global de la empresa, generando un elevado nivel de incertidumbre y riesgo para la industria.
- El incremento de los poderes de la Comisión Europea para desarrollar reglas más restrictivas sin un equilibrio en el proceso legislativo, así como la ausencia de representantes de la industria.
- La limitación a las actividades de marketing, *profiling*, y el no considerar el interés legítimo de terceras partes de conocer o emplear datos personales, a la hora de evaluar la justificación para el tratamiento de datos, puede limitar en gran medida actividades y modelos de negocio actuales y futuros, dificultando la innovación.

Reacciones iniciales en el ámbito internacional

Este impacto no solo será sobre aquellos países, como Perú, Marruecos, Uruguay, Túnez, etcétera, que han adoptado leyes de protección de datos alineadas con la Directiva 95/46/EC, sino también en aquellos en los que los marcos de protección de datos son distintos y que desarrollan una intensa actividad comercial o de cooperación con la UE en las que se vea involucrado el intercambio de datos personales.

63. Ver: a) Data Industry Platform, Initial Business Impact Analysis on the Draft European General Data Protection Regulation Version 56 (29 November 2011), y b), ETNO and GSMA Europe Joint Statement on the draft General Data Protection Regulation proposal (GDPR).

Este es el caso de EE. UU., donde se ha generado un debate en torno a la nueva regulación europea y a su impacto. Este debate, desarrollado principalmente a través de audiencias en comités de la Cámara de Representantes[64] y congresos organizados por la FTC, se ha intensificado tras la filtración y posterior publicación de la propuesta de Reglamento de la Comisión, generando el envío de una nota informal del Departamento de Comercio de EE. UU. a la Comisión Europea[65] en la que se señalan las principales áreas de preocupación para la compatibilidad, cooperación e intereses comerciales de EE. UU.

En primer lugar, se señala el impacto negativo que algunas medidas de la propuesta europea pueden tener sobre la compatibilidad con el marco regulador estadounidense, y el sobrecoste para las empresas estadounidenses que tienen operaciones en Europa. A ese respecto, la nota señala los siguientes casos que divergen de los estándares actuales:

- Los requisitos de notificación en caso de violación de los datos personales. Si bien la medida es consistente con la recomendación realizada por la FTC, se considera que algunos de los requisitos son demasiado estrictos (como, por ejemplo, los cortos plazos de tiempo para la notificación), imponiendo costes superiores a los beneficios, y que posiblemente sean trasladados a los usuarios. Asimismo, la nota muestra su preocupación por el posible impacto sobre el bienestar de los consumidores en EE. UU., al desviar las empresas multinacionales estadounidenses con actividad en Europa su atención de temas centrales a la privacidad, como la mejora de las prácticas de seguridad, para atender los nuevos requisitos impuestos por la regulación europea.
- La codificación del derecho al olvido, que obliga al borrado de enlaces y copias públicas de los datos personales, es tratado en la nota informal como una posible fuente de problemáticas. No solo por la dificultad de implementación de la medida, que en muchas ocasiones será impracticable por haberse distribuido la información fuera de las fronteras de la UE, sino porque puede plantear incompatibilidades legales con algunos derechos, como el de libertad de expresión.

En segundo lugar, la nota considera que los requisitos de verificación de la adecuación de terceros países se incrementarán bajo la nueva propuesta de Regulación, aumentando las trabas del proceso así como su opacidad e indeterminación. Asimismo, se critica la falta de claridad respecto hasta qué punto otros mecanismos alternativos, como los códigos de autoconducta o los mecanismos de certificación, permitirán la transferencia de datos personales entre la UE y terceros países.

Igualmente, la publicación por parte de la Casa Blanca de la estrategia de revisión del marco estadounidense supone, tal y como plantea Alan Charles Raul en su contribución, una respuesta a la propuesta de la Comisión, y una reafirmación del papel internacional del modelo de EE. UU.

Impacto sobre la innovación y los modelos de negocio

El impacto que la nueva Regulación europea pueda tener sobre el desarrollo y la viabilidad

64. Durante 2011 el Comité de Energía y Comercio de la Cámara de Representantes de Estados Unidos realizó dos audiencias sobre privacidad, analizando de forma específica en una de ellas el impacto de la regulación Europea. Disponible en: http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8905 y http://energycommerce.house.gov/hearings/hearingdetail.aspx?NewsID=8769

65. La nota informal ha sido publicada en la página web de la asociación European Digital Rights. Accesible en: http://edri.org/files/12_2011_DPR_USlobby.pdf

de los distintos modelos de negocio surgidos de la captura, el tratamiento y la potencial compartición de datos personales en un entorno *online* –y presentados con gran detalle en el capítulo 3– subyace a algunas de las críticas y desventajas señaladas. Algunas de las limitaciones a los nuevos productos y servicios que introduce la propuesta de Regulación son: la prohibición al marketing directo salvo consentimiento explícito, limitando los modelos de negocio basados en la publicidad segmentada; la limitación de las prácticas de clasificación o *profiling* a partir de datos personales sin consentimiento previo de los usuarios, limitando las herramientas de inteligencia de negocio; o la limitación que supone no considerar los beneficios de terceras partes en el equilibrio entre los derechos de los usuarios y los legítimos intereses de las empresas, limitando la capacidad de capturar datos personales de aquellos agentes cuyo modelo de negocio se basa en la venta de información privada o de carácter personal.

James Andrew Lewis

James Andrew Lewis es miembro principal y director de Programa del Centro de Estudios Estratégicos e Internacionales (CSIS) de EE. UU., donde escribe sobre tecnología, seguridad y economía internacional. Antes de unirse al CSIS, trabajó en los Departamentos de Estado y de Comercio como titular de Relaciones Exteriores y miembro del Servicio Ejecutivo Superior. Lewis ha escrito más de setenta publicaciones desde su adhesión al CSIS. Se ha doctorado por la Universidad de Chicago.

3. Contribuciones para «Modelos reguladores de protección de datos para una era global»

3.1 Privacidad y ciberseguridad en transición

James A. Lewis.
Miembro principal y director de programa del Centro de Estudios Estratégicos e Internacionales de Estados Unidos

3.1.1 Introducción

Estamos estrechamente conectados a través de nuestras redes digitales en una forma que nadie imaginaba hasta el momento en que produjo el tránsito de Internet para uso comercial. Esta conexión digital ha dado lugar a una proximidad virtual por la que todos somos vecinos, y ha planteado nuevos retos tanto para la privacidad como para la seguridad. La porosidad y vulnerabilidad de las redes cibernéticas y la facilidad con la que quienes poseen intención maliciosa logran acceder a la información sin el permiso del propietario supone nuevos riesgos para los individuos, empresas y naciones, y al mismo tiempo añade una nueva dimensión a cualquier esfuerzo por preservar la privacidad individual.

La privacidad y la ciberseguridad no son lo mismo. La ciberseguridad es la protección de los servicios e infraestructuras críticas frente a cualquier irrupción, así como la protección de la información contra accesos no autorizados. La privacidad es el derecho que todo individuo tiene a controlar el acceso a su información personal y el uso de la misma. La normativa sobre privacidad funciona en aquellas circunstancias en que las empresas y los individuos acatan el estado de derecho. La normativa y acciones necesarias para proteger la privacidad no son adecuadas para la ciberseguridad, pues no se ocupan de la protección de las infraestructuras críticas ni de la existencia de agentes maliciosos. De manera similar, el hecho de que las redes sean seguras no implica una adecuada protección de la privacidad. Las medidas de ciberseguridad no evitarán la recopilación y uso de datos generados por las acciones de cada individuo en Internet; de hecho, algunas medidas sobre ciberseguridad (como una mejor autenticación de la identidad *online*) podrían facilitar la recopilación de dichos datos e incrementar los riesgos contra la privacidad. Aunque la ciberseguridad y la privacidad comparten algunos problemas y soluciones (tales como el uso de la encriptación o la notificación de violaciones de datos), deberíamos tratarlas como dos

cuestiones políticas distintas e independientes, de las que se requieren soluciones para conseguir el beneficio económico completo de las tecnologías digitales.

Los riesgos de una ciberseguridad débil han recibido una atención considerable durante los últimos años al ir aumentando la cantidad de incidentes perjudiciales o embarazosos. Pero a pesar de toda la atención, muchas estrategias de ciberseguridad nacional no son adecuadas, pues se basan en enfoques desfasados. El antiguo enfoque recalcaba la acción voluntaria de las redes individuales, coordinadas de manera flexible a través de una mezcla de procesos que comparten información. Sin embargo, el enfoque voluntario ya no resulta idóneo para las amenazas a las que se enfrentan las naciones en el ciberespacio. La creación de un CERT, el uso de información compartida en un «punto de defensa» técnico y la infraestructura crítica como objetivo principal no son una estrategia adecuada para la ciberseguridad.

Resulta fácil malinterpretar los riesgos de una ciberseguridad pobre, y suele subestimarse la magnitud de la amenaza para las redes y los datos. La actividad maliciosa implica el robo de propiedad intelectual, el espionaje y otros delitos penales, más que la creencia popular de los ataques de terroristas contra las infraestructuras críticas. Las principales amenazas contra la seguridad son el espionaje (tanto económico como político), los delitos financieros transnacionales y el potencial de acciones militares. Cada uno de esos problemas requiere políticas y prioridades distintas y conlleva implicaciones diferentes para la privacidad.

En la actualidad, tan solo unos pocos poderes cibernéticos altamente desarrollados disponen de las funciones más avanzadas contra los ataques cibernéticos (aunque más de treinta naciones están desarrollando doctrinas y tecnologías relativas a conflictos cibernéticos).[66] Contra estos poderes cibernéticos la defensa es excepcionalmente difícil. Ha habido, como muy pocos, dos o tres «ataques» reales, siendo el más conocido el Stuxnet. Pero todo esto acabará cambiando. Podemos calcular que el riesgo de los ataques cibernéticos siga creciendo hasta que se apliquen las medidas preventivas adecuadas, lo cual exigirá acciones nacionales y consenso internacional.

Lo que resulta inquietante es que la capacidad de lanzar ataques cibernéticos se esté convirtiendo en un bien de consumo. La velocidad de esta conversión no está clara, pero cabe esperar un despliegue de las capacidades de lanzamiento de ataques cibernéticos que permitirá a otros actores hacer uso de las mismas. Los florecientes mercados negros del crimen cibernético ofrecen información personal robada, herramientas de ataque, información sobre vulnerabilidades del software, «bot-nets» (conjunto de miles de ordenadores infectados que pueden ser controlados vía remota y utilizarse para ataques de *spam* o de denegación de servicio) y otros tipos de software malicioso. Aunque las capacidades de ataque más avanzadas pueden no aparecer en estos mercados, es inevitable que haya cierta proliferación de las mismas. Estas herramientas están incrementando su capacidad de acceso ilegal a las redes o equipos informáticos para extraer la información.

Podemos considerar varios interrogantes que explican la relación entre la seguridad y la privacidad: ¿hasta qué punto exige una mejor ciberseguridad el uso de tecnologías más invasivas que pongan en riesgo la privacidad? ¿Cuándo se refuerzan mutuamente la ciberseguridad y la privacidad, cuándo entran en conflicto y cuándo la mejora de una de ellas es irrelevante para la mejora de la otra? ¿Cuál es la importancia del anonimato para la privaci-

66. United Nations Institute for Disarmament Research, *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization* (2011), http://kms1.isn.ethz.ch/serviceengine/Files/ISN/134215/ipublicationdocument_singledocument/9b169842-9151-454e-a469-44ac39346672/en/pdf-1-92-9045-011-J-en.pdf

dad y las libertades civiles? ¿Qué tipo de privacidad requiere la libertad política? Se trata de interrogantes esencialmente políticos cuyas respuestas dependen de la constitución y cultura de cada nación.

La privacidad siempre estará en peligro sin una ciberseguridad adecuada, pero una mejor ciberseguridad en sí misma no protegerá la privacidad. La información personal puede explotarse sin el permiso o conocimiento del propietario en el nuevo entorno digital. Existe una falta de claridad en cuanto a cuál es la información que posee carácter público. Si emprendes una acción en Internet, ¿sería pública y por tanto susceptible de ser recopilada para uso comercial? ¿Debería exigirse a la empresa que solicitara el consentimiento? Los gobiernos pueden reducir el riesgo de sus ciudadanos mediante la regulación de la conducta comercial, pero la privacidad exige dos tipos de regulación, en cuanto al uso de la información personal y en relación a la seguridad de las redes digitales.

Resulta sencillo creer que la ciberseguridad y la privacidad están en conflicto. Algunos de los defensores de la privacidad no confían en gobiernos y empresas, pues les hacen sospechar de la ciberseguridad. La ciberseguridad, con la implicación inevitable de los cuerpos de seguridad del Estado y de las agencias de inteligencia, puede originar inquietudes en cuanto a las libertades civiles. Mientras que una ciberseguridad débil pone en peligro la privacidad, los procesos de defensa pueden exigir a los gobiernos emprender medidas invasivas con el fin de controlar las comunicaciones y detectar el software malicioso y otras acciones ilegales.[67] Esta vigilancia, si no se regula adecuadamente mediante normas y procedimientos de control, podría suponer un riesgo para la privacidad, aunque sin ella la tarea de la ciberseguridad podría resultar imposible. Quizá ese sea el motivo por el que la Comisión Europea, en su propuesta para el nuevo Reglamento general de protección de datos, permita un acceso no autorizado a los datos «en la medida en que sea estrictamente necesario para garantizar la seguridad de la red y de la información.»[68]

La tensión entre la seguridad y la privacidad se sostiene sobre los pilares de Internet, que comenzó como una herramienta de investigación y se convirtió, de manera involuntaria, en una red global. Los creadores de Internet no tuvieron en cuenta muchos aspectos de importancia durante el proceso de diseño, entre los que se incluyen la seguridad y la privacidad. El diseño original de Internet se centraba en garantizar una conectividad sencilla y fiable. En su defensa cabe decir que no eran conscientes de que estaban sentando las bases de una infraestructura global que usarían cientos de millones de personas de todos los países del mundo tanto para fines comerciales como políticos y sociales.

De hecho, a pesar de todo, Internet no se creó para ser seguro y no preocupaba la autenticación de la identidad de los usuarios. Las acciones en Internet tan solo están asociadas ligeramente con un individuo concreto cuando sale de su red. Al mismo tiempo, su progreso a través de la red deja una «huella digital» que puede rastrearse muy fácilmente, aportando una cantidad inmensa de datos sobre el individuo. Esto también cambiará al tiempo que las tecnologías y protocolos existentes se revisan y mejoran, aunque los cambios serán graduales, conformados en función de los valores políticos de las empresas y los individuos que los efectúen, y se implantarán con demasiada lentitud como para poder mejorar la situación. Los cambios tecnológicos

67. *"European attitudes towards surveillance* may be indicative of a more balanced and less politicized approach.» Benjamin Goold, «Making Sense of Surveillance in Europe», (2009), *European Journal of Criminology.*
68. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, January 25, 2012, p. 23

no mejorarán la seguridad ni la privacidad a la velocidad que necesitan las sociedades, que cada vez dependen más de las redes digitales.

Puesto que dependemos de una arquitectura insegura, la protección de la privacidad no se encuentra integrada en las tecnologías que usamos, y se han aplicado varios remedios provisionales. El anonimato puede proteger la privacidad, pero también puede perjudicar a la seguridad. Y lo que es más, el anonimato y la falta de confianza en los procesos digitales a que da lugar viene acompañado de un «coste de oportunidad», principalmente debido a la distorsión o ralentización del uso continuado de Internet y la obstaculización que supone a las tecnologías digitales a la hora de obtener beneficios adicionales. Crear confianza requerirá progresar tanto en la protección de la privacidad, como de la ciberseguridad, aunque ambas requerirán marcos reguladores y políticos distintos.

3.1.2 La naturaleza cambiante de la privacidad

La relación entre la privacidad y la ciberseguridad es complicada y se halla en constante evolución, al igual que cambian nuestros conceptos relativos a la privacidad en la era digital. Existe más información sobre los individuos y puede accederse más fácilmente a la misma, una tendencia acelerada gracias al despliegue de las redes sociales. Las redes digitales desdibujan la distinción entre lo privado y lo público. Los usuarios de Internet pueden creer que sus acciones son privadas, incluso que pueden prohibir el acceso a cualquier transacción o dato; sin embargo, este no es el caso. La tecnología ha dado lugar a una tendencia por la que cada vez más información adquiere carácter público y menos información puede ser privada. El simple hecho de navegar *online* supone un riesgo a la privacidad a menos que el usuario tome medidas extraordinarias contra ello, pero son demasiado complejas para la mayoría de los consumidores.

La propagación de la informática y las redes implica que exista un mayor conocimiento sobre los individuos y por tanto una menor privacidad. Las tecnologías y redes digitales han creado masas de información sobre los individuos y han hecho cada vez más difícil la creación de límites en torno a esta información. Internet, al reducir los costes y eliminar las limitaciones espaciales, está socavando el antiguo concepto de la privacidad. Las nuevas tecnologías han reducido los costes de creación, publicación, búsqueda y uso de la información. La audiencia que puede acceder a una cierta información ha aumentado de manera significativa. En algunos casos, el coste de compartir o adquirir la información personal (a través de redes sociales, blogs u otras publicaciones web) es casi nulo. La circulación de la información supone un reto a la creación de una regulación que establezca qué es personal o confidencial y qué información requiere un permiso para acceder a la misma u obtenerla.

Este tipo de divulgación generalizada de la información personal no existía antes de Internet. Se suponía que la gente no compartía su información personal en gran medida debido a que quería preservar su privacidad. Otra explicación es que a la gente no le importaba que ciertos tipos de información adquirieran carácter público, pero no querían pagar el precio en tiempo y dinero que se requería para hacerlo en la era del papel y la tinta. Las actitudes con respecto a la privacidad también podrían haber cambiado gracias al efecto de la reducción de los precios y el cambio en la economía de la divulgación de la información. Internet ha cambiado los precios al reducir los gastos de transacción. Dichos gastos de transacción incluyen el gasto de adquisición de la información y de la comunicación o negociación con otros. En algunos casos, Internet ha eliminado prácticamente dichos gastos, y la conducta y actitud de las personas a este respecto ha cambiado como resultado.

Existe un conflicto inherente entre la privacidad y una acción en una red pública, pues

dichas acciones son públicas. Cuando se navega por la red se deja una huella digital que puede recabarse y evaluarse. Creamos información tangible con respecto a nosotros mismos y nuestros hábitos e intereses simplemente por interactuar en Internet. Al utilizar un ordenador u otro equipo para conectarnos a una red existe una ilusión de privacidad, aunque realmente se está en un espacio público. Internet puede compararse con un centro comercial donde los propietarios permiten un uso público. Al caminar por este centro, no se espera privacidad alguna, pero en el mundo virtual, puesto que se está físicamente solo, se asume una privacidad que en realidad no hay.

Los cambios de actitud con respecto a la privacidad deben examinarse más de cerca, pues la gente ha optado por publicar más información personal (quizá en algunos casos sin percatarse de la medida en que la ha hecho pública). El hecho de que las personas estén más dispuestas o deseen compartir su información personal no significa que también deseen que dicha información se recabe o use para fines comerciales o gubernamentales sin su consentimiento previo. Al mismo tiempo, las exigencias de consentimiento podrían convertirse en una carga u obstáculo para el uso eficiente de la tecnología. Cuantos más datos se almacenen en la nube, más grande será el problema.

La «nube» es un término impreciso para un nuevo servicio comercial. Los proveedores de servicios permiten que los consumidores almacenen datos y accedan a los programas desde una ubicación remota. Es probable que el consumidor no sepa cuál es la situación física real de los datos o servicio. Esta localización puede cambiar rápidamente, pues las empresas distribuyen el almacenamiento en todo el mundo en base al menor precio de cadamomento. Algún tipo de consentimiento general, vinculado a protecciones contractuales sobre el uso y acceso a los datos, podría ser necesario para unas operaciones eficientes «en la nube».

Si se tuviera que redefinir la privacidad, sería conveniente afirmar que sus contornos han cambiado. Las sencillas restricciones en cuanto al acceso y el uso de la información ya no son adecuadas para las preferencias públicas, y el diseño de una nueva normativa debe tener este aspecto muy en cuenta. Cuando la gente opta por crear y publicar información, desea ahora en muchos casos exponerla a una inmensa audiencia. Existen algunas categorías de información que se consideran actualmente como privadas cuando la gente se muestra indiferente en cuanto a su uso, pero hay otras categorías sobre las que no desean que se recabe y use información sin su consentimiento. La normativa sobre privacidad debe encontrar nuevas formas de dar cabida a las opciones individuales sobre la protección de datos de manera que se reconozca que no toda la información personal tiene el mismo valor y que los consumidores podrían encontrarse con obstáculos si se instauraran procesos engorrosos de acceso a sus datos de menor valor.

En el futuro, conforme se digitalicen los registros públicos y el uso de las redes sociales se vuelva universal, la información personal adquirirá un carácter cada vez más omnipresente y podríamos tener que redefinir la privacidad como algo que permite un mayor control individual sobre el uso de los datos, en lugar de como algo que persigue impedir su descubrimiento. Este enfoque debería ser coherente con otros nuevos enfoques relativos a la ciberseguridad, si se asume que los actores maliciosos tendrán acceso a las redes y, en vez de intentar defender la división entre lo público y lo privado, se intente restringir su capacidad de usar los datos que contienen esas redes. Podemos controlar el uso, que no el acceso.

Las definiciones de lo privado y lo público no se diseñaron para un entorno de red, y las incompletas medidas de protección existentes a la recopilación, agrupación y uso de los datos personales no hacen más que agravar el problema. Las normas actuales en cuanto a la información personal se basan, en parte,

en un concepto desfasado del «dominio público». El concepto consiste en que las acciones emprendidas en público, donde no se espera, dentro de lo razonable, que exista una privacidad, no son privadas; son de dominio público y por tanto no están protegidas. Si hago una fotografía o recojo una señal de una calle abarrotada, no necesito el permiso de nadie y soy el dueño de esos datos. Sin embargo, el cambio tecnológico ha socavado esta distinción entre lo público y lo privado. El entorno de red abre muchas vías nuevas de recopilación de datos, y el tratamiento previo al uso de la red relativo a las acciones privadas y al dominio público debe ajustarse a estas nuevas tecnologías.

3.1.3 Valores políticos y tecnología

El debate sobre la privacidad y la ciberseguridad nos conduce rápidamente a los valores que conforman el ciberespacio.

Los arquitectos originales trabajaron desde un punto de vista democrático y libertario.[69] Este punto de vista era bastante flexible y fomentaba el crecimiento, aunque inadecuado para asegurar lo que se ha convertido en una infraestructura global que constituye el centro del comercio. El desplazamiento hacia una red global más segura conlleva el riesgo, no obstante, de que dichos valores democráticos puedan ser sacrificados en pos no solo de la seguridad de la red, sino de la seguridad política de los regímenes autoritarios. Será una tarea ardua el desentrañar este problema, ya que los valores que guían a las sociedades democráticas y las no democráticas son muy dispares. El punto central de este debate será el alcance del anonimato en el ciberespacio y los requisitos para una autenticación robusta de la identidad.

El anonimato en el ciberespacio puede proteger la privacidad, pues evitaría que las empresas y las agencias del gobierno identificaran a los usuarios de Internet o se aprovecharán de ellos. No obstante, al mismo tiempo, el anonimato podría facilitar los delitos y fomentar el extremismo. Tal y como está diseñado en la actualidad, es fácil mantener el anonimato en Internet. Al permitir los delitos cibernéticos, el anonimato reduce la privacidad, pero la mayoría de los defensores de la privacidad argumentarían que el riesgo de delitos cibernéticos es inferior al riesgo de aprovechamiento de los datos por parte de empresas y agencias del gobierno que queda bloqueado mediante el anonimato. Volver a sopesar el anonimato es uno de los mayores retos a los que se enfrenta el uso extendido de las tecnologías de redes digitales, aunque también conlleva un riesgo político real. El problema fundamental reside en cómo hacer que Internet sea más segura reduciendo el anonimato pero sin sacrificar la privacidad y las libertades civiles.

El grupo (o grupos) que usa el nombre de Anonymous ilustra este problema. Anonymous creció a partir de una página web llamada «4Chan», que comenzó como una página de debate sobre el manga japonés y los dibujos animados. Sus usuarios, por lo general hombres jóvenes, podían registrarse para publicar comentarios o bien optar por dejar su comentario de modo «anónimo». Y de ahí viene el nombre que utilizan casi todos los que participan en esa web. A lo largo del tiempo, los temas que se publicaban y se comentaban en 4Chan se incrementaron e incluyeron problemas políticos y sociales, y el sitio ejerce cierto grado de influencia sobre sus muchos usuarios. 4Chan es una comunidad virtual cuyos miembros no se crean ni están vinculados (como ocurre en las comunidades tradiciona-

69. Véase, por ejemplo, «Wizards, Bureaucrats, Warriors & Hackers: Writing the History of the Internet,» Roy Rosenzweig, *American Historical Review,* (diciembre de 1998); John Markoff, «What the Dormouse Said»; «How the Sixties Counterculture Shaped the Personal Computer Industry».

les) por su proximidad geográfica, sino por los intereses que comparten. La dinámica se parece más bien a la de una multitud: no hay líderes formales ni estructura que no sean los que la web ofrece, pero sus participantes pueden ser movilizados para emprender acciones.

La comunidad de 4Chan ha hecho uso de ataques distribuidos de denegación de servicio contra páginas web de entidades que no son del agrado de esta multitud, tales como la de la cienciología, las empresas de tarjetas de crédito y las agencias del gobierno. En respuesta al que consideraban trato indebido a Wikileaks por parte las empresas de las tarjetas de crédito y los comercios *online*, los participantes anónimos de 4Chan crearon un programa para descargar, «Low Orbit Ion Cannon» (LOIC), por el que se permitía a los usuarios que, voluntariamente, participaran con sus ordenadores en eventos DDOS (ataques de denegación de servicio). En diciembre de 2010 había al menos treinta mil descargas de LOIC, y los usuarios más astutos de LOIC canalizaron su tráfico a través de servicios web de anonimato tales como «Tor», que ocultaba sus direcciones de Internet. Como arma, LOIC era débil, pero la organización espontánea y el liderazgo tras este fueron excelentes.

Se ha arrestado a unos cuantos individuos ocupados de la organización de los ataques de Anonymous, pero la capacidad para movilizar a una comunidad de Internet ingente, con tendencia a la anarquía para los fines políticos, y para proporcionarles las herramientas de ataque, constituye una nueva forma de activismo político que podría perjudicar a la seguridad pública. Los ataques de denegación de servicio son simples molestias. Pero ¿qué ocurriría si los individuos que participan en Anonymous consiguieran acceder a herramientas de ataque cibernético más potentes y creyeran, tanto si es cierto como si no, que sus escudos de anonimato les protegen de las consecuencias de cualquier acción?

La autenticación de la identidad es lo opuesto al anonimato. En la actualidad, Internet solo ofrece una autenticación débil. Si un usuario de Internet afirma tener una identidad es difícil determinar cuándo esta es fraudulenta. Por otro lado, aunque sería técnicamente posible crear unos mecanismos de autenticación muy sólidos que vincularan de manera firme la aseveración de una identidad en Internet con la personal real, esto destruiría la privacidad. De hecho, el anonimato inherente a Internet brinda cierta protección de la privacidad, aunque su naturaleza inherentemente colectiva crea nuevas formas de información pública relativa a estos individuos anónimos.

Los esfuerzos por reducir el anonimato *online* y mejorar la autenticación de la identidad ha dado lugar a una oposición enérgica, tal y como muestra la experiencia de muchos países europeos y de EE. UU., que se han esforzado por instaurar sistemas nacionales de identidad. El anonimato tiene ciertos matices comerciales y políticos que benefician a la privacidad. El anonimato evita que las páginas web recojan datos que puedan utilizarse para fines comerciales, como por ejemplo cuando una persona navega por Internet buscando información sobre condiciones médicas pero no quiere que se emita publicidad dirigida ni que se vendan los datos a su seguro de salud o a otras partes interesadas de este.

El anonimato se considera esencial para la libertad de expresión. Esta idea merece especial atención. Es cierto que los países autoritarios controlan Internet para localizar discrepancias y pueden castigar las críticas. Los defensores de la privacidad aducen que la reducción del anonimato podría permitir que dichos países suprimieran la libertad de expresión, vulneraran los derechos humanos y produjeran un efecto coercitivo. Pero tal cosa carece de sentido. En primer lugar, la libertad de expresión no requiere del anonimato en un país democrático. Se podría argumentar incluso que todo discurso político verdaderamente serio requiere la identificación del autor. En segundo lugar, los países autoritarios ya pueden

rastrear a los usuarios. Los gobiernos de estos países son los propietarios o controlan a los proveedores de servicios de Internet, y usan este control para identificar y suprimir cualquier divergencia política en Internet. El anonimato aporta ciertas ventajas cuando los disidentes se conectan a servicios situados fuera de su país, tales como las redes sociales o los blogs, pero incluso esto no supone un obstáculo que un estado dictatorial determinado no pueda salvar a nivel técnico. Si unanación no respeta los derechos de sus ciudadanos, la tecnología ofrece muy poca protección.

De estos ejemplos podemos concluir que es deseable cierto anonimato, pero que este no debería ser condición automática para las comunicaciones en Internet. Los costes de la seguridad pública y la de los estados democráticos sobrepasan las ventajas del anonimato. El objetivo de una Internet más segura debería ser el de permitir que las dos partes implicadas en una transacción puedan escoger. Los remitentes deberían poder escoger cuándo desean enviar datos o navegar de manera anónima, pero los receptores deberían poder escoger cuándo rechazar un tráfico anónimo o con una autenticación débil. La instauración de esta opción en las tecnologías de red será crítica para la ciberseguridad y podrá requerir la ampliación y modificación de las políticas sobre privacidad.

3.1.4 La «defensa activa» y el riesgo para la privacidad

Una autenticación mejorada (que controlase el anonimato) fomentaría la seguridad, pero mal gestionada podría perjudicar la privacidad. Otros avances en ciberseguridad implican el mismo riesgo. Hasta ahora, la ciberseguridad se ha basado en un enfoque disgregado de la misma que estipula que cada red o usuario de Internet es responsable de su propia defensa. La ventaja de este enfoque es que minimizaba toda una gama de problemas políticos. La desventaja, obviamente, es que incluso un oponente no cualificado puede derribar fácilmente una defensa disgregada. La era de la defensa disgregada está llegando a su fin conforme nos adentramos en un entorno de servicios basados en la red (como en *cloud computing*) y, por implicación, a una defensa basada en la Red. En este contexto, acudiremos a terceros que nos presten los servicios de Internet y redes esenciales, y como resultado dichos terceros estarán en mejor posicionados para defenderse.

Un planteamiento de la ciberseguridad, conocido como defensa activa, requiere una mayor monitorización y análisis del tráfico para localizar actividades maliciosas. Los sistemas de defensa dinámica controlan el tráfico para localizar software malicioso y, en algunos casos, actividades anómalas. Estos sistemas toman medidas de bloqueo de dicho tráfico antes de que pueda penetrar en la Red que protegen. En cuanto se identifica el tráfico problemático, los sistemas de defensa usan decisiones preprogramadas que dictan al sistema qué medida tomar cuando se localiza una firma concreta o una clase de firmas como maliciosas. Algunos planteamientos sobre la defensa dinámica pueden parecer «conflictos centrados en la Red», debido a su énfasis en las redes más que en las plataformas y la divulgación de la información con el fin de incrementar la concienciación sobre la situación del defensor y acelerar cualquier respuesta.

La capacidad de controlar el tráfico para localizar códigos maliciosos y neutralizarlos antes de que alcance a sus objetivos, mediante la combinación de una vigilancia amplia de las comunicaciones y la capacidad de explotar la inteligencia exterior con el fin de identificar y derribar cualquier amenaza a la ciberseguridad, mejoraría en gran medida nuestra defensa cibernética. Existen técnicas y tecnologías para la ciberseguridad que son menos invasivas que la defensa activa, pero no son suficientes para cubrir las amenazas existentes. Los programas Einstein del Departamento de

Seguridad Nacional de EE. UU. y otros programas relacionados apuntan hacia otros enfoques más efectivos.[70] Las tecnologías de defensa activa podrían ser más invasivas si no buscan tan solo amenazas cibernéticas, sino también información personal.

Este tipo de control exige «escudriñar» todo el tráfico. La tecnología ya puede explorar el tráfico para buscar códigos maliciosos sin «leer» el contenido, igual que cuando se entrega a una persona una carta que escrita en un idioma que no entiende y se le dice que busque ciertos patrones o símbolos. «Leen» la carta y buscan los patrones sin comprender el contenido. Si se usa este método para proteger las redes nacionales se necesitaría una vigilancia amplia de las comunicaciones combinada con la capacidad de aprovechar la inteligencia exterior para identificar y derrotar amenazas a la ciberseguridad.

Sin embargo, estas medidas son invasivas. Requieren acciones rápidas, una respuesta lo más inmediata posible. Por último, y para conseguir la efectividad máxima, deben ser informadas mediante datos de inteligencia. La combinación del control, la velocidad y la inteligencia en un enfoque dinámico de la ciberseguridad, tanto si se trata de las redes del gobierno como de un conjunto más amplio de infraestructuras, plantea problemas políticos que giran en torno al control y la supervisión que podrían suponer un obstáculo para la mejora de la ciberseguridad. La defensa activa, aunque beneficiosa para la ciberseguridad, tan solo puede funcionar si hay confianza y si los problemas en cuanto al riesgo para la privacidad y las libertades civiles se superan. La normativa sobre privacidad en sí misma no es adecuada para crear el nivel de confianza necesario. Así, la protección adecuada de la privacidad se ha convertido en un aspecto esencial para los nuevos enfoques sobre ciberseguridad.

3.1.5 Privacidad y ciberseguridad en transición

Los nuevos planteamientos en materia de ciberseguridad se enfrentan a varios retos serios. Existe un debate en curso en cuanto al papel del gobierno. Las empresas temen una regulación adicional y los defensores de la privacidad temen la intrusión del gobierno. Resulta complicado crear cooperaciones público-privadas sólidas. La definición del papel correcto de las fuerzas de seguridad a la hora de impedir los ataques cibernéticos o defender la infraestructura civil plantea problemas constitucionales en todas las democracias. Existe una profunda discrepancia ideológica, centrada en EE. UU., entre los defensores de la ciberseguridad y los pioneros de Internet, quienes sostienen que el ciberespacio no debería estar restringido (para promover la innovación y preservar los derechos), debería ser una comunidad autogobernada liderada por la sociedad civil con poca necesidad de intervención del gobierno. Finalmente, la ciberseguridad supone un nuevo problema para la seguridad internacional y requiere estrategias diplomáticas nuevas en materia de defensa y comercio. En las áreas clave (seguridad, comercio, aplicación de la ley), EE.UU. ha efectuado bastantes progresos, aunque estos aspectos complican y ralentizan el ritmo de instauración de defensas mejores.

La creación de una estructura de gobernanza para una nueva infraestructura global infringiría de manera invariable los derechos individuales. Demasiados derechos individuales y un mundo caótico, un lugar hobbesiano donde la fuerza es el árbitro ante toda disputa y la confianza es limitada. Esa es la Internet de hoy en día. La alternativa es un Estado con alto grado de regulación, más frecuente en el cine que en la vida real, donde los derechos de los individuos están oprimidos. Las democra-

70. Department of Homeland Security, *Privacy Impact Assessment: EINSTEIN Program: Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government* (2004), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf

cias occidentales se han esforzado al máximo por lograr un equilibrio al determinar cuándo los derechos de los individuos deben restringirse por el bien común. Los gobiernos ya realizaron esta tarea cuando las tecnologías previas que se extendieron a nivel global crearon nuevas conexiones entre los países, y un aspecto de la historia del siglo anterior ha sido la creación de normas e instituciones para las interacciones que no están sujetas a la jurisdicción de un único estado, sino de distintos convenios sobre la protección de la propiedad intelectual y aplicables al comercio, las finanzas y los viajes. Hemos aprendido que es mejor que el individuo ceda parte de su libertad en ciertas transacciones (viajes aéreos, finanzas, comercio marítimo) a cambio de una mayor seguridad para todos.

Ya es hora de aplicar esto al ciberespacio. Los aficionados del cine antiguo reconocerán el guión del *western* clásico, *El hombre que mató a Liberty Valance*, donde un abogado dubitativo reemplaza al *cowboy* macho y el estado de derecho llega hasta la frontera, finalizando el período del férreo individualismo. El estado de derecho alcanzó al oeste debido a que el férreo individualismo de la frontera es inadecuado, implica riesgos y limita el crecimiento. La transición del ciberespacio desde una frontera pionera hasta una infraestructura global es complicada debido al deseo de algunos poderosos agentes de utilizar esta transición para acabar con la capacidad de Internet de ofrecer un acceso sin trabas a la información. Pero será una transición en la que la forma en que las naciones, las empresas y los individuos organizan y colaboran para la gobernanza, la seguridad y la privacidad en el ciberespacio cambiará de forma inevitable.

A la hora de orientar este cambio podría resultar útil dejar cierta distancia entre la privacidad y la ciberseguridad y tratarlas como aspectos independientes que requieren soluciones independientes. Existen áreas de superposición y acciones que refuerzan tanto la privacidad y como la seguridad, pero el éxito en una área no reduciría de manera adecuada el riesgo de la otra. Las políticas y la regulación que protegiesen de manera apropiada la privacidad de los datos personales, por ejemplo, no reducirían el riesgo de la ciberseguridad de manera idónea. Ambos son elementos del problema mayor de convertir la red global, de la que dependen hoy día las naciones y sus economías, en un lugar más seguro.

La protección de la privacidad se tuvo en cuenta de manera superficial mediante algunos de los defectos del diseño original de Internet: la facilidad de actuar de manera anónima, por ejemplo. Otros defectos del diseño ponen en peligro la privacidad: la capacidad de recabar información de usuarios que no son conscientes de ello. En ambos casos se han desarrollado engorrosas soluciones temporales. Es posible que en el futuro la tecnología avanzada mitigue algunos de estos problemas, pero tan solo si se puede definir claramente lo que se desea que dicha tecnología consiga. La privacidad es un valor apreciado, aunque la naturaleza de la privacidad se está redefiniendo mediante las nuevas tecnologías. La seguridad pública y personal también son valores apreciados. Ni la privacidad ni la seguridad son absolutas, pues pueden equilibrarse y «compensarse» entre ellas conforme se desarrollan nuevas políticas y leyes. La tensión fundamental entre la privacidad y la ciberseguridad es política, el resultado de valores y visiones del futuro que rivalizan. La tarea consiste ahora en explorar estas tensiones e identificar la manera de compensarlas al tiempo que se construye el nuevo marco de las redes digitales globales.

Paul M. Schwartz

Paul M. Schwartz es profesor de Derecho en la Facultad de Derecho de la Universidad de California-Berkeley y director del Centro de Derecho y Tecnología de Berkeley. Es uno de los expertos líderes del mundo en materia de legislación sobre privacidad de la información, y autor de múltiples publicaciones a este respecto. Junto con Daniel Solove, es coautor de *Privacy Law Fundamentals* (Fundamentos de la legislación sobre privacidad, 2011) y de la colección *Information Privacy Law* (Legislación sobre privacidad de la información, 4.ª ed., 2011). Su página web es www.paulschwartz.net

3.2 Privacidad *online*: planteamientos jurídicos en Estados Unidos y la Unión Europea

Paul M. Schwartz
Profesor de Derecho en la Universidad de California-Berkeley
Director del Centro de Derecho y Tecnología de Berkeley

3.2.1 Introducción

En EE. UU., la ley regula la privacidad *online* mediante un mosaico de normas que dejan muchas áreas desprovistas de normativa legal formal. A lo largo de la última década, la Comisión Federal de Comercio (FTC, *Federal Trade Commision*, Comisión Federal del Comercio) ha incrementado su protección de la privacidad al emprender numerosas medidas ejecutorias. Sin embargo, el nivel resultante de privacidad dista mucho de la creación de una gama completa de prácticas leales de la información.

En Europa, por el contrario, la legislación en materia de protección de datos está anclada en unas leyes ómnibus sobre privacidad que han dado lugar a un reglamento sobre el uso de la información personal. Estas leyes permiten además una mayor especificación de la normativa mediante la promulgación de leyes sectoriales. La abundancia legislativa resultante puede provocar complicaciones, no obstante, a la hora de decidir cuál se ha de aplicar. Tal y como se analiza a continuación, además, el proyecto de Reglamento de protección de datos de la UE quizá no pueda poner fin a esta complejidad.

3.2.2 El planteamiento estadounidense

En Estados Unidos, la ley regula la privacidad *online* mediante un sistema mixto que deja muchas áreas desprovistas de normativa legal formal. En 1999, opiné, en el marco de la privacidad *online* en EE. UU., que la protección legal de los datos personales era «por lo general limitada y a menudo incoherente» (Schwartz, 1999, p. 1632)[71]. En 2012, este veredicto requiere tan solo una ligera modificación: hoy día, la protección de la privacidad en EE. UU. sigue estando limitada y cuenta con una naturaleza incoherente, pero la miríada de medidas coercitivas de la FTC ofrece hoy día ciertos elementos generales de protección. En este apartado analizaré la manera en que el sistema jurídico estadounidense regula la privacidad de la información y comentaré cómo el resultado dista mucho de parecerse a un sistema completo de prácticas leales de información.

71. Schwartz, P. M. «Privacy and democracy in cyberspace» (1999), *Vanderbilt Law Review*, 52, 1609-1701.

Mosaico legislativo de EE. UU.

En EE.UU. no existe una ley general que regule la privacidad en Internet. La legislación en cuanto al tratamiento de la información personal suele estar destinada a actividades sectoriales específicas, incluyendo la información sobre el crédito y el alquiler o venta de «cintas de videocasete o material audiovisual similar pregrabado», regulada por la Ley de protección de la privacidad audiovisual[72]. Además, la legislación estadounidense efectúa una distinción importante entre los sectores público y privado. Distintas leyes regulan el tratamiento de datos por parte del gobierno y las actividades similares del sector privado.

Además, el derecho sobre responsabilidad civil proporciona una especie de red de seguridad, aunque como mucho logra proporcionar una protección débil. Varias restricciones establecidas dentro de cada una de las cuatro ramas del derecho sobre responsabilidad civil logran eliminar en gran medida su utilidad a la hora de responder a cuestiones contemporáneas relativas a la privacidad en el ciberespacio. Entre estas restricciones se encuentran los requisitos de «alto contenido ofensivo» de tres de los cuatro delitos contra la privacidad[73]. Los delitos contra la privacidad relativos a la divulgación pública de hechos privados, a la intrusión en la intimidad y los delitos de difamación exigen que la vulneración de la privacidad sea «de alto contenido ofensivo para toda persona razonable» antes de que se permita el resarcimiento (Schwartz & Peifer, 2010, p. 1957)[74]. Puede resultar todo un reto para los demandantes demostrar que una intrusión de su privacidad cumple con estas elevadas exigencias.

Del mismo modo, muchos tribunales permiten a los medios ocupar un gran papel a la hora de decidir la naturaleza de los materiales de interés periodístico. Tal y como ya observara William Prosser (1960)[75], el gran creador del derecho estadounidense moderno sobre delitos contra la privacidad, «La prensa, con su extensa experiencia o instinto a la hora de prever lo que sus lectores desearán saber, ha conseguido crear en gran medida su propia definición de las noticias.» (p. 412). Más recientemente, J. Thomas McCarthy (2009)[76] resumió la cuestión en su tratado con las siguientes palabras: «De hecho, muchos tribunales simplemente disienten de la opinión de los escritores y editores de los medios en lo que respecta a su calificación de lo que tiene «interés periodístico».» (p. 587). Y quizá todavía más importante, la protección de la Primera Enmienda a la Libertad de Expresión plantea ciertas restricciones a los delitos contra la privacidad relativos a la divulgación pública de hechos privados así como a los de difamación.

El acrecentamiento de la FTC como reguladora de la privacidad

Dentro de este mosaico de protección jurídica, la FTC ha asumido un papel cada vez más importante y que ha representado el cambio más significativo de la última década en la legislación sobre privacidad *online* en EE. UU. Desde su fundación en 1914, la FTC ha sido una agencia federal independiente dedicada a la protección del consumidor y el establecimiento de prácticas comerciales leales. Pero también se han planteado límites importantes al alcance de actividades de la FTC como protectora de la privacidad de la información. Antes de comentar estos factores restrictivos, analizaré los cinco pilares de su jurisprudencia en materia de privacidad y después pasaré a describir las actividades de la FTC en el área de la privacidad. Dichos pilares son:

72. Video Privacy Protection Act, 18 U.S.C. § 2710.
73. RESTATEMENT (SECOND) OF TORTS § 652 (1977).
74. Schwartz, P. M., and Peifer, K. »Prosser's Privacy and the German Right of Personality» (2010), California Law Review, 98, 1925-1988.
75. Prosser, W. «Privacy» (1960), *California Law Review*, 48, 383-423.
76. McCarthy, J. T. *The rights of publicity and privacy* (2nd ed.). St. Paul, MN: West Publishers (2009).

1. la protección contra las «promesas sobre privacidad incumplidas»;
2. la promoción de la transparencia;
3. la exigencia de una seguridad adecuada de los datos;
4. el requerimiento a las empresas que utilicen la información personal que desarrollen un «programa integral sobre privacidad»; y
5. la petición del «consentimiento expreso» a cualquier usuario antes de que la empresa cambie las prácticas declaradas y proceda a efectuar una divulgación nueva o adicional de la información personal del usuario (inclusión limitada).

Numerosas acciones de la FTC han desarrollado y hecho cumplir estos cinco elementos. Para estar seguros, las resoluciones de conciliación de la FTC tan solo vinculan a las empresas concretas para las que se emitan y que firmen los convenios resultantes. No obstante, estos convenios suponen la base jurídica de la privacidad de la información en Internet. Se advierte claramente a las empresas que se incluyan bajo la jurisdicción de la FTC que deben seguir dicha normativa.

Desde 1998, la FTC ha mantenido la postura relativa a que cualquier uso o divulgación de información personal de manera que se infrinja la política de privacidad de una empresa se considera una práctica fraudulenta en el sentido de la Ley de la Comisión de Comercio Justo de 1914[77]. Esta opinión representa el primer pilar de su jurisprudencia en materia de privacidad, y prohíbe a las empresas el incumplimiento de sus promesas en cuanto a la misma. La FTC interpreta la conducta de las empresas que incumplen su política de privacidad declarada como «actos desleales o fraudulentos» en virtud de lo estipulado por la Ley de la Comisión Federal de Comercio de 1914.

Más allá de la supervisión de las promesas de las organizaciones, la FTC ha desarrollado además otros pilares que sostienen su jurisprudencia sobre privacidad. Sus dos elementos siguientes consisten en la promoción de la transparencia y la protección contra una seguridad inadecuada. La atención de la FTC hacia la transparencia requiere una difusión adecuada de las prácticas de privacidad, y no solamente términos misteriosos y enterrados en algún lugar de un contrato de términos del servicio. De esta forma, en un proceso ejecutorio contra Sears, que se resolvió en 2009, la FTC alegó que Sears había cometido prácticas desleales al no revelar de manera adecuada en qué medida efectuaba un seguimiento a los clientes a quienes se pagaba por utilizar un programa que registraba sus visitas en Internet[78]. La FTC actuó incluso aunque Sears había proporcionado a los usuarios un contrato de licencia que, aunque redactado en un lenguaje confuso, podría decirse que informaba a los usuarios de que estaban siendo observados. La FTC adujo que la falta de revelación adecuada del alcance de la recopilación de datos por parte de Sears constituía un acto fraudulento. Su auto de conciliación exigía a Sears que proporcionara una relevación clara y prominente de «los tipos de datos que [el software] monitorice, registre o transmite.»[79].

Las actividades ejecutorias de la transparencia de la FTC continuaron en 2010 mediante una resolución contra EchoMetrix[80]. En este caso, el software de «control parental», comercializado como una medida para que los pares pudieran controlar las actividades de sus hijos en la Red, también recopilaba datos de manera clandestina sobre las actividades informáticas de los menores y transmitía la

77. Fair Trade Commission Act of 1914, 15 U.S.C. § 45.
78. Sears Complaint. Complaint, In re Sears Holdings Mgmt. Corp., File No. C-4264 (F.T.C. Aug. 31, 2009).
79. Sears Settlement. Decision and Order, In re Sears Holdings Mgmt. Corp., File No. C-4264 (F.T.C. Aug. 31, 2009), (p. 4).
80. EchoMetrix Settlement, Stipulated Final Order for Permanent Injunction and Other Equitable Relief, F.T.C. v. EchoMetrix, Inc., File No. CV10-5516 (E.D.N.Y. Nov. 30, 2010).

información resultante a los vendedores. La teoría de la FTC en cuanto a este caso es que la empresa no ofreció una revelación adecuada sobre este control.

En cuanto a las acciones contra las empresas que no proporcionan una seguridad adecuada a sus datos, y que constituyen el tercer pilar de la FTC, esta emprende dichas acciones tan solo cuando se produce una filtración de datos. Dentro de estas medidas ejecutorias, la agencia puede pretender sancionar a las empresas que no formen a sus empleados en cuanto a la privacidad y prácticas de seguridad de datos adecuadas (Schwartz & Solove, 2011, p. 1857)[81].

Implicación de la FTC en la regulación de las redes sociales: Google Buzz y Facebook

La FTC ha desarrollado el cuarto y quinto pilar de su jurisprudencia sobre privacidad de manera más clara dentro del contexto de las medidas ejecutorias en relación con a las redes sociales. En EE.UU., la FTC dictaminó en octubre de 2010 una resolución ejecutoria contra Google que implicaba al servicio Buzz de la empresa, que constituyó su breve plataforma inicial de red social. Poco más de un año después, en noviembre de 2011, la FTC dictaminó una resolución ejecutoria contra Facebook. A través de Internet y las tecnologías móviles, las redes sociales permiten compartir contenido generado por los usuarios. Millones de individuos del mundo entero usan hoy día las redes sociales: Facebook cuenta con unos 800 millones de usuarios; Twitter con 200; LinkedIn con 100; y Google+ con 60. Las redes sociales pueden plantear complejos problemas sobre privacidad. Las cuestiones importantes sobre privacidad de las plataformas sociales están relacionadas con la divulgación a terceros del contenido generado por los usuarios y su acceso a la información sobre las actividades de éstos.

En 2010, Google presentó a Buzz, su primer intento de crear una plataforma social, y lo hizo de manera que produjo una amplia difusión de la información personal de los usuarios. Buzz permitía a los usuarios compartir actualizaciones, comentarios, fotografías, vídeos y otra información a través de publicaciones llamadas «buzzes». Tal y como apuntó la FTC en su demanda contra Google[82], sin embargo, «sin que se les notificara previamente o tuvieran la oportunidad de dar su consentimiento, los usuarios de Gmail se vieron configurados, en muchos casos, automáticamente con «seguidores» (gente que sigue al usuario). Además, después de registrarse en Buzz, la configuración de los usuarios de Gmail cambió automáticamente para «seguir» a otros usuarios.» (p. 2).

La resolución de la FTC sobre Google[83] contiene muchos elementos importantes. A los fines que aquí nos ocupan, un aspecto inicial de importancia es que exigiera a Google que obtuviera el «consentimiento expreso» (p. 4) de todo usuario antes de cambiar sus prácticas establecidas que llevaran a una «divulgación nueva o adicional» (p. 3) de la información del usuario a favor de un tercero. En la jerga de la legislación sobre privacidad, esta conciliación exige pues una «inclusión voluntaria» (u «opt-in») de los usuarios ante cualquier cambio en la compartición de información.

El segundo aspecto de importancia de la resolución sobre Google es el requerimiento a esta para que estableciera un «programa integral de privacidad» (p.4). El programa de privacidad integral debe contar con un «diseño razonable» que se ocupe de los riesgos a la privacidad en relación con los «productos y servicios nuevos o existentes para el consu-

81. Schwartz, P. M., and Solove, D. J. «The PII problem: Privacy and a new concept of personally identifiable information» (2011), New York University Law Review, 86, 1814-1894.
82. Google Complaint. Complaint, In re Google, Inc., File No. 102-3136 (F.T.C. Mar. 30, 2011).
83. Google Settlement. Decision and Order, In re Google, Inc., File No. 102-3136 (F.T.C. Oct. 24, 2011).

midor», y que «proteja la privacidad y confidencialidad de la información cubierta» (p. 4). El programa deberá designar además a las partes que coordinen el programa de privacidad, identificar los riesgos para la privacidad y diseñar e implantar controles de privacidad razonables. Dentro de este programa de privacidad, se exigió a Google que autorizara la realización de auditorías externas e independientes sobre privacidad. Éstas incluían una evaluación inicial y después bianual de su programa de privacidad efectuada por un «profesional cualificado, objetivo, independiente y externo» (p. 5). Estas auditorías externas deberán continuar durante un periodo de veinte años.

En cuanto a la resolución de la FTC de noviembre de 2011 contra Facebook[84], ha demostrado ser similar al pleito Buzz de la agencia contra Google. Según la resolución, Facebook:

- no deberá distorsionar la privacidad ni la seguridad que ofrece a la información personal de los consumidores;
- deberá «obtener el consentimiento expreso de los consumidores antes de aplicar cualquier cambio que anule sus preferencias sobre privacidad» (p. 5);
- deberá prevenir cualquier acceso externo al material de las cuentas eliminadas de los usuarios;
- deberá crear y mantener un programa integral de privacidad; y
- deberá realizar auditorías externas e independientes de su programa de privacidad durante un plazo de veinte años.

De estos requisitos, una de las mayores inquietudes es, tal y como se indica en la resolución Google, la necesidad del «consentimiento expreso». La resolución exige a Facebook que obtenga el permiso de los usuarios antes de superar de manera sustancial «las restricciones impuestas por los ajustes sobre privacidad del usuario» (p. 5).

En definitiva, las resoluciones sobre las redes sociales de la FTC refuerzan su jurisprudencia actual en materia de privacidad. Sin embargo, estas medidas requisitorias de la FTC no deberían confundirse con la instauración de una gama completa de prácticas leales de la información.

Prácticas leales de la información y límites de la normativa sobre privacidad de la FTC

Las prácticas leales de la información constituyen el sustento de la legislación moderna sobre privacidad de la información. Para que no quepa duda, no existe ley sobre privacidad, ni en EE. UU. ni a nivel internacional, que contenga todas las prácticas leales de la información de la misma manera o forma exactas. Una cuestión fundamental es que el contenido preciso de las normas varía en base al contexto del tratamiento de los datos, la naturaleza de la información recabada y el entorno regulador y organizativo específico en que se formule la normativa.

No obstante, existe un paquete de herramientas básico para conseguir unas prácticas leales de la información. Puede decirse que los elementos estándares son (Schwartz, 2009, p. 908)[85]:

- los límites sobre el uso de la información;
- los límites a la recopilación de datos (minimización de los datos);
- los límites a la divulgación de información personal;
- la recopilación y uso exclusivamente de información que sea correcta, relevante y actualizada (principio de calidad de los datos);
- los derechos a notificación, acceso y corrección para el individuo;

84. Facebook Settlement. Agreement Containing Consent Order, In re Facebook, Inc., File No. 092-3184 (F.T.C. Nov. 29, 2011).
85. Schwartz, P. M. «Preemption and Privacy» (2009), Yale Law Journal, 118, 902-947.

- la creación de sistemas de tratamiento que pueda comprender el individuo implicado (sistemas de tratamiento transparentes);
- la seguridad de los datos personales; y
- el control del tratamiento de la protección de datos, tanto a través de una entidad pública independiente como de un «responsable» que determine «los fines y medios del tratamiento», tal y como estipula la Directiva de protección de datos en su Art. 2 (d).

A la luz de este listado de prácticas leales de la información ya podemos proceder a evaluar el alcance de las medidas ejecutorias de la FTC. Una de las partes más importantes de esta jurisprudencia se centra en el elemento 5, es decir, el derecho a notificación, acceso y corrección para el individuo. No obstante, la atención de la FTC se ha centrado principalmente en el aviso y el consentimiento; su principal objetivo ha sido asegurarse de que las empresas mantengan sus promesas de privacidad, que informen a sus clientes sobre cualquier cambio sustancial en sus políticas y que obtengan el consentimiento antes de efectuar cualquier modificación a las mismas. La FTC no ha prestado atención a los derechos de acceso y corrección de los datos.

En segundo lugar, la FTC pretende proteger el elemento 6 e incrementar la transparencia; de nuevo centrándose en las políticas sobre privacidad publicadas pero también en casos que implican una divulgación inadecuada. Ya hemos visto un buen ejemplo de este planteamiento en la resolución EchoMetrix de la FTC.

En tercer lugar, la FTC ha prestado atención al elemento 7 a través de sus diversas acciones sobre seguridad de los datos. En cuarto lugar, la exigencia de la FTC de que cada empresa cree un programa de privacidad demuestra la atención que le presta al elemento 8 y su mandato sobre el control interno y externo. De hecho, a través de su papel activo en la protección de la privacidad, la FTC actúa como cierto tipo de «autoridad de supervisión». Y lo que es más, en las resoluciones de Google y Facebook, la FTC exigió a las empresas que crearan sus propios programas internos de privacidad. La clave es la creación y mantenimiento de operaciones de tratamiento de datos responsables gestionadas por profesionales de la privacidad y sujetas a auditorías externas con regularidad.

En conclusión, el planteamiento de la FTC ha ayudado a reforzar el mosaico existente en EE. UU. relativo a la protección de la privacidad *online*. Aun así, esta comparación con la gama completa de prácticas leales de la información demuestra que existen ciertos límites en las medidas resultantes de protección. Escasean en gran medida: los intentos de interponer límites al uso de la información y la recopilación de datos (minimización de datos); los requisitos de acceso a la información personal en manos de terceros; y los requisitos sobre la calidad de los datos.

La función de la FTC tiene otros dos tipos de limitaciones. Para empezar en primer lugar, su jurisprudencia sobre «promesas rotas», tal y como hemos visto, implica que la FTC garantice que las empresas cumplan sus promesas. Y aun con todo, las empresas solo tienen que no prometer demasiado. Las políticas sobre privacidad pueden redactarse utilizando términos vagos y otros que proporcionen a la empresa una flexibilidad máxima en el futuro. Y lo que es más, existen estudios han demostrado que pocos consumidores leen las políticas sobre privacidad, y que quienes lo hacen a menudo no pueden comprenderlas. De hecho, los consumidores suelen creer de manera errónea que las páginas web con una «política de privacidad» publicada ofrecen una protección de peso (Schwartz & Solove, 2011).

En segundo lugar, la FTC no tiene jurisdicción sobre todas las empresas. Existen muchos tipos de instituciones financieras, líneas aéreas, operadores de telecomunicaciones y otras entidades que no entran dentro de la competencia de la FTC. Puesto que existen

esas limitaciones jurisdiccionales, seguirá habiendo cierta incoherencia en la normativa sobre la privacidad *online*. Por último, la Ley de la Comisión de Comercio Justo no contempla fundamentos de demandas privadas. Los fundamentos de demandas privadas pueden ser efectivos a la hora de permitir a los ciudadanos que asuman el rol de «fiscalía privada» al presentar demandas que sean de interés público. Y aun así, la FTC es la única que puede hacer valer la ley, y esta agencia cuenta con muchas otras obligaciones aparte de la privacidad, como por ejemplo la aplicación de la ley antimonopolio y otros aspectos de la competencia leal.

3.2.3 El planteamiento europeo

¿Cómo puede compararse pues el planteamiento sobre la privacidad *online* de EE. UU. con el de la UE? En la UE, la legislación sobre protección de datos está anclada a unas leyes comunes que prescriben las normas a aplicar en el ámbito general, y que a menudo suelen ir sustentadas por leyes sectoriales que regulan ámbitos de aplicación más pequeños. Al mismo tiempo, el ordenamiento jurídico resultante debe luchar por aplicar la legislación existente a Internet, lo cual plantea nuevos problemas e incluso ambigüedades jurídicas. En esta parte comentaré tanto el impacto de la Directiva de protección de datos promulgada en 1995 como la silueta emergente del Reglamento general de protección de datos, cuyo borrador se ha publicado en enero de 2012.

Leyes ómnibus y el concepto de la «prohibición con reserva de autorización» para el tratamiento de datos

Una distinción importante entre la legislación europea y la estadounidense en materia de privacidad es la preferencia europea por el afianzamiento de la legislación sobre protección de datos a leyes ómnibus sobre privacidad. Dichas leyes establecen el marco regulador para una extensa área. Por ejemplo, la ley típica nacional sobre protección de datos europea establece las reglas de tratamiento de la información tanto para las entidades públicas como las privadas.

Después de que la primera generación de legislación sobre protección de datos en Europa se emitiera en forma de leyes ómnibus, la promulgación de la Directiva de protección de datos de la UE en 1995 siguió fomentando esta tendencia. La Directiva de protección de datos exige a todos los Estados miembros de la UE que sigan sus preceptos «transponiéndolos» al ordenamiento jurídico nacional. Da la opción a cada uno de los Estados miembros de utilizar instrumentos jurídicos específicos y, al menos teóricamente, los países europeos pueden optar por promulgar una combinación de leyes sectoriales con el fin de cumplir con la Directiva. Aun así, todos los Estados miembros han promulgado leyes ómnibus que transponen la directiva al ordenamiento jurídico nacional. Tal y como apuntara Ulrich Dammann (2006)[86], el favoritismo universal por las leyes ómnibus en la UE no resulta sorprendente, pues la Directiva exige la transposición «en todo su ámbito de aplicación» (p. 133). Un conjunto de leyes sectoriales podría haber supuesto una carga para cada país de la UE, que hubiera tenido que promulgar «una multitud de reglamentos sectoriales» (p. 133).

El derecho colectivo típico suele permitir una mayor especificación de las normas mediante el uso de leyes sectoriales. Por ejemplo, la ley federal alemana sobre privacidad, la *Bundesdatenschutzgesetz* (BDSG)[87], estipula de manera explícita en su primer artículo que las leyes sectoriales federales tendrán prece-

86. Dammann, U. (1997). EG-Datenschutzrichtlinie Kommentar. Baden-Baden, BW: Nomos Verlag.

87. Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist.

dencia sobre sus propias disposiciones (BDSG Art. 1 (3)). Y en Alemania, al igual que en otros países miembros de la UE, no escasean las leyes sectoriales. Tal y como veremos en la siguiente sección, además, esta abundancia de regulación ha planteado cuestiones complejas relativas al entorno *online*.

Otra norma importante en la UE tiene que ver con la necesidad de contar con una base jurídica adecuada antes de que pueda procesarse la información personal. Esta es otra diferencia relevante con respecto a la ley sobre privacidad de la información en EE. UU. La Directiva de protección de datos establece condiciones limitadas de legitimidad del tratamiento de datos. Según ella, los datos personales solo pueden procesarse conforme a un pequeño grupo de categorías, tales como el consentimiento inequívoco, la ejecución del consentimiento, el cumplimiento de las obligaciones legales, la protección de un interés vital de la persona registrada, las tareas en pos del interés público o el interés legítimo del responsable del tratamiento de los datos personales[88]. Asimismo, en el caso del tratamiento por un interés público o legítimo del responsable del mismo, el sujeto registrado deberá tener el derecho a oponerse dicho tratamiento[89].

Este planteamiento es el que se ha seguido en cada ordenamiento jurídico de los Estados miembros de la UE. A modo de ejemplo, la ley alemana expresa este concepto como una «*Verbot mit Erlaubnisvorbehalt*», o «prohibición con reserva de autorización». La ley alemana prohíbe en principio la recopilación, tratamiento y uso de datos personales. Esta prohibición se levanta, sin embargo, si una entidad legal autoriza la recopilación, tratamiento y uso de los datos en cuestión (Solove & Schwartz, 2012)[90].

El punto básico de partida contrasta notablemente con el planteamiento de los EE. UU. El planteamiento jurídico de EE. UU. suele permitir el uso de la información personal a menos que la ley lo prohíba. Esta tendencia se debe, en parte, a la sólida protección de la libertad de expresión ejercida por la Primera Enmienda. Recientemente, el Tribunal Superior ratificó este compromiso en su sentencia del caso *Sorrell contra IMS Health Inc.* (2011)[91]. Derogó una ley de Vermont por la que se prohibía la venta, difusión y uso de registros farmacéuticos por parte de agentes que utilizaban dicha información para ayudar a captar a médicos que vendieran ciertos productos farmacéuticos. El Tribunal Superior afirmó que «La expresión en pos del marketing farmacéutico... es una forma de expresión protegida por la Cláusula de Libertad de Expresión recogida en la Primera Enmienda.»

Opuestamente a este punto de partida, el planteamiento de la UE prohíbe la recopilación y tratamiento de datos personales a menos que una ley lo permita expresamente o que esté implicado otro conjunto de categorías permisivas. La propuesta de Reglamento general de protección de datos no solo continúa con esta tradición sino que, en ciertos aspectos, la refuerza. Por ejemplo, su Artículo 55 (c) permite el tratamiento de datos personales «siempre y cuando no pudiera conseguirse el mismo objetivo mediante el tratamiento de información que no contenga datos personales»[92]. La propuesta de Reglamento general de protección de datos establece también unos estrictos límites al consentimiento, una condición permisible para el tratamiento, y de hecho, sitúa la «carga de la prueba» sobre el responsable del tratamiento,

88. Directiva de protección de datos, Sección II, Art. 7.
89. Directiva de protección de datos, Sección VII, Art. 14.
90. Solove, D. J., and Schwartz, P. M. Information Privacy Law (4th ed.). Boston, MA: Aspen Publishers (2012).
91. Sorrell v. IMS Health Corp., 564 U.S. _ (2011).
92. European Commission, Draft Data Protection Regulation. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

que deberá demostrar que el sujeto registrado ha otorgado su consentimiento para el tratamiento de sus datos (Art. 7 (1)). De este modo, los puntos jurídicos de partida para el uso de la información personal son bastante distintos en Europa y EE. UU. A pesar de ello, la regulación resultante en ambos ordenamientos puede ser muy similar. En la siguiente sección exploraremos una de las razones relativas a las cuestiones jurídicas complejas que se han planteado hoy en día en las naciones de UE en cuanto al uso de datos en la red.

Complejidad legal y cuestiones pendientes acerca de la privacidad online

Hemos visto que en EE. UU. la regulación se efectúa por medio de leyes sectoriales con cierta cobertura añadida a través de las medidas ejecutorias de la FTC. El resultado deja varias lagunas importantes de cobertura: por ejemplo, los datos personales generados mediante las ventas en Internet de DVD están regulados por la Ley de protección de la privacidad audiovisual, pero no existe una protección federal a la privacidad análoga para los datos personales generados a partir de la venta *online* de libros. Otro ejemplo más[93] serían las normas jurídicas especiales en vigor con respecto al uso que las compañías telefónicas hacen de la llamada «información de red propiedad del cliente.» Sin embargo, no existe protección similar de la información del consumidor que recopilan las páginas web o los ISP (*Internet Service Providers)*.

En cuanto a la privacidad online en la UE, se regula mediante directivas europeas, leyes de protección de datos ómnibus a nivel nacional y leyes sectoriales que regulan áreas específicas del uso de la información. Las directivas UE clave comenzaron a raíz de la Directiva de protección de datos de 1995, que tal y como se ha comentado, será sustituida finalmente por el Reglamento general de protección de datos. Además, tenemos la Directiva sobre la privacidad y las comunicaciones electrónicas de 2002, modificada en gran parte por la de 2009. Una de las modificaciones importantes de 2009 a la Directiva sobre la privacidad y las comunicaciones electrónicas, la del Art. 5 (3), exige el consentimiento del usuario para almacenar información, como sucede con las *cookies*, en los equipos. Se ha producido un debate considerable en las naciones de la UE en cuanto a cómo podría obtenerse dicho consentimiento de manera válida.

Diversos estados de la UE cuentan con niveles distintos de cobertura legislativa de la privacidad *online* dependiendo de la naturaleza de sus leyes sectoriales. El resultado es que en algunas naciones concretas de la UE, distintos tipos de comunicación online son susceptibles de recibir distinta protección de privacidad de la información. Alemania es un buen ejemplo a este respecto.

En primer lugar, la ley alemana sobre privacidad comienza por aplicar las leyes constitucionales y el derecho general de la personalidad a la hora de regular la privacidad del contenido. El Tribunal Constitucional Federal de Alemania se ha mostrado extremadamente activo en esta área. En su «Sentencia sobre la Búsqueda *Online*» (2008)[94], reafirmó su ya antiguo «derecho de autodeterminación informativa», que data de 1983, mediante la identificación en la Ley básica, la constitución alemana, del derecho a «la confianza y la integridad de los sistemas de la información».

En segundo lugar, en el marco de las leyes constitucionales y el derecho general de la personalidad, la ley alemana utiliza el modelo jurídico denominado *Schichtenmodel*, o «modelo estratificado». El modelo estratificado hace uso de distintas leyes para regular el contenido de las comunicaciones *online*, los servicios prestados online y el aspecto técnico. En cuanto al contenido de la comunicación

93. Solove & Schwartz, 2012, pp. 905-910)
94. Online Search Decision, 120 BVerfGE 274 (2008).

online, este está regulado por la Ley federal de protección de datos y por legislación sectorial. Los servicios prestados en Internet están regulados por la *Telemediengesetz*, o Ley de Servicios a Distancia. Por último, el nivel al que tienen lugar las transferencias se regula mediante la *Telekommunikationsgesetz*, o la Ley de telecomunicaciones.

No obstante, puede resultar muy difícil determinar cuál es la ley a aplicar a cada aspecto de los productos, servicios o comunicación *online*. Tal y como comentara Thomas Hoeren (2011)[95], «Debido a la aceleración de la actividad legislativa en los últimos años, cada vez se añaden más leyes a la legislación sobre protección de datos sin llevar a cabo una coordinación cuidadosa de las áreas de aplicación de las leyes resultantes.» Un ejemplo de las confusiones creadas es, según Hoeren, la dificultad de decidir cuándo se aplica la Ley de telecomunicaciones o la Ley de servicios a distancia al uso de los datos personales en Internet. Los protocolos de voz sobre IP (VoIP) y otros aspectos de convergencia técnica no han hecho más que complicar la distinción, a efectos legales, entre los distintos estratos.

Un ejemplo que puede explicar estas complejidades legislativas pueden ser las redes sociales. En EE. UU., y a pesar de la demanda de la FTC contra Google, la regulación de las redes sociales a efectos de la privacidad sigue siendo relativamente laxa. Según comentó William McGeveran (2009)[96], «Parece improbable que el marketing social pueda infringir la mayoría de las leyes estadounidenses sobre privacidad.» (p. 1136). En Europa, la situación es mucho más complicada. Un ejemplo de ello puede ser la continua controversia sobre Facebook en Schleswig-Holstein, un estado alemán.

En otoño de 2011, el Centro Independiente del Estado para la Protección de Datos de Schleswig-Holstein publicó un dictamen pericial[97] por el que se determinaba que las páginas de fans de Facebook y sus complementos sociales, como el botón «me gusta», infringían distintas leyes alemanas sobre protección de datos, incluyendo la Ley de servicios a distancia. Thilo Weichert, el director del centro e Inspector de Protección de Datos de Schleswig-Holstein, solicitó que todas las organizaciones del sector privado y el público de Schleswig-Holstein eliminaran sus páginas de fans de Facebook y amenazó con imponer sanciones a quienes incumplieran tal recomendación[98]. Weichert hizo además un llamamiento al gobierno de Schleswig-Holstein para que retirara su página de fans de Facebook el 31 de octubre de 2011. Como respuesta, el gobierno mantuvo la página pero añadió un aviso a la misma[99]. Dicho aviso informaba a los visitantes que si pinchaban sobre el botón «me gusta» de la página de fans su información se compartiría en Facebook.

El Servicio Científico del Parlamento alemán llevó a cabo su propio análisis de la base jurídica aplicable a las averiguaciones del Centro Independiente del Estado para la Protección de Datos de Schleswig-Holstein[100]. A diferencia de

95. Hoeren, T., «Wenn Sterne kollabieren, entsteht ein schwarzes Loch – Gedanken zum Ende des Datenschutzes" (2011) Zeitschrift für Datenschutz, 4/2011, 145-146.
96. McGeveran, W. «Disclosure, Endorsement, and Identity in Social Marketing» (2009), University of Illinois Law Review, 1105-1166.
97. ULD Expert Opinion (2011, August 19). Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook. Retrieved from https://www.datenschutzzentrum.de/facebook/facebook-ap-20110819.pdf
98. ULD Press Release (2011, August 19). ULD an Webseitenbetreiber: «Facebook-Reichweitenanalyse abschalten.» Retrieved from http://www.schleswig-holstein.de/cae/servlet/contentblob/1035478/publicationFile/111031_stk_cds_facebook.pdf
99. Landesregierung Schleswig-Holstein Media Information (2011, October 31). Datenschutz Facebook: Staatssekretär Dr. Wulff will Fan-Page Schleswig-Holstein nicht abschalten http://www.schleswig-holstein.de/cae/servlet/contentblob/1035478/publicationFile/111031_stk_cds_facebook.pdf
100. Wissenschaftliche Dienste Deutscher Bundestag (2011, October 7). Die Verletzung datenschutzrechtlicher Bestimmungen durch sogenannte Facebook Fanpages und Social-Plugins. Retrieved from https://www.datenschutzzentrum.de/facebook/material/WissDienst-BT-Facebook-ULD.pdf

Weichert, se negó a declarar que las redes sociales y el uso de sus complementos infringieran ninguna de las leyes alemanas sobre protección de datos. El Servicio Científico afirmó que: «La ley sobre protección de datos aplicable está marcada por la incertidumbre, lo cual hace difícil aportar una respuesta inequívoca a las cuestiones jurídicas de este área.» De hecho, comentó la falta de claridad de otras áreas, tales como la situación legal de las direcciones IP y las *cookies*. El Servicio Científico concluyó: «Puesto que la postura legal es compleja y confusa y existe cierta dificultad a la hora de clasificar correctamente los procesos técnicos, en nuestra opinión es imposible efectuar una evaluación definitiva sobre la protección de datos.» (p. 19).

Habida cuenta de la incertidumbre a nivel nacional, la Unión Europea se encuentra en vías de revisar su Directiva de protección de datos fundamental. Peter Hustinx (2012)[101], supervisor europeo de protección de datos, afirmó lo siguiente:

> *"La realidad actual es que la Directiva está empezando a mostrar signos de obsolescencia. Se está acercando a su «fecha de caducidad» y es evidente que no podrá sostenerse durante mucho tiempo. Cuando la Directiva se adoptara en 1995, Internet se conocía bastante poco y en cualquier caso distaba mucho de su alto dinamismo actual.»*

Algunos miembros de la academia jurídica europea han recalcado también la necesidad de actualizar la Directiva de protección de datos.

En sus comentarios en cuanto al proceso de revisión de la Directiva, Viviane Reding (2011)[102], vicepresidenta de la Comisión Europea, ha acentuado la magnitud de los gastos de conformidad actuales que deben asumir las empresas que operan en los distintos Estados miembros. Según su estimación, la carga administrativa asociada con la fragmentación de los regímenes de protección de datos europeos supone a las empresas unos 2.300 millones de euros al año. También señaló la «desigualdad en los niveles de protección de los individuos en toda la UE.» El resultado es que los consumidores se enfrentan además a un nivel fragmentado de protección de la privacidad en la UE. Se espera que el planteamiento revisado a nivel europeo con respecto a la privacidad de la información proporcione una mayor certeza y una protección más sólida y consecuente.

La publicación de la propuesta de Reglamento general de protección de datos en enero de 2012 apunta al menos dos áreas que deben incrementar su certeza jurídica. Primero, la certeza jurídica debe incrementarse mediante un reglamento en vez de una directiva en vigor con respecto a la protección de datos. Según la legislación europea, los reglamentos ejercen un efecto legal vinculante con carácter inmediato tras su promulgación. Por el contrario, las directivas conllevan la necesidad de que cada estado de la UE promulgue sus propias leyes, las cuales pueden distar de manera sutil o notable. En consecuencia, el Reglamento general de protección de datos tiene el potencial de aumentar la similitud de las leyes sobre privacidad de la información de cada estado y, por tanto, de promover la certeza jurídica.

En segundo lugar, el Reglamento crea el Consejo Europeo de Protección de Datos. La

101. Hustinx, P. «Ensuring stronger, more effective and more consistent protection of personal data in the EU» (2012), New Europe. Disponible en: http://www.neurope.eu/blog/ensuring-stronger-more-effective-and-more-consistent-protection-personal-data-eu

102. Reding, V. «Building trust in the digital single market: Reforming the EU's data protection rules.» (2011), Speech 11/814. Disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/814&format=HTML&aged=0&language=EN&guiLanguage=en

máxima autoridad de supervisión de cada estado de la UE y el supervisor europeo de Protección de Datos serán miembros de dicha entidad (Art. 64(2)). Al emitir sus dictámenes en cuanto a ciertas resoluciones importantes de los supervisores de la protección de datos a través de un «mecanismo de consistencia», el Consejo Europeo de Protección de Datos podrá aumentar la uniformidad de la legislación europea sobre la privacidad en todos los Estados miembros (Art. 57).

Asimismo, el poder de los legisladores se incrementará mediante la creación de niveles estructurados de sanciones para las infracciones intencionadas o dolosas del Reglamento general de protección de datos. La sanción máxima para ciertos delitos será del 2% del volumen de ventas mundial anual de la empresa (Art. 79 (6)). Uno de los motivos para la imposición de dicha sanción sería la falta de notificación «puntual o completa» a la autoridad de supervisión o el sujeto registrado en cuanto a cualquier violación de los datos personales.

Al mismo tiempo, el Reglamento podría dar lugar a ciertos tipos de incertidumbre a causa de las nuevas propuestas. Una de las disposiciones de mayor interés contenidas en la propuesta de Reglamento general de protección de datos se refiere a la proposición del «derecho al olvido y a la supresión» (Art. 17). Viktor Mayer-Schönberger redactó un ensayo pionero sobre la «virtud de olvidar» (2011)[103]. En su opinión, «existe la necesidad de establecer fechas de vencimiento como posible complemento a otras respuestas en nuestra búsqueda por revivir el olvido y ayudar de esta manera a humanizar nuestra era digital.» (p. 195). De manera similar a la obra de Mayer-Schönberger, la propuesta de Reglamento general de protección de datos permite al sujeto registrado contar con el «derecho a solicitar al responsable del tratamiento que elimine los datos personales relativos a su persona y que se abstenga de seguir difundiendo dichos datos» (Art. 17 (1)). Este derecho se aplica cuando «los datos ya no se necesiten para los fines a los que se recabaran o procesaran inicialmente», cuando el sujeto registrado retire su consentimiento, cuando el sujeto registrado ejerza su interés y se oponga al tratamiento o cuando el tratamiento de los datos no cumpla no el Reglamento (Art. 17 (1)).

La propuesta de Reglamento general de protección de datos impone límites también al derecho al olvido. Este interés se ha visto reducido por el derecho a la libertad de expresión, por cuestiones de salud pública, por «motivos de investigación histórica, estadística y científica» y por el cumplimiento de las leyes sobre la conservación de datos (Art. 17 (3)). En vista de las excepciones, existen muchas dudas pendientes en cuanto al alcance del derecho al olvido. Y lo que es más, cada Estado miembro puede interpretar dichos límites a la luz de su propia tradición jurídica con el fin de lograr el equilibrio adecuado entre la privacidad y cualquier excepción concreta, como la libertad de expresión y la investigación histórica.

3.2.4 Conclusión

La circulación global de datos se sucede de manera continuada y en múltiples ubicaciones. A causa de ello, algunas de las opiniones recientes de mayor interés escuchadas en los debates sobre la legislación relativa a la protección de datos ofrecen distintas perspectivas en cuanto a la necesidad de «modernizar» la normativa de manera que refleje la nueva realidad de los intercambios rutinarios internacionales de información personal. Un paso importante hacia esta modernización de la ley sería el aumento de la cooperación entre EE.UU. y la UE a la hora de definir la mutua comprensión del significado de las prácticas leales de la información en lo tocante a la privacidad *online*.

103. Mayer-Schönberger, V Delete: The Virtue of Forgetting in the Digital Age. Princeton, NJ: Princeton University Press (2011).

Alan Charles Raul

Alan Charles Raul es el coordinador global principal de privacidad, seguridad de datos y práctica del derecho de la información en Sidley. Tiene una amplia experiencia en litigios y como asesor en materia de regulación gubernamental, *enforcement*, derecho administrativo, conformidad empresarial, privacidad y derecho de la información. La experiencia práctica de Raul en estas áreas incluye cuestiones de privacidad federal, estatal e internacional, programas de protección global de datos, seguridad de la información, ciberseguridad y representación en casos de violaciones de seguridad. También representa clientes en cuanto a leyes de Internet, comercio electrónico, marketing, publicidad y cuestiones de protección al consumidor.

Sidley ha sido designada una de las principales empresas estadounidenses en privacidad y seguridad de datos en la Chambers Global y Chambers USA. Raul ha sido incluido en el *ranking* de los mejores expertos en privacidad y seguridad de los datos en 2009 y 2010. Ha sido nombrado abogado principal de comercio electrónico internacional e Internet en *Who´s Who Legal*. También ha sido elegido en la categoría de privacidad y seguridad de datos en el listado «Attorneys Who Matter» del *Ethisphere Institute*, que reconoce a los abogados con más alto compromiso al servicio público, a la comunidad legal y académica.

3.3. Privacidad y protección de datos en Estados Unidos

Alan Charles Raul
Coordinador global de las áreas de privacidad, seguridad de datos y derecho de la información en Sidley

3.3.1 Introducción

El sistema de protección de datos estadounidense es, posiblemente, el esquema de privacidad más antiguo, más sólido, mejor desarrollado y más efectivo del mundo. Aunque esta afirmación podría suscitar cierta polémica en algunos lugares, especialmente en Europa, resulta coherente con los hechos. En 1791, la Cuarta Enmienda a la Constitución americana, en su Declaración de Derechos (desarrollando la doctrina legal inglesa), garantizó el «derecho de las personas a estar seguras en sus... papeles y pertenencias frente a cualquier inspección y allanamiento irrazonable» por parte del gobierno. La protección legal de la privacidad de la sociedad civil se ha venido reconociendo en el derecho consuetudinario estadounidense desde al menos 1890, cuando se publicó el importantísimo artículo «El derecho a la privacidad», del profesor Samuel D. Warren y Louis D. Brandeis (futuro juez del Tribunal Supremo) en la Revista Jurídica de Harvard (4 Harv. L. Rev. 193).

Esta revolucionaria doctrina americana ideó teorías sobre recursos cautelares y de desagravio en caso de intromisiones en la intimidad (incluyendo compensaciones por los perjuicios morales). El derecho a la privacidad de Warren/Brandeis, junto con el derecho a no estar expuesto a intromisiones del Estado, fue sustentado en 1973 por el primer compromiso afirmativo del gobierno a proteger la intimidad en la era informática. La nueva filosofía se expresó en el «Comité Asesor del Secretario en materia de sistemas de datos personales automatizados», publicado por el Ministerio de Sanidad, Educación y Bienestar de EE. UU. (ahora el Ministerio de Sanidad y Servicios Sociales). Este informe desarrolló los principios de las «prácticas leales de la información» que se adoptaron con posterioridad en la Ley sobre privacidad de 1974 de EE. UU., y finalmente por la UE en 1995 en su Directiva de protección de datos. Los «principios para una práctica leal de la información» establecidos en EE. UU. en 1973-1974 siguen estando operativos en gran medida en todos los regímenes y sociedades del mundo que respetan los derechos a la privacidad de la información personal. Los principios fundamentales de la Ley de privacidad en EE. UU. Eran los siguientes:

- No pueden existir sistemas de almacenamiento de datos personales cuya existencia sea secreta.
- Debe existir una forma en que todo individuo pueda averiguar el modo en que se registra y se utiliza su información.

- Debe existir una forma en que todo individuo pueda evitar que la información obtenida sobre él para un fin determinado se utilice o proporcione para otros fines para los que no haya dado su consentimiento.
- Debe existir una forma en que todo individuo pueda corregir o modificar la información que le identifique.
- Cualquier organización que cree, mantenga, use o divulgue archivos que contengan datos personales de identificación deberá garantizar la fiabilidad del uso de los datos para el fin específico para el que se recopilarán y tomar las medidas de precaución necesarias que eviten un uso indebido de los datos.

Aun con tal índole de protección de la privacidad de la información personal, ¿por qué siguen considerando algunos que EE. UU. es un protector atípico de datos? Es decir, ¿cómo es una jurisdicción que no ofrece una protección de la privacidad «adecuada», según opinan los legisladores europeos? Esta impresión equívoca se deriva de un error a la hora de apreciar la naturaleza extensiva, omnipresente y derivada del sistema de protección de datos estadounidense. Mientras que Europa y los países cuyos sistemas de protección de datos están considerados «adecuados» por parte de los legisladores europeos han creado un marco jurídico integral y colectivo de protección de la privacidad, es obvio que no queda claro si este enfoque funciona mejor en la práctica (o en la teoría) que el modelo estadounidense de protección de la privacidad y seguridad de la información formado por una densa selección de leyes federales, estatales y teorías de derecho consuetudinario que se entrelazan. Sencillamente, no puede existir un argumento creíble que afirme que el brazo ejecutor combinado de la Comisión Federal de Comercio de EE. UU., de la Comisión Federal de Comunicaciones, de la Oficina de Protección Financiera del Consumidor (y otros organismos de regulación financiera y bancaria), del Ministerio de Sanidad y Servicios Sociales, del Ministerio de Educación, de la Fiscalía General del Estado y por último, aunque no menos importante, de la implacable asociación de abogados litigantes de EE. UU, no disciplinen enérgicamente el uso o abuso de los datos personales. No se puede aducir de manera creíble que existe algún sistema de protección de datos en alguna parte del mundo que haya generado más sentencias judiciales, resoluciones, decretos por consentimiento y, quizá lo más importante, programas de cumplimiento de normas corporativas en favor de la privacidad que tal y como se ha atestiguado en EE. UU. Por ejemplo, la FTC impuso una sanción de 15 millones de dólares a Choice Point para que recompensara sus graves fallos en materia de privacidad y seguridad de los datos. Y, tal y como el apéndice a este capítulo demuestra (se trata de un extracto del registro público de Choice Point en la Comisión de Bolsa y Valores de 2006), la resolución multimillonaria de la FTC tan solo era la punta del iceberg en cuanto a la ejecución/reparación de la privacidad a la que tuvo que enfrentarse Choice Point a causa de la infracción de las normas estadounidenses de protección de datos. Las graves infracciones a la privacidad de Choice Point (según se alegó) dieron lugar a diversas medidas de ejecución reglamentaria, investigaciones del gobierno, pleitos de accionistas y pensionistas, litigios por fraude bursátil, demandas colectivas de consumidores, auditorías y programas continuados de cumplimiento de normas corporativas. En resumidas cuentas, la inobservancia de la legislación estadounidense sobre privacidad le costó muy cara a Choice Point.

Mientras que la propuesta de Reglamento de protección de datos europeo de 2012 incluye posibles sanciones draconianas (y de hecho, absurdas) del 2 % del volumen de venta (o ingresos por ventas) total anual a las infracciones a la privacidad (prestando poca o nula atención al principio de la proporcionalidad o del procedi-

miento justo), la realidad es que las medidas de cumplimiento de la privacidad de los datos fuera de EE. UU. han sido relativamente mínimas. Para estar seguros, este hecho podría cambiar en cuanto el nuevo Reglamento se apruebe y entre en vigor, pero podría afirmarse con bastante seguridad que la promulgación y dependencia europea en códigos legales estrictos e integrales ha dado lugar a una mezcolanza de resultados. De hecho, Jeffrey Rosen, un perspicaz analista de muchos temas importantes relacionados con la privacidad, comentó en la Revista Jurídica de Stanford en febrero de 2012[104] que siempre ha existido una dicotomía en Europa entre la estricta legislación en el papel y la relajada aplicación práctica. Refiriéndose al fuerte impacto que la sanción anual propuesta del 2 % a los ingresos podría ejercer sobre la libertad de expresión en Internet al combinarse con el nuevo «derecho al olvido», el profesor Rosen escribió lo siguiente:

> *Es posible, por supuesto, que aunque el [proyecto de] Reglamento europeo defina el derecho al olvido con carácter bastante amplio, se aplique en realidad de manera más restringida. Los europeos acostumbran desde hace mucho a promulgar abstractos derechos de privacidad en la teoría que no aplican en la práctica.*

Al igual que la UE, con su nuevo proyecto de Reglamento de protección de datos, el gobierno estadounidense tiene como objetivo la revisión, el perfeccionamiento y la extensión de la política actual estadounidense sobre privacidad. En el momento de escribir estas líneas, la Casa Blanca y el Ministerio de Comercio de EE. UU. están introduciendo un nuevo marco regulador de la privacidad del poder ejecutivo; la FTC está desarrollando su propio marco revisado de prácticas disciplinarias de la privacidad en lo respectivo a los consumidores; la FTC está redactando un conjunto de normas para páginas web y aplicaciones para móviles que afectan a la privacidad de los menores; la Administración de Servicios Generales y el Ministerio de Defensa están considerando incluir nuevas obligaciones de seguridad de la información para proveedores en la nube y contratistas del ejército; el Congreso está preparado para revisar, retomar, reformar o promulgar diversas leyes sobre privacidad, creación de perfiles, seguimiento, comunicaciones electrónicas, notificación sobre vulneración de datos y seguridad cibernética. Miembros del Congreso de ambos partidos se han comprometido a examinar, exponer, celebrar vistas, investigar y restringir una amplia gama de prácticas de privacidad y usos dudosos de datos. La mayoría de esta actividad congresista, al igual que la de la FTC y la de los litigantes privados, ha sido provocada por un conjunto de periodistas y de organizaciones no gubernamentales (ONG) de gran activismo que no toleran que ninguna transgresión punible de la privacidad pase inadvertida.

Lo cierto es que la protección de la privacidad en EE.UU. está sujeta a cierto contrapeso. El factor más importante es, quizás, el derecho a la libertad de expresión garantizado por la Primera Enmienda. La garantía de los derechos a la libertad de expresión de todo el mundo implica obviamente ciertas complicaciones para el «derecho al olvido», pues el derecho de toda persona al olvido puede contraponerse al sentimiento de nostalgia de otra persona (o al deseo de otro de plasmar el pasado para bien o para mal).

La Primera Enmienda se ha interpretado además de manera que proteja el derecho de cada individuo a conocer la información de interés público, incluso aunque menoscabe hasta cierto punto la privacidad individual.

104. (64 Stan. L. Rev. Online 88)

También se considera que las empresas tienen el derecho, según la Primera Enmienda, a comunicarse con relativa libertad con sus clientes mediante el intercambio de información en ambas direcciones (siempre que la información sea verídica, no engañosa, y que no sea objeto de una práctica comercial desleal o fraudulenta).

En EE. UU., suele pensarse que la política reguladora se fomenta mediante lo que resulte razonable, justo y equilibrado; lo que sea eficiente y rentable; lo que favorezca al bienestar general del consumidor y que promueva la protección del consumidor al tiempo que se mantenga el crecimiento económico y la innovación y se respeten los derechos patrimoniales. Por decirlo de otro modo, a menudo deben conciliarse entre sí objetivos opuestos. Es probable que la perspectiva de la rentabilidad se aplique también a la política de privacidad en el futuro, pues el presidente Obama (al igual que sus predecesores del poder ejecutivo) ha abrazado expresamente este tipo de análisis para las nuevas regulaciones. Evidentemente, los cálculos de rentabilidad también se están teniendo cada vez más en cuenta fuera de EE. UU. Por ejemplo, la propuesta de Reglamento general de protección de datos iba acompañada de una «evaluación de impacto» relativa a los gastos previstos del cumplimiento de la nueva normativa. Los representantes de la Comisión Europea han expresado asimismo su preocupación por que la nueva normativa sobre la privacidad proteja la innovación y fomente las nuevas tecnologías (como los servicios prestados en la nube). Lo que todavía se halla en proceso de cambio en EE. UU., no obstante, es la forma de evaluar los impactos intangibles sobre la privacidad personal que no puedan cuantificarse o incluso calificarse de manera rigurosa. Hasta la fecha, los tribunales no han impuesto, por lo general, daños y perjuicios por vulneración de datos o usos de datos, por ejemplo, cuando dichos daños y perjuicios alegados han sido especulativos, artificiosos o muy dudosos. Esta situación no implica, no obstante, que los problemas emocionales, los daños a la imagen y los atentados contra la dignidad personal se tomen a la ligera por parte de los reguladores estadounidenses o en los litigios de este país. Estos daños intangibles se respetan bastante si se dan las circunstancias adecuadas.

El 23 de febrero de 2012, la Administración del presidente Obama emitió una importante iniciativa política plasmada en un libro blanco y por la que se establecía un marco de privacidad integral, el primero de su clase que hubiera introducido administración presidencial alguna. El libro blanco se titulaba *Privacidad de los datos del consumidor en un mundo conectado: marco de protección de la privacidad y promoción de la innovación en la economía digital global* (a partir de ahora, el *Libro Blanco*), y representa la culminación del desarrollo de una extensa política por parte del Ministerio de Comercio y la Comisión Federal de Comercio de EE. UU. El *Libro Blanco* constituye, además, la respuesta estadounidense al Proyecto de Reglamento europeo de protección de datos que sustituye a la Directiva UE de protección de datos 95/46/CE. El Libro Blanco debería ayudar a restituir el liderazgo de EE. UU. entre los creadores internacionales de políticas de privacidad, y quizá a demostrar que el marco estadounidense de protección de datos es sustancialmente sólido y digno de «reconocimiento mutuo» por parte de la UE. Tal vez la dimensión más importante del *Libro Blanco* sea, sin embargo, quién lo ha emitido, cómo y dónde: al anunciar el *Libro Blanco* en la Casa Blanca acompañado de una declaración y con la impronta del presidente, se pretende que represente una nueva iniciativa presidencial derivada; tal hecho podría incrementar en gran medida la categoría de las cuestiones sobre privacidad y protección de datos en la jerarquía general de la política federal. El papel de la Comisión Federal de Comercio queda tam-

bién bastante reforzado en el nuevo marco de privacidad.

En general, el nuevo marco adopta un planteamiento equilibrado ante el polémico debate sobre la privacidad, considerándola como un derecho humano fundamental y no como un obstáculo a la innovación. En primer lugar, el *Libro Blanco* confirma de manera expresa el compromiso declarado por la Administración hacia Internet como una plataforma de comunicación, innovación y crecimiento económico abierta, descentralizada e impulsada por los usuarios. El *Libro Blanco* reconoce las ventajas obvias que aporta a los consumidores al promover y preservar la transparencia, la flexibilidad y la innovación en relación con la recopilación y el uso de los datos. En segundo lugar, aunque se proponen unos cambios relativamente modestos a la ley sobre privacidad estadounidense, confirma en esencia que el modelo existente de dicha ley funciona razonablemente bien a la hora de proteger la intimidad y promover la innovación. Y en tercer lugar, reconocer que los valores sustanciales que subyacen al planteamiento estadounidense de la privacidad, tal y como se expresan en el mismo marco, equivalen en lo fundamental a los expresados en la Directiva de protección de datos europea y el Marco de Privacidad del Foro de Cooperación Económica de Asia-Pacífico (APEC).

El *Libro Blanco* establece cuatro «elementos clave» para proteger la privacidad. Estos elementos son: a) la primera «Declaración de Derechos de Privacidad del Consumidor» de la historia (CPBR); b) el desarrollo de «códigos de conducta adecuados y jurídicamente vinculantes» con la colaboración de entidades públicas y privadas; c) la aplicación por parte de la FTC de la Declaración de Derechos de Privacidad del Consumidor, y d) el «reconocimiento mutuo» y la «colaboración ejecutoria» para conseguir una «interoperabilidad global». Entre los principios de mayor importancia avanzados en el Libro Blanco se encuentran las normas que obligan a las empresas a limitar la cantidad general de datos que recaban de sus consumidores de manera más «orientada», así como a restringir los datos que recaban y usan en virtud del «contexto» de su relación con los consumidores. Al mismo tiempo, el *Libro Blanco* hace hincapié en que los consumidores también tienen una responsabilidad significativa en la gestión de la privacidad de sus propios datos.

Y quizá con mayor relevancia, el marco propone aumentar la coherencia y la utilidad de la práctica industrial de la privacidad y la seguridad para los consumidores mediante el desarrollo de códigos de conducta y planteamientos homogeneizados a nivel nacional con respecto a las declaraciones y opciones de privacidad. De hecho, el *Libro Blanco* expresa en todo momento su fuerte inclinación por un enfoque unificado y nacional de la privacidad y la seguridad de los datos mediante normas federales y la prioridad sobre las leyes estatales. En concreto, aduce que el mosaico de leyes estatales sobre vulneración de datos supone cargas que no conllevan beneficios acordes, y que la ampliación de la autoridad ejecutoria de la FTC reforzaría la homogeneización al reforzar el poder del regulador federal central.

Aunque el *Libro Blanco* recalca la importancia de la uniformidad nacional, no pretende sustituir ni refutar el papel o la idoneidad de las leyes federales específicas de cada sector que constituyen la ley sobre privacidad y seguridad actual de EE. UU. De hecho, el *Libro Blanco* confirma que el marco de privacidad existente de EE. UU. funciona bien, y que la aplicación individualizada de este protege de manera efectiva la privacidad del consumidor. Aun así, el *Libro Blanco* pide al Congreso que promulgue su «Declaración de Derechos de Privacidad del Consumidor», que otorgue mayor autoridad de aplicación y regulación a la FTC para el sector de la privacidad y que apruebe leyes federales sobre vulneración de datos que tengan prioridad sobre la miríada de leyes estatales en vigor en la actualidad. El *Libro Blanco* indica que la

mayoría de sus principios pueden aplicarse sin necesidad de legislar, y no queda claro si el Congreso emitirá legislación a este respecto con rapidez.

Resumiendo, el cerco de políticas estadounidenses sobre privacidad y seguridad de la información se halla en un estado considerable de cambio. Calificar la situación actual de la protección de datos en EE. UU. como cualquier cosa menos altamente sustantiva, ampliamente derivada y dinámica, sería, no obstante, impreciso o erróneo. Incluso el recientemente inactivo Consejo de Supervisión de la Privacidad y las Libertades Civiles, que operó en la Casa Blanca durante la Administración anterior, podría volver a ser resucitado pronto (fuera de la Casa Blanca como resultado de los cambios legislativos), pues el presidente Obama ha designado a un nutrido grupo de candidatos para este importante Consejo. De esta manera, aunque el ordenamiento jurídico estadounidense en materia de privacidad y seguridad de la información podría no ser ideal, parecería mucho más adecuado que otros muchos modelos alternativos. A continuación se analizan con brevedad las distintas leyes y garantías de la privacidad y seguridad en vigor en EE. UU.

3.3.2 Análisis

El modelo de privacidad y protección de datos estadounidense abarca diversas leyes específicas de cada sector y cada materia y leyes generales destinadas a una gama flexible de prácticas de privacidad y seguridad «desleales o fraudulentas» reforzadas por obligaciones del derecho consuetudinario impuestas por los litigantes del sector privado. En lugar de una única ley sobre privacidad integral o colectiva que regule la privacidad, la protección de datos y la seguridad de la información de todos los sectores industriales y categorías de datos, en EE. UU. existe una abundancia de leyes de protección de datos y seguridad de la información (incluyendo las leyes sobre privacidad específicas de cada sector), y las empresas se enfrentan a obligaciones de conformidad adicionales derivadas de las obligaciones generalizadas de impedir las conductas negligentes, las infracciones de la expectativa razonable de privacidad y las prácticas desleales o fraudulentas. Y, tal y como se comentara con anterioridad, todos los gobiernos de EE. UU. (tanto los federales como los estatales y los locales) están obligados a respetar el derecho de cada individuo a la privacidad de la información según la Cuarta Enmienda a la Constitución federal, que garantiza el «derecho de las personas a estar seguras en sus... papeles y pertenencias frente a cualquier inspección y allanamiento irrazonable».

La Ley de privacidad de 1974 protege también la información personal que recaba y mantiene el Gobierno federal. La Ley de privacidad estadounidense se considera comúnmente como la primera encarnación oficial de los principios y prácticas leales de la información que se han incorporado en muchos otros sistemas de protección de datos, incluyendo, por supuesto, la Directiva de protección de datos de 1995 de la Unión Europea.

EE. UU. ha sido pionero mundial no solo en la creación de modelos de normas de protección de datos gracias a la Ley de privacidad de 1974, sino también al imponer la notificación afirmativa de vulneración de datos y los requisitos de seguridad de la información a las entidades privadas que recaban o procesan los datos personales de los consumidores, los empleados y otros individuos. El Estado de California fue el primero en abrir camino en la seguridad de datos y notificación sobre la vulneración de datos al exigir a las empresas en 2003 que informaran a los individuos cuya información personal estuviera en peligro o se hubiera conseguido de manera indebida. Desde entonces, aproximadamente 47 estados, el distrito de Columbia y otras jurisdicciones estadounidenses y las agencias de la banca federal, sanidad y comunicaciones, han exigi-

do a las empresas que emitan notificaciones obligatorias sobre vulneración de datos e instauren medidas administrativas, técnicas y físicas que protejan la seguridad de la información personal sensible. También existen en otros estados docenas de otras leyes de privacidad médica y financiera.

El amplio régimen estadounidense de aplicación de la privacidad y protección de datos se halla documentado perfectamente en distintas publicaciones oficiales, incluyendo, de manera más notoria, los materiales proporcionados por EE. UU. a la UE en relación con el Puerto Seguro de Protección de Datos acordado entre las dos jurisdicciones en el 2000[105]. Está claro que desde el 2000 se han promulgado cantidad de leyes federales y estatales adicionales y se han adoptado otras normas en relación con la privacidad, la vulneración de datos, la seguridad de la información, la seguridad cibernética y se ha emitido una gran cantidad de sentencias judiciales, procesos ejecutorios y convenios financieros en la esfera de la privacidad. Y la Casa Blanca, el Ministerio de Comercio y la Comisión Federal de Comercio están considerando la creación de otros marcos reguladores.

A nivel federal, las obligaciones de protección de datos del sector privado pueden clasificarse en cuatro amplias categorías: tres sectores industriales específicos (las instituciones financieras, las entidades sanitarias y las compañías de telecomunicaciones) y una dimensión genérica que prohíbe a las empresas que comercian a nivel interestatal que cometan prácticas «desleales» o «fraudulentas», incluyendo las infracciones relativas a la intimidad y la seguridad de los datos. La FTC, la «reguladora de la privacidad» *de facto* en EE. UU., se encarga de la aplicación de la última categoría. Cabe mencionar además que los fiscales y los litigantes privados pueden aplicar las normas de privacidad según las normas análogas de «actos y prácticas desleales y fraudulentas» (UDAP) de la ley estatal.

En cuanto a la privacidad financiera, las agencias federales de la banca y la FTC han sido, hasta hace poco, responsables primarios de la ejecución de la Ley Gramm-Leach-Bliley (GLBA), que se aplica a las instituciones financieras. Después de la reciente legislación «Dodd-Frank», dichas leyes se aplicaron, en primer lugar, por parte de la nueva Junta de Protección Financiera del Consumidor (CFPB), que cuenta con facultades reguladoras y ejecutorias importantes e independientes. La FTC, no obstante, seguirá siendo la responsable principal de la administración de la Ley de Información Crediticia Imparcial y de las normas de los UDAP en virtud de la Ley de la FTC y la Ley de protección de la privacidad infantil *Online* (COPPA), que impone obligaciones positivas sobre privacidad a las entidades que recaben información personal de niños menores de trece años.

En cuanto a la privacidad de la Sanidad, las agencias del Ministerio de Sanidad y Servicios Sociales (HSS) administran y aplican la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA), modificada por la Ley de Tecnologías de la Información para la Salud Económica y Clínica (HITECH). Estas leyes no solo limitan el acceso y el uso de la información médica, sino que imponen además otras estrictas normas sobre seguridad de la información.

Para la privacidad de las comunicaciones, la Comisión Federal de Comunicaciones (FCC, del inglés Federal Communications Commission), el Ministerio de Justicia y, hasta cierto punto, los litigantes privados pueden aplicar las normas de protección de datos establecidas por la Ley de Privacidad de las Comunica-

105. Los documentos descritos por la Ley de privacidad y las autoridades ejecutorias de EE. UU., a partir del 2000, se incluyeron en la siguiente página web del Ministerio de Comercio de EE. UU. donde pueden consultarse: http://export.gov/safeharbor/eu/eg_main_018493.asp.

ciones Electrónicas, la Ley de fraude y abuso informático y las distintas leyes sobre Comunicaciones. Estas leyes criminalizan o prohíben y otorgan extensos derechos privados de demanda contra cualquier intercepción o adquisición ilegal de comunicaciones, el pirateo o acceso no autorizado a ordenadores y la divulgación de la información personal del consumidor sin su consentimiento. Otras leyes adicionales, como la Ley de protección del consumidor telefónico (que prohíbe los faxes no deseados), la Ley CAN SPAM (que restringe el envío de correos electrónicos comerciales no solicitados), la Ley de protección de la privacidad audiovisual (que evita el acceso a registros de alquiler de vídeos) y otras normas de la FTC y la FCC que han creado un registro denominado «Do Not Call» para evitar llamadas de marketing telefónico no deseadas, ayudan a proteger también la privacidad de la información de los individuos.

Incluso la colección de leyes de privacidad descritas con anterioridad no es exhaustiva. Cabe mencionar además que existen otras leyes de privacidad a nivel federal para tipos especiales de información, incluyendo los expedientes académicos, los registros de conductores y vehículos motorizados, las investigaciones de antecedentes, los informes de crédito del consumidor, etc. Además, cada agencia federal debe contar con un oficial de privacidad, y el Consejo de Supervisión de la Privacidad y las Libertades Civiles informa al Presidente y ofrece una orientación, supervisión y coordinación de alto nivel sobre las implicaciones de las actividades contra el terrorismo y de contrainteligencia.

Además de las leyes sobre la vulneración de datos y la seguridad de la información descritas con anterioridad, muchos estados cuentan con diversos requisitos de privacidad adicionales, incluyendo la obligación de publicar políticas sobre privacidad *online*, de proteger un tipo de información concreta (como los números de la seguridad social), los resultados de pruebas genéticas, el historial crediticio, la información sobre la infección o no con el virus de la inmunodeficiencia humana (VIH), etcétera. Y quizá de mayor importancia es la capacidad de los individuos que crean que se ha vulnerado su derecho a la privacidad de denunciar, con arreglo al derecho consuetudinario, delitos tales como la intromisión en la intimidad, la divulgación pública de hechos privados, intrusiones no autorizadas, difamación, calumnias y, evidentemente, por simple negligencia o allanamiento.

A raíz de este breve resumen, el análisis que sigue amplía ciertas áreas específicas de especial interés en lo que respecta a la privacidad.

3.3.3 Protección del consumidor

El Artículo 5 de la Ley de la FTC, 15 U.S.C. § 45(a)(1), prohíbe «los actos o prácticas desleales o fraudulentos relacionados con el comercio». Aunque la Ley de la FTC no regula expresamente la privacidad o la seguridad de la información, la FTC aplica el Artículo 5 a la privacidad de la información, la seguridad de los datos, la publicidad *online*, el seguimiento conductual y otras actividades comerciales en las que se vean implicados los datos. La FTC ha iniciado procesos judiciales satisfactorios según el Artículo 5 contra empresas que no publicaron en debida forma sus prácticas de recopilación de datos, que no cumplieron con las promesas contenidas en sus políticas de privacidad, que no se atuvieron a sus compromisos en materia de seguridad o que no proporcionaron un nivel «justo» de seguridad para la información del consumidor.

Según el Artículo 5, un acto o práctica se considera fraudulento si: a) existe una revelación u omisión de información que pudiera inducir a error a cualquier consumidor que actúe de manera razonable según esas circuns-

tancias concretas, y b) la revelación u omisión es «sustancial», es decir, si se trata de un acto o práctica «que pudiera afectar a la conducta o decisión del consumidor en lo tocante a un producto o servicio». Todo acto o práctica se considera «desleal» según el Artículo 5 si provoca o es susceptible de provocar daños materiales a los consumidores sin posibilidad de evitarlo en la medida de lo razonable y si carece de las ventajas que lo compensen tanto para los consumidores como frente a la competencia.

La FTC opina que las empresas deben revelar sus prácticas sobre privacidad de manera adecuada, y en ciertas circunstancias, que deben comunicarlo de manera oportuna, clara y destacada, en especial en caso de usos nuevos, inesperados o delicados. La FTC entabló diligencias en 2009 contra Sears por supuesta falta de revelación adecuada del alcance en que recopilaba la información personal al rastrear la navegación por la red de consumidores que descargaban cierto software. La información de los consumidores supuestamente recopilada incluía «casi todo el comportamiento en Internet que tiene lugar en [...] los ordenadores». La FTC exigió a Sears que revelara de forma destacada todas las prácticas de los datos que pudieran tener repercusiones inesperadas de importancia en una pantalla independiente fuera de cualquier contrato de usuario, política de privacidad o condiciones de uso.

Se entiende de manera generalizada que el Artículo 5 prohíbe además a las empresas que utilicen los datos personales previamente recopilados de forma sustancialmente distinta a la que se informara inicialmente al sujeto registrado y sin haber conseguido su consentimiento previo adicional.

La FTC ha emitido una extensa guía sobre la publicidad basada en el comportamiento *online* a través de la cual recalca los cuatro principios para la protección de la privacidad del consumidor: a) transparencia y control, al informar de manera significativa a los consumidores y darles la opción de elegir si desean que se recopile su información; b) preservar la seguridad de los datos y limitar la retención de estos; c) el consentimiento expreso antes de usar la información de manera sustancialmente distinta a la indicada en la política de privacidad en vigor en el momento de la recopilación de los datos, y d) el consentimiento expreso antes de usar cualquier dato sensible con fines de publicidad basada en la conducta. No obstante, el informe de la FTC no requiere el consentimiento de inclusión voluntaria para el uso de información no sensible en la publicidad basada en la conducta.

3.3.4 Privacidad en las comunicaciones

La Ley de privacidad de las comunicaciones electrónicas de 1986 (ECPA) protege la privacidad y seguridad del contenido de ciertas comunicaciones electrónicas y registros relacionados. La ECPA está formada por otras tres leyes independientes. La Ley de intervenciones prohíbe la intercepción o divulgación de «comunicaciones electrónicas» mientras se estén transmitiendo o emitiendo o el uso de comunicaciones interceptadas de manera ilegal. La Ley de comunicaciones almacenadas prohíbe el acceso o divulgación intencionados y no autorizados de las comunicaciones almacenadas o los registros protegidos. La Ley de registro de llamadas salientes prohíbe el uso del mismo o de un dispositivo de control y rastreo de llamadas para grabar la «información de marcación, asignación de ruta, destino o señalización» distinta al contenido y sin haber conseguido previamente una orden judicial.

La Ley de fraude y abuso informático (CFAA), 18 U.S.C. § 1030 et seq., prohíbe el pirateo y otras formas de acceso o intrusión no autorizados y perjudiciales en sistemas informáticos, y a menudo se apela a ella cuando expertos internos desleales o crimi-

nales cibernéticos intentan robar secretos comerciales o malversar información corporativa de valor localizada en redes informáticas de empresa.

3.3.5 Privacidad de la sanidad

La HIPAA se aplica a las «entidades cubiertas», entre las que se encuentran los planes de salud, los centros de intercambio de información sanitaria y el personal sanitario implicado en transacciones electrónicas así como, a través de la HITECH, los proveedores de servicios de entidades cubiertas que necesiten acceder a la información sanitaria protegida para poder realizar sus labores. Impone además varios requisitos relacionados con el seguro médico de los empleados.

«Información sanitaria protegida» se define extensamente como la «información sanitaria identificable individualmente», «transmitida o guardada en medios electrónicos» o en «cualquier otro formato o medio». La «información sanitaria que identifica al individuo» se define como un subconjunto de información sanitaria que incluye datos demográficos que «se creen o reciban por parte de un proveedor sanitario, un plan médico, un empresario o un centro de intercambio de datos sanitarios»; y «está relacionada con la salud o situación física o mental, tanto pasada como presente o futura, de un individuo; la prestación de asistencia sanitaria a un individuo; el pago pasado, presente o futuro de las prestaciones sanitarias a un individuo» y que bien identifique al individuo o que proporcione los medios razonables por los que se le pueda identificar. La HIPAA no se aplica a la información no identificable.

Una «entidad colaboradora» es una entidad que hace las veces o ayuda a una entidad cubierta en el cumplimiento de una función o actividad que implique el uso o revelación de información sanitaria protegida (incluyendo, a modo de ejemplo, el tratamiento de reclamaciones o las actividades administrativas). Las entidades asociadas deben celebrar contratos, llamados contratos de entidades colaboradoras, por los que se exige a estas que usen y divulguen la ISP solo si así se permite o lo exige el contrato de entidad colaboradora o la ley y que implanten las medidas de protección adecuadas que prevengan el uso o revelación de la ISP fuera de lo establecido en el contrato de entidad colaboradora, aparte de contener otras cláusulas de confidencialidad, integridad y disponibilidad de la ISP.

3.3.6 Privacidad financiera

La Ley de modernización de los servicios financieros de 1999 se conoce como la Ley Gramm-Leach-Bliley (GLBA). La GLBA regula la privacidad y seguridad de la información financiera mediante la creación de normas que protegen la «información personal de carácter privado» (o información financiera que permite la identificación personal) almacenada por las «entidades financieras» y exigiendo a estas que informen sobre sus prácticas de divulgación de la información. En resumen, la GLBA exige a las entidades financieras: que avisen sobre las políticas y prácticas relativas a la revelación de información personal; que prohíban la revelación de dichos datos a terceros independientes a menos que se ofrezca a los consumidores la opción de exclusión voluntaria de dicha revelación o se apliquen otras excepciones; y que instauren medidas que protejan la seguridad de la información personal.

La Ley de información crediticia imparcial (FCRA), 15 U.S.C. § 1681, et seq., enmendada por la Ley de transacciones crediticias justas y exactas de 2003 (FACTA), impone restricciones a las entidades que posean o guarden información crediticia del consumidor o información generada a raíz de informes crediticios del consumidor. Los informes del consumidor son «toda comunicación escrita, verbal o de cualquier otro tipo de información de una agencia de informes de crédito para el consumidor que incluya la solvencia de un consumi-

dor, su situación crediticia, su capacidad crediticia, su carácter, su reputación general, sus características personales o su estilo de vida y que se use o se vaya a usar o recabar en su totalidad o en parte a los fines de servir como factor determinante de la idoneidad del consumidor» a la hora de solicitar un crédito, un seguro, empleo o demás cuestiones similares.

3.3.7 Privacidad en el puesto de trabajo

Los empresarios estadounidenses han disfrutado por lo general de una amplia potestad a la hora de controlar sus propios sistemas informáticos, incluyendo el uso de dichos sistemas por parte de los empleados. Esta potestad suele incluir la capacidad de controlar el uso por parte de los empleados de los sistemas informáticos por motivos personales, tanto con el fin de conservar y proteger los equipos informáticos de los empleados como para calcular la productividad de estos o garantizar que no hagan un uso indebido de los sistemas de manera que pudieran perjudicar a otros o exponer al empresario a cualquier responsabilidad. Sin embargo, algunos límites sobre la capacidad de controlar a los empleados en su puesto de trabajo están cambiando.

En general, la posibilidad de controlar al empleado depende de si este último disfruta de una expectativa razonable de privacidad. El Tribunal Supremo ha reconocido que los empleados tienen un interés legítimo a la hora de controlar el lugar de trabajo. Cuando los empresarios proporcionan a sus empleados una política e información clara sobre las actividades de control, se entiende por lo general que eliminan cualquier expectativa razonable de privacidad del empleado.

3.3.8 Conclusión

El campo de la privacidad y la protección de datos en EE. UU. está sujeto a una extensa y creciente legislación así como a las omnipresentes normas y procesos ejecutorios de la FTC, a otras agencias federales, los fiscales del Estado y los demandantes privados. Las demandas ejecutorias y las demandas colectivas multimillonarias así como los acuerdos en demandas colectivas son cada vez más frecuentes a causa de vulneraciones graves de datos o abusos de datos a raíz de los cuales los individuos se exponen a un peligro concreto y no meramente especulativo o remoto. No obstante, los tribunales se han mostrado escépticos cuando las demandas por privacidad han alegado teorías vagas sobre lesiones o en los casos en que las empresas legítimas utilizan los datos de los consumidores para prácticas de marketing de naturaleza bastante corriente. Y lo que es más, se reconoce por lo general que gran cantidad del material «gratuito» de Internet está sustentada por la capacidad de los publicistas de orientar sus mensajes a (y en beneficio último de) unos consumidores potencialmente receptivos.

El anterior análisis demuestra que el sistema de privacidad y protección de datos estadounidense no solo es sólido, sino que también ha sido líder mundial en cuanto a implantación de principios leales de la información, de seguridad de la información y de requisitos de notificación sobre vulneraciones de datos. Aunque el mercado y el estamento político de EE. UU. están bastante familiarizados con muchos de los tipos de publicidad y marketing personalizados y la garantía que establece la Primera Enmienda a la libertad de expresión protege a una extensa serie de comunicaciones comerciales y recopilaciones de información, existen también otras tendencias estrictas que exigen la transparencia, la publicación y la equidad en las prácticas relativas a los datos. La normativa sobre privacidad en EE. UU., al igual que en Europa, Asia y el resto del mundo, se encuentra, inevitablemente, en un estado de gran agitación. Mientras la era de la información siga generando innovaciones y revolu-

ciones comerciales a un ritmo frenético, las comunidades interesadas en la protección de datos seguirán a la contienda.

3.3.9 Apéndice: Choice Point 2006 10-K Divulgación denunciada ante la Comisión de Bolsa y Valores de EE. UU. (Extractos relacionados por la privacidad/seguridad de los datos)[106]

En febrero de 2006 alcanzamos un acuerdo con la FTC para poner fin a una investigación de dicha entidad sobre nuestro cumplimiento de las leyes federales que regulan la seguridad de la información del consumidor y otros temas relacionados, incluyendo incidentes fraudulentos de acceso a los datos. La sentencia final decretada y la orden de sanciones civiles, suspensión definitiva y otros recursos en equidad (en adelante la «orden decretada») nos exigía pagar 10 millones de dólares a modo de sanción y una reparación al consumidor de 5 millones de dólares. La orden decretada nos requería, además, que institucionalizáramos una serie de prácticas de seguridad de la información, de verificación y credenciales, de auditoría y conformidad y de emisión de informes y retención de registros. Además, se nos conminó a obtener, cada dos años y durante un plazo de veinte años, una evaluación de un profesional cualificado, independiente y externo por el que se garantice que nuestro programa de seguridad de la información cumple con lo dictaminado por la orden decretada. Ya hemos aplicado ciertas mejoras operativas y estamos buscando otras medidas adicionales destinadas a cumplir la orden decretada. Cualquier incumplimiento de la orden decretada podría afectar de manera adversa a nuestra empresa, operaciones y buen nombre.

Punto 3. Procedimiento judicial

A continuación se incluye una descripción del procedimiento judicial pendiente de la sociedad. Aunque la resolución última de las cuestiones que se comentan a continuación no puede determinarse en la actualidad, cualquier resultado desfavorable en tales casos podría provocar un importante perjuicio a la situación financiera o los resultados de las operaciones de la sociedad.

Demandas colectivas

El 11 de agosto de 2003 se interpuso una demanda colectiva contra la sociedad ante el Tribunal de Primera Instancia del Distrito Sur de Florida, EE. UU. (Fresco, et al. contra Automotive Directions Inc., et al.) por la que se alegaba que la sociedad había obtenido, revelado y utilizado información obtenida del Departamento de Seguridad Vial y Vehículos Motorizados de Florida (DHSMV). Los demandantes pretendían representar a clases de individuos de los que se hubiera obtenido, revelado y utilizado información personal contenida en los registros del DHSMV de Florida con fines de marketing u otros usos supuestamente permitidos por parte de ChoicePoint sin el consentimiento expreso de cada individuo. Varias empresas de la competencia de la sociedad también han sido demandadas dentro del mismo pleito u otro similar en Florida. Este litigio pretende conseguir la calificación de demanda colectiva, además de daños y perjuicios, los honorarios y gastos de representación jurídica y otras medidas cautelares y diversas. ChoicePoint se ha unido a otros demandados y ha presentado una petición de sentencia según los alegatos de la defensa de que los demandantes hubieran «buscado» la demanda. Hasta la fecha, el tribunal no se ha pronunciado sobre dicha petición. Tras defenderse enérgicamente contra la demanda, los demandados

106. Puede consultarse en: http://www.secinfo.com/d14D5a.u19qb.htm

que comparecieron ante el tribunal solicitaron mediación a comienzos de febrero del 2006. Se presentó una propuesta de acuerdo ante el tribunal el 20 de diciembre del 2006 y las partes de la conciliación todavía esperan que se programe la vista de aprobación preliminar del acuerdo. La sociedad cree que cualquier responsabilidad adicional que pudiera derivarse de la resolución de este pleito y que pudiera superar las cantidades estipuladas no ejercerá efecto sustancial sobre la situación financiera, los resultados de las operaciones ni los flujos de caja de la sociedad.

El 5 de enero del 2007 se formuló una pretendida demanda colectiva contra la sociedad y algunas de las empresas de la competencia ante el Tribunal de Primera Instancia del Distrito Este de Texas (Taylor contra Acxiom Corporation) en nombre de cada uno de los individuos del estado de Texas cuyo nombre, dirección, número de carné de conducir y otros datos de identificación constaban en los registros de vehículos motorizados que obtuvieron los demandados del Departamento de Seguridad Pública de Texas sin el consentimiento expreso de cada individuo durante el período transcurrido entre el 1 de junio del 2000 y hasta la fecha de la sentencia. El demandante presentó además alegatos solicitando formar parte del litigio Fresco y oponiéndose al acuerdo propuesto para dicho litigio. Dicho demandante solicitó además que se dictara auto de sobreseimiento del litigio Fresco a expensas del resultado de la determinación de calificación colectiva del caso Taylor por parte del tribunal de Texas. El 8 de febrero del 2007, la sociedad presentó una solicitud de desestimación de la demanda Taylor basándose en el hecho de que se había interpuesto en primer lugar la demanda Fresco, que la demanda colectiva a nivel nacional Fresco abarcaba la demanda colectiva de Texas, y que, por motivos de economía procesal y principios fundamentales de equidad, no cabía la duplicación de las demandas colectivas en tribunales federales.

Acceso fraudulento a los datos

El análisis de ChoicePoint sobre el acceso fraudulento a los datos descrito en los archivos públicos de la sociedad y otros incidentes similares sigue su curso. La sociedad cree que la cantidad de consumidores a los que enviará notificación sobre un posible acceso fraudulento a los datos podría ser mayor que la cantidad de consumidores a los que ya ha informado, pero no cree que dicho aumento sea relevante.

La sociedad está envuelta en varios procedimientos judiciales o investigaciones relacionados con esas cuestiones. ChoicePoint no puede predecir en este momento el resultado de dichos procesos. La resolución final de esas cuestiones podría ejercer una incidencia negativa importante sobre los resultados financieros, la situación financiera y la liquidez de la sociedad, así como en el precio de cotización de las acciones ordinarias de esta. Independientemente de los fundamentos y del resultado final de dichas demandas y otros procedimientos, los litigios y procesos de este tipo suelen ser caros y exigen la dedicación de muchos recursos de la sociedad y tiempo de los altos directivos para defenderse ante estas causas.

ChoicePoint ha llegado a un acuerdo con la FTC con respecto a esta investigación sobre el cumplimiento por parte de la sociedad de las leyes federales que rigen la seguridad de la información del consumidor y otros temas relacionados, incluyendo el acceso fraudulento a los datos que tuvo lugar en el 2004. Los términos del acuerdo exigían una sanción civil no deducible a efectos fiscales de 10 millones de dólares, la creación de un fondo de 5 millones de dólares que administraría la FTC para iniciativas de resarcimiento de los consumidores, la ejecución de ciertas actividades de acreditación puntuales y continuadas de los consumidores, tales como certificaciones adicionales y visitas sobre el terreno, y la asunción de otras obligaciones complementarias relacionadas con la seguri-

dad de la información. Además, el acuerdo exigió a ChoicePoint que obtenga, cada dos años durante un plazo de veinte años, una evaluación de un profesional cualificado, independiente y externo por el que se garantice que su programa de seguridad de la información cumple con lo dictaminado por la orden decretada. Como parte de este acuerdo, ChoicePoint no admitió la veracidad ni responsabilidad por las cuestiones alegadas por la FTC. En el cuarto trimestre del 2005, la sociedad registró un cargo antes de impuestos de 8 millones de dólares (8,8 millones de dólares después de impuestos) correspondiente al acuerdo con la FTC que representaba una sanción civil de 10 millones de dólares, el fondo de 5 millones de dólares para las iniciativas de resarcimiento de los consumidores y un cargo de 4 millones de dólares para otras obligaciones adicionales según la orden compensados por 11 millones de dólares de beneficios de los seguros. La sociedad percibió los beneficios de los seguros en el primer trimestre del 2006.

La sociedad ha recibido además diversas consultas y peticiones de fiscales como resultado del acceso fraudulento a los datos. Por lo general, los fiscales piden que todos los individuos afectados de cada estado correspondiente reciban la notificación conveniente. La sociedad ha enviado notificaciones por correo a los posibles consumidores afectados identificados hasta la fecha. Asimismo, algunos fiscales han solicitado información y documentos, incluso mediante el uso de citaciones, con el fin de determinar si ChoicePoint ha infringido alguna ley relativa a la protección del consumidor y asuntos relacionados. La sociedad está colaborando con los fiscales en lo tocante a estas solicitudes.

La Comisión de la Bolsa y Valores (CBV) de EE. UU. Envió, el 12 de mayo del 2005, a ChoicePoint una notificación por la que le informaba de que estaba efectuando una investigación de las circunstancias en torno a una posible usurpación de la identidad que comerciaba con los valores de ChoicePoint a través de su director general y su director de operaciones. La sociedad colaboró con la CBV y aportó la información y documentos solicitados.

La sociedad ha sido objeto de una supuesta demanda colectiva derivada de la fusión de cuatro demandas colectivas anteriores presentadas ante el Tribunal de Primera Instancia del Distrito Central de California[107]. La Primera Demanda Colectiva Enmendada y Fusionada del demandante contra ChoicePoint Inc. y tres subsidiarias alega infracciones de la FCRA y otras leyes de California. Los seis demandantes designados pretenden hacer valer la demanda en nombre de un grupo de personas a nivel nacional sobre quienes ChoicePoint entregó un informe, de consumo tal y como se describe en la FCRA, a consumidores deshonestos, así como en nombre de cinco clases de personas afectadas en California. Los demandantes exigen daños y perjuicios efectivos, legítimos y punitivos así como medidas de desagravio, los honorarios de representación jurídica y las costas. El 10 de julio del 2006, el Tribunal de Primera Instancia fusionó la causa Harrington con la causa Wilson, tal y como se describe a continuación. Estas causas siguen su cauce por separado, pero el juez las está considerando como una única causa.

El 15 de junio del 2005 se interpuso contra ChoicePoint Inc. otra pretensión de demanda colectiva similar ante el Tribunal de Primera Instancia del Distrito Norte de Georgia, División de Atlanta, Wilson contra ChoicePoint Inc., 1-05-CV-1604. Los demandantes alegaron infracción de la FCRA, la DPPA y la Ley uniforme de prácticas comerciales fraudulentas de Georgia (DTPA), y los demandantes comparecientes pretendían re-

107. Harrington, et al. contra ChoicePoint, CV05-1294

presentar a un colectivo nacional de personas cuyos informes crediticios de consumo, tal y como los define la FCRA, o su información personal o altamente restringida tal y como lo define la DPPA, se había revelado a terceros como resultado de actos u omisiones por parte de ChoicePoint. Los demandantes exigían daños y perjuicios efectivos, legítimos y punitivos así como medidas de desagravio, los honorarios y las costas. El 28 de febrero del 2006, el tribunal aceptó la petición de ChoicePoint de transferir la causa Wilson al Tribunal de Primera Instancia del Distrito Central de California. La sociedad presentó una solicitud de fallo sumarial parcial el 10 de agosto del 2006. El Tribunal aceptó dicha solicitud el 12 de octubre del 2006 en relación con las pretensiones de seis de los nueve demandantes. La sociedad pretende defenderse enérgicamente del resto de las pretensiones.

El 4 de marzo del 2005, un comprador de valores de la sociedad presentó una demanda contra la sociedad y varios de sus ejecutivos ante el Tribunal de Primera Instancia del Distrito Central de California. La demanda alegaba que los demandados habían infringido leyes federales sobre valores al emitir información falsa o engañosa en relación con el acceso fraudulento a los datos. Se han interpuesto otras demandas con pretensiones similares por parte de otros compradores de los valores de la sociedad ante el Distrito Central de California, el 10 de marzo del 2005, y el Distrito Norte de Georgia, el 11 de marzo del 2005, el 22 de marzo del 2005 y el 24 de marzo del 2005. Un auto judicial ha remitido las causas pendientes del Distrito Central de California al Distrito Norte de Georgia. Mediante resolución judicial de 5 de agosto del 2005, el tribunal fusionó cada una de las causas pendientes en una única demanda consolidada, en la causa del Litigio sobre Valores de ChoicePoint Inc., 1:05-CV-00686. El 13 de enero del 2006 se interpuso una Demanda Consolidada Enmendada que pretendía la calificación como demanda colectiva y otros daños y perjuicios sin especificar, honorarios de representación legal, costas y otras medidas de resarcimiento. El 14 de marzo del 2006, los demandados presentaron una solicitud de desestimación de la Demanda Consolidada Enmendada, que sigue pendiente de respuesta del tribunal. El 21 de noviembre del 2006, el tribunal emitió resolución por la que denegaba la solicitud de desestimación de los demandados. Por tanto, los demandados se personaron en el juzgado para solicitar una revisión inmediata de dicha resolución. El tribunal accedió a dicha solicitud el 10 de enero del 2007. El 25 de enero del 2007 los demandados presentaron una solicitud por la que rogaban al Tribunal Federal de Apelación nº 11 que les permitiera presentar una apelación con carácter interlocutorio. La respuesta del demandado se presentó el 16 de febrero del 2007. Si el Tribunal Federal de Apelación nº 11 admite a trámite la solicitud del demandado, entonces este establecerá un plazo de presentación de la apelación del demandado a la resolución del 21 de noviembre. El tribunal de primera instancia declaró el cierre administrativo del caso a expensas de la resolución pendiente de la apelación interlocutoria. En consecuencia, todos los procedimientos del tribunal de primera instancia están en este momento suspendidos. La sociedad pretende defenderse enérgicamente ante este pleito.

El 20 de mayo del 2005, se interpuso una supuesta demanda colectiva ante el Tribunal de Primera Instancia del Distrito Norte de Georgia contra ChoicePoint y ciertos individuos a quienes se acusó ser fiduciarios del Plan de Distribución de Beneficios (en adelante «el Plan») de ChoicePoint Inc. 401(k), en la causa de Curtis R. Mellott contra ChoicePoint Inc., et al., 1:05-CV-1340. La demanda alegaba infracciones de las normas fiduciarias ERISA a través de la adquisición y retención de acciones de ChoicePoint por parte del Plan a partir del 24 de noviembre del 2004. Los demandantes solicitaban daños y perjui-

cios, medidas de resarcimiento y otras reparaciones en equidad, los honorarios de representación jurídica y las costas. El 14 de abril del 2006, los demandados presentaron una solicitud de desestimación que sigue pendiente de respuesta del tribunal. La sociedad pretende defenderse enérgicamente de estas acusaciones.

El 27 de junio del 2005 se notificó a la sociedad que se había presentado contra ella una demanda derivada de los accionistas. El pleito inicial se interpuso ante el Tribunal Superior del Condado de Gwinnett, Georgia, y este alegaba que algunos de los altos ejecutivos de la sociedad habían incumplido sus obligaciones fiduciarias al abusar de la información privilegiada, y exigía daños y perjuicios sin especificar, honorarios de representación jurídica, costas y otras medidas de desagravio. El 6 de julio del 2005 se interpuso otra demanda derivada de los accionistas ante el Tribunal Superior del Condado de Fulton, Georgia, y esta alegaba que algunos de los altos ejecutivos de la sociedad habían cometido abusos de la información privilegiada y que todos los miembros del consejo habían incumplido sus obligaciones fiduciarias al no supervisar de forma adecuada las operaciones de la sociedad. El litigio del condado de Gwinnett se transfirió seguidamente al condado de Fulton, y el Tribunal Superior del Condado de Fulton fusionó los dos casos en una única demanda, la Demanda Derivada de ChoicePoint Inc., 2005-CV-103219. Los demandantes exigían daños y perjuicios efectivos y punitivos sin especificar, los honorarios de representación jurídica, las costas y otras medidas de resarcimiento. El 12 de enero del 2006, la sociedad solicitó la desestimación y respondió a la Demanda Consolidada Enmendada. El Tribunal admitió a trámite la solicitud de desestimación de la sociedad y desestimó la demanda el 8 de junio del 2006. El 28 de junio del 2006, los demandantes apelaron dicha desestimación de la demanda ante el Tribunal de Apelación de Georgia. La apelación de los demandantes se ha instruido por completo y sigue pendiente de respuesta del Tribunal de Apelación de Georgia.

La sociedad sigue reforzando sus procedimientos de acreditación de los clientes y está entregando nuevas acreditaciones a los miembros de su base de clientes, en especial a aquellos con acceso a los productos regulados por la Ley de información crediticia imparcial. Es más, la sociedad sigue analizando e investigando otras cuestiones relacionadas con la acreditación y el uso de los clientes. Las investigaciones de la sociedad así como las relativas al cumplimiento de la ley siguen su curso. La sociedad cree que podrían existir otras instancias que podrían requerir la notificación a los consumidores. Tal y como se ha confirmado con anterioridad, la sociedad desea notificar a los consumidores, independientemente de que así lo exija la legislación estatal en vigor, si averiguara que otras entidades no autorizadas han adquirido información personal sensible que pudiera identificarles. La sociedad no cree que el hecho de notificar a los consumidores afectados ejerza un impacto importante sobre su situación financiera, los resultados de las operaciones o los flujos de caja.

Alexander Alvaro

Alexander Alvaro, MPE (FDP/ALDE) es vicepresidente del Parlamento Europeo y, desde su elección en 2004, es miembro activo de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de la Comisión de Industria y del Comité Presupuestario. Está al tanto e informa a los liberales del Parlamento Europeo sobre el nuevo proceso legislativo en materia de protección de datos.

3.4 *Cookies*, consentimiento previo y la Directiva sobre la privacidad y las comunicaciones electrónicas

Alexander Alvaro
Vicepresidente del Parlamento Europeo

3.4.1 Introducción

La Directiva de la UE sobre la privacidad y las comunicaciones electrónicas (2009/136/CE) fue modificada en el año 2009 como medida incluida dentro de un paquete mayor de reformas de la legislación sobre comunicaciones electrónicas de la UE.

Como ponente del Parlamento, mi intención ha sido la de asegurar que el delicado equilibrio entre la privacidad y la seguridad permanezca intacto, garantizando al mismo tiempo un marco practicable para los modelos empresariales existentes y los nuevos e innovadores. El marco regulador de las comunicaciones electrónicas ya ha entrado en vigor, pero todavía parecen existir ciertas dudas con respecto a la implantación de la parte de la Directiva sobre la privacidad y las comunicaciones electrónicas que afecta a las *cookies*.

Gracias, en parte, a los avances tecnológicos, ha tenido lugar un crecimiento exponencial de la cantidad de bases de datos de los sectores público y privado. Las personas entregan sus datos personales a cambio de servicios y productos. Reservan billetes de avión y hoteles, compran cosas, presentan las declaraciones de impuestos, buscan pareja o amigos, solicitan opinión médica, contratan seguros o se unen a clubes, y todo ello en Internet. Hacen llamadas de teléfono y envían mensajes de texto, y con los móviles mandan correos, navegan por Google, usan tarjetas de crédito, hacen pagos *online*, sacan libros y CD de la biblioteca y consiguen tarjetas de fidelidad de los centros comerciales. En la calle y en lugares públicos los movimientos de las personas no solo se registran, sino que además podrían ser analizados por cámaras y micrófonos inteligentes capaces de grabar cada mínima inflexión vocal o movimiento muscular y de decidir si son sospechosos o no de algo.

Durante todo el día cada individuo está dejando su rastro. Sin darnos cuenta, nuestra vida y nuestras acciones pueden reconstruirse hasta el detalle más ínfimo y personal. La normativa sobre privacidad y derechos de la ciudadanía actuales se crea para un territorio específico, por lo general el territorio de una nación. Pero los datos personales pueden dar la vuelta al mundo en una fracción de segundo.

Conforme aumentan el uso de Internet y la prestación de servicios y contenido *online* y se convierten cada vez más en parte de nuestras vidas, cada uno de nosotros debería conocer los parámetros y las consecuencias de sus acciones *online*. Puesto que el comercio electrónico y todos los bienes y servicios relacionados

con él, las redes sociales, el correo electrónico, la «nube», la banca y equipos *online* permiten acceder a estos servicios en todo momento, los usuarios deben disponer al menos de una comprensión razonablemente sólida sobre su propia «huella» en la Red y sobre lo que pueden y deben hacer para garantizar su privacidad. En un entorno de complejidad creciente, tanto la legislación como la información de los usuarios deben ir acordes con los tiempos. En especial, debe garantizarse en todo momento una protección adecuada de los datos dentro de un contexto más amplio de derechos del consumidor y libertad de elección para los 500 millones de ciudadanos de la UE.

3.4.2 Las *cookies* en la revisión del marco de las comunicaciones electrónicas

El objetivo de la revisión del 2009 sobre la legislación existente en materia de telecomunicaciones consistía en mejorar la seguridad y la integridad en la red, aumentar la protección de los datos personales de los usuarios y mejorar las medidas de bloqueo del correo no deseado y los ataques cibernéticos. Por primera vez en la legislación europea se introdujo la definición de «violación de los datos personales» y el requisito de notificación de dicha violación.

La Directiva sobre la privacidad y las comunicaciones electrónicas, dentro de sus estipulaciones sobre la protección y seguridad de los derechos de los usuarios, introdujo el principio del consentimiento informado. El Artículo 5(3) y la parte expositiva acompañante a la Directiva sobre la privacidad y las comunicaciones electrónicas se modificaron específicamente para evitar los programas espía *(spyware)*. En su texto original, exigía el consentimiento previo del usuario o suscriptor de un servicio antes de que se almacenara la información en un terminal o se solicitara acceso a la información ya almacenada. La exigencia del consentimiento previo se estableció principalmente con el fin de incrementar la transparencia y la concienciación del usuario en cuanto a que sus datos personales podrían estar ofreciéndose o poniéndose en peligro sin su conocimiento y podría tener acceso a ellos cualquier tercero sin necesidad de proceso adicional. Al dar su consentimiento, los usuarios tienen la facultad de elegir si desean compartir sus datos o conceder acceso a ellos.

La mayoría de los usuarios probablemente encuentren muy complicado encontrar la información adecuada sobre cualquier página web (si es que realmente la hubiera), y de hacerlo, seguramente no comprendan la jerga legal de las 48 páginas en letra pequeña. Para que el consumidor pueda disfrutar de la opción de elegir de forma transparente y de levantar la guardia ante los ataques espía o el software malicioso e incluso el uso no intencionado de sus datos personales por parte de terceros, debe proporcionarse una información clara y comprensible que permita a los consumidores poder conceder un consentimiento real.

En sus debates a este respecto, el Parlamento Europeo decidió rechazar la expresión «consentimiento previo» a favor de un texto que permitiera una mayor flexibilidad. Esto se refleja especialmente en la adopción del considerando 66, el cual pretendía aclarar que los parámetros del navegador configurados por el usuario o suscriptor podrían considerarse como un indicio de consentimiento. En su texto original, tal y como lo propuse, el requisito de consentimiento a través de los parámetros del navegador se incluía asimismo en la modificación correspondiente del Artículo 5(3). El pasaje en cuestión sencillamente se desplazó al considerando y fue modificado por la Comisión y el Consejo durante las negociaciones del paquete completo. Este es el motivo por el cual la forma más sencilla en que los usuarios pueden dar su consentimiento adaptando los parámetros del navegador ya no es parte del texto legislativo en sí, sino que se explica en el considerando 66.

Este hecho parece haber creado cierta confusión entre los analistas con respecto a la im-

plantación de la directiva. Mientras que el considerando 65 es muy claro al avisar sobre los riesgos de los programas espía y la necesidad de informar adecuadamente al usuario, el considerando 66 profundiza sobre la manera en que la información del consumidor y su consentimiento informado pueden llevarse a efecto. La excepción al requisito del consentimiento se permite tan solo para fines técnicos exclusivos de almacenamiento, y el texto cita de forma muy clara que siempre que sea «técnicamente posible y eficaz», los parámetros por defecto del navegador y otras aplicaciones constituyen una forma de conceder el consentimiento. Si se leen el Artículo 5(3) y el considerando 66 en conjunto, cualquier duda con respecto a la intención y viabilidad del requisito de consentimiento debería quedar despejada.

Si el Parlamento hubiera exigido que la activación de todas las *cookies* en el equipo de los usuarios requiriera el consentimiento «previo» o «explícito» de ellos, se hubiera adoptado dicho lenguaje o incluso presentado un listado exhaustivo de los tipos de *cookies*, etc. que requerirían el consentimiento. Y en consonancia con otros pasajes y apariciones de dichos términos en el resto del texto, el Parlamento tampoco habría redactado el considerando 66 tal cual está hoy día.

3.4.3 El consentimiento y la Directiva de protección de datos

El concepto del consentimiento del usuario en la Directiva sobre la privacidad y las comunicaciones electrónicas se extrajo realmente de la Directiva de protección de datos 95/46/CE y es idéntico al de esta, como puede comprobarse en el considerando 17 de la Directiva sobre la privacidad y las comunicaciones electrónicas:

> *A efectos de la presente Directiva, el consentimiento de un usuario o abonado, independientemente de que se trate de una persona física o jurídica, debe tener el mismo significado que el consentimiento de la persona afectada por los datos tal y como se define y se especifica en la Directiva 95/46/CE. El consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre inequívoca e informada de la voluntad del usuario, por ejemplo mediante la selección de una casilla de un sitio web en Internet.*

El consentimiento, tal y como se define y utiliza en la Directiva de protección de datos, no tiene por qué ser «previo» ni «explícito», a menos que se mencione de manera concreta (el «consentimiento explícito» se menciona dos veces solamente en la Directiva de protección de datos), tal y como es el caso de la Directiva sobre la privacidad y las comunicaciones electrónicas, en la cual los términos «consentimiento» y «previo» aparecen unidos bastante a menudo. Aunque se han dado intentos de interpretación del consentimiento como algo distinto en otras partes de la Directiva, sigo sin creer que se requiera mayor aclaración o definición. Incluso en la próxima revisión de la Directiva de protección de datos no veo la necesidad de ampliar la definición existente del consentimiento, aparte de, quizá, la actualización de su alcance, pues es posible que deba incrementarse el listado de datos sensibles.

De darse el caso no se haría más que complicar la cuestión, en mi opinión. La legislación europea debería determinar el marco adecuado para su aplicación a nivel nacional. Por este motivo, el considerando 66 de la Directiva sobre la privacidad y las comunicaciones electrónicas permite el derecho de denegación sin otorgar preferencia a un modelo de inclusión o exclusión voluntarias *(opt-in/opt-out)* para

la implantación. Las opciones de inclusión voluntaria permiten el uso de información personal pero exigen el consentimiento de inclusión voluntaria antes de revelar la información personal a un tercero. La principal repercusión de los sistemas de exclusión voluntaria sería que la compartición de datos se llevaría a cabo y que el tercero podría emplear la información del cliente recabada por otras partes. Cuando la legislación exige que se otorgue a los individuos el derecho de elección, el sistema de exclusión voluntaria es el que se usa con mayor asiduidad. Tal hecho se debe probablemente a que los usuarios deberían tener que buscar una manera de averiguar por qué están incluidos en un grupo de distribución, por no hablar de la forma de excluirse de ella, de querer hacerlo, con lo cual los usuarios ni siquiera se molestarían en comenzar a buscar. De nuevo, el consentimiento informado tan solo puede otorgarse si la información necesaria es fácil de conseguir y está disponible de manera transparente.

La forma correcta y efectiva de aplicar lo anterior es que el proveedor de servicios lo escoja dentro del marco del artículo y el considerando correspondiente. La competencia europea no se extiende a los modelos empresariales ni debería imponerlos.

3.4.4 ¿Cuándo se necesita el consentimiento del usuario?

Aquí es donde los aspectos prácticos de la correcta aplicación de la Directiva parecen haber producido una mayor divergencia de opiniones sobre la mejor forma de manejar el requisito de consentimiento. Por ejemplo, la opinión del Grupo de Trabajo del Artículo 29 (Opinión 2/2010 del 22 de junio del 2010) afirma de manera muy adecuada en su estudio sobre la publicidad basada en el comportamiento que los requisitos de transparencia constituyen una condición clave para que los individuos puedan dar su consentimiento a la recopilación y tratamiento de sus datos personales, y por tanto para que puedan ejercer una capacidad de elección efectiva. Puesto que la práctica de la publicidad basada en el comportamiento depende de que los datos personales relevantes estén disponibles, esta afecta directamente al almacenamiento y acceso de los datos en los equipos de los usuarios. Para que pueda funcionar la publicidad basada en el comportamiento, los movimientos de los usuarios de Internet se registran en la Red (a menudo con el uso de *cookies* de rastreo) a lo largo del tiempo para generar un perfil específico. Este perfil se combina después con anuncios al deducir el interés del individuo por ciertos productos o servicios. Aunque esta práctica no tiene por qué permitir la creación de un perfil completo del usuario con todos sus datos personales, reúne información sensible y personal sin que el sujeto sea consciente de ello. En combinación con el software de minería de datos, que descubre información o patrones que podrían comprometer la confidencialidad y obligaciones de privacidad, la suma de todos los datos recabados infringirá la legislación en materia de privacidad en muchas ocasiones. Por ejemplo, los controles de seguridad de Flash LSA son distintos de los controles del usuario para las *cookies*, con lo que los objetos almacenados a nivel local o global pueden estar habilitados aunque no lo estén las *cookies*. Por tanto, y dado que el usuario medio no puede detectar y eliminar las *cookies flash* de manera sencilla tal y como se tratara de *cookies* de terceros (bien mediante los ajustes del navegador o de manera manual), estas burlan los ajustes personales del navegador del usuario y por consiguiente sortean automáticamente la cuestión del consentimiento, es decir, se aplica entonces el Artículo 5.3 de la Directiva sobre la privacidad y las comunicaciones electrónicas. Lo mismo ocurre con otros dispositivos, como los de las técnicas HTML5, Java API, Silverlight o similares. Por tanto, los usuarios deberán estar informados sobre la finalidad del tratamiento de sus datos (tal y como lo contempla la Di-

rectiva de protección de datos 95/46/CE) antes de que se acceda a ellos para así poder tener la opción de permitir o denegar dicho acceso en cualquier momento.

Aunque en el informe del Grupo de Trabajo del Artículo 29 este mostraba su preocupación por que la adaptación de los ajustes del navegador no constituya el consentimiento informado del cliente, yo creo que refleja justamente eso. Es cierto que la mayoría de navegadores vienen predeterminados para aceptar todas las *cookies* por defecto. Sin embargo, no hay nada que pueda impedir la emisión de la notificación correspondiente cuando se instale el navegador por la que se informe al usuario sobre este hecho o sobre cualquier otro cambio significativo de los ajustes, tal y como viene siendo práctica acostumbrada de muchos proveedores de servicios durante años. Como se ha mencionado anteriormente, el objetivo del Artículo 5.3 de la Directiva sobre la privacidad y las comunicaciones electrónicas consiste en proteger a los usuarios contra el abuso de sus datos personales sin su consentimiento mediante software espía o malicioso. La mayoría de *cookies* «benignas» no acceden ni almacenan datos personales sensibles para después usarlos para fines que desconozca el usuario; estas son las que puede visualizar el usuario en sus ajustes del navegador. Pero no es el caso de las *cookies flash*, que se vuelven a generar de manera automática y burlan el requisito de consentimiento. Sin las *cookies*, Internet sería «olvidadizo» y se perderían ventajas evidentes de que disfruta el usuario.

3.4.5 El análisis de la Directiva de protección de datos

La Comisión es muy consciente de que los medios de recopilación de datos personales son cada vez más sofisticados y complicados de detectar. Durante conversaciones preliminares con la comisaria Reding antes de la publicación del Reglamento me aseveró que la Comisión no se mostraría excesivamente restrictiva en la revisión de la Directiva de protección de datos. Testimonio del valor de la Directiva de 1995 es que no haya necesitado ser revisada hasta ahora. La actualización debería ocuparse del impacto de las nuevas tecnologías y mejorar la coherencia del marco legal de protección de datos europeo, con un poco de suerte sin extralimitarse al final. La Comisión, a la hora de incrementar la coherencia de la legislación europea sobre protección de datos a través de la Directiva sobre la privacidad y las comunicaciones electrónicas y la Directiva de protección de datos, deberá considerar qué datos personales o sensibles requerirán consentimiento si quisieran compartirse. Este hecho podría afectar a otros sectores por completo pero también, en el contexto de la privacidad y comunicaciones electrónicas, a otras tecnologías distintas a las *cookies* de origen y las de terceros, una distinción necesaria entre los usos principales y secundarios y, por ejemplo, los contadores de visitas.

El derecho a la protección de los datos personales queda establecido mediante el Artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y el Artículo 16 del TFUE, así como en el Artículo 8 del Tribunal Europeo de Derechos Humanos (TEDH), y debe considerarse, en relación con su función en la sociedad, vinculado estrechamente al respeto por la vida privada y familiar, tal y como se refleja también en el Artículo 7 de la Carta de los Derechos Fundamentales y el Artículo 1 de la Directiva de protección de datos 95/46/CE. Para poder seguir construyendo un marco de protección de datos sólido en Europa deben superarse los retos que han planteado los avances recientes de la tecnología. Esto, a su vez, debe hacerse de tal forma que infunda confianza tanto en los ciudadanos como en la economía digital que se está desarrollando en el Mercado Único de la UE. Para ello, los derechos y protección de los datos personales deben salvaguardarse de manera uniforme en todos los Estados miembros de la UE, eliminando cualquier obstáculo existente relativo a

las diferencias en la aplicación e implantación de la Directiva de protección de datos 95/46/CE que se han dado hasta la fecha.

El nuevo Reglamento de protección de datos no debe introducir ni legislación engorrosa en términos de burocracia ni procedimientos de verificación complicados, como por ejemplo para el consentimiento, si quiere conseguir una protección coherente de los datos en todo el territorio europeo. Tal cosa solo podrá conseguirse sometiendo la nueva propuesta legislativa a un análisis exhaustivo de la realidad y encontrando las definiciones más claras posibles para todas las cuestiones de las que se ocupe dicha propuesta legislativa. El Parlamento Europeo examinará en profundidad la propuesta legislativa desde este punto de vista.

Se esperan soluciones para los siguientes problemas conocidos en su debido momento: la legislación europea actual sobre protección de datos es un mosaico de distintos reglamentos y debe ser más coherente, cuanto menos para permitir a los proveedores de servicios europeos y no europeos que ofrezcan sus modelos empresariales dentro de un marco regulador claro. Debe crearse un espacio donde los principios existentes sobre privacidad (por ejemplo, la privacidad por defecto, la privacidad desde el diseño, las notificaciones de infracción de la privacidad obligatoria) se respeten e implementen en la mayor medida posible. De esta forma, Europa podrá predicar con el ejemplo y ayudar a establecer estándares globales.

Pilar del Castillo Vera

Pilar del Castillo Vera es diputada en el Parlamento Europeo desde el año 2004 y coordinadora del Grupo Parlamentario Popular Europeo en la Comisión de Industria, Investigación y Energía, donde ha sido ponente de diferentes informes relacionados con la revisión del Marco Regulador europeo de Comunicaciones Electrónicas y con el establecimiento de la Agenda Digital para Europa. Es presidenta del Board of Governors de la European Internet Foundation (EIF), miembro del Transatlantic Policy Network (TPN) y del European Energy Forum (EEE). Es, asimismo, catedrática de Ciencia Política y de la Administración por la UNED y doctora en Derecho por la Universidad Complutense.

3.5 Un modelo de protección de datos para un Mercado Único Digital

Pilar del Castillo Vera
Diputada en el Parlamento Europeo y coordinadora del Grupo Parlamentario Popular Europeo en la Comisión de Industria, Investigación y Energía (ITRE)

Las tecnologías de la información y la comunicación (TIC) impregnan hoy día prácticamente todos los aspectos de la vida. Están estrechamente relacionadas con el deseo de conseguir una economía próspera y competitiva, de preservar el entorno y de crear una sociedad más democrática, abierta y global. No obstante, este deseo solamente se hará realidad si todos los ciudadanos se movilizan y se les dota de las facultades para impulsar y participar al completo en la nueva sociedad digital. Los negocios tal y como se han venido haciendo hasta ahora no son una opción.

Dotar a la gente de las facultades necesarias para el mundo digital actual implica varios aspectos fundamentales. Para facultarla se le debe conceder acceso a redes fiables y resistentes de banda ancha tanto inalámbricas como por cable, además de las competencias y capacidades necesarias para poder aprovechar las oportunidades que brinda la era digital, y poder sustentarse en un marco legal claro que proteja los derechos de los individuos y que proporcione la confianza y la seguridad necesarias en este nuevo entorno *online*.

Todavía queda mucho para poder completar, en el sentido amplio de la palabra, el Mercado Único Digital Europeo (en adelante «Mercado Digital»); si se echa un vistazo al movimiento libre de servicios digitales, hoy día gravemente afectado por las normas fragmentadas a nivel nacional, resulta evidente que aún no se han desarrollado economías de escala que ayuden a convertir a la UE en una economía digital líder.

En la actualidad, y más que nunca, el Mercado Digital se ha convertido en un excelente ruedo donde no solo pueden desarrollarse contenidos creativos, sino también modelos empresariales creativos adecuados a estos tiempos de crisis.

Es cierto que el Mercado Digital es un mercado con características muy específicas. De hecho, no había señales de este mercado cuando se definió el Mercado Único Europeo como la piedra angular del proyecto de una Europa común para los países europeos. El escenario digital intangible en el que tiene lugar este mercado no hace más que complicar la definición de sus requisitos para convertirse en un verdadero Mercado Único.

La cantidad de obstáculos a los que se enfrentan las empresas cuando intentan vender fuera de sus fronteras es también bastante evidente. La diversidad de normas comunitarias, así como de los Estados miembros, que deben aplicarse en áreas tales como la protección del consumidor, el impuesto sobre el va-

lor añadido (IVA), el reciclaje de dispositivos eléctricos y electrónicos, la función de las sociedades de derechos colectivos, las normas específicas de cada producto y las transacciones de pago o la distinta implantación del sistema de protección de datos de 1995 ha dado lugar a importantes discrepancias en la aplicación a lo largo de la UE, que ha impedido a las empresas y a los consumidores que exploten todo el potencial de la economía digital.

No cabe duda de que los costes de la actual fragmentación de la UE son muy elevados. Según datos recientes, el cálculo de los gastos de dicha fragmentación asciende a unos 20.000 millones de euros al año. Un factor de costes que se eliminaría en parte si se implantara de manera efectiva la revisión del marco regulador de las comunicaciones electrónicas y se confiara a Europa un sistema de protección de datos integral. A este respecto, resulta esencial para Europa que cada uno de los Estados miembros transponga e implante por completo la nueva normativa cuanto antes. Todos los obstáculos legislativos clave que perjudican al mercado de los servicios digitales deben eliminarse, pues aunque se cuenta con un mercado potencial de 500 millones de consumidores, seguirá siendo potencial a menos que se suprima la fragmentación actual del mercado.

No obstante, ya que la implantación efectiva del marco constituye una condición indispensable, si se quiere conseguir un verdadero mercado digital no debe tratarse únicamente de un requisito previo. Hoy día, tan solo el 12 % de todas las transacciones efectuadas por los consumidores europeos en la Red son transfronterizas; y solo el 35 % de la población total de la UE ha utilizado servicios de Internet avanzados durante los últimos tres meses (los servicios de Internet avanzados se refieren a la subida o descarga de contenido o a la participación en redes sociales). Debemos potenciar el mercado de los servicios digitales y, a este respecto, la protección de la privacidad constituye un valor esencial que desempeñará un papel clave a la hora de aportar a todos los usuarios la confianza y la seguridad necesarias para interactuar en Internet. Por consiguiente, todo el mundo debería controlar sus propios datos personales, incluyendo el «derecho al olvido» (que es el derecho a exigir la eliminación de los datos personales cuando estos se recaban en principio con el consentimiento del sujeto registrado). Así pues, si se debe contribuir al desarrollo del Mercado Único Digital en Europa y cubrir las necesidades del entorno digital actual, habrá que superar la fase de adaptación de la Directiva de protección de datos actual.

Sin duda alguna, esta no será tarea fácil. El carácter especialmente fluido de Internet, donde los datos migran continuamente, la estructura de las organizaciones activas en la Red es extremadamente dinámica y ya no existe la posición dominante de los sistemas públicos centralizados de recopilación de datos (que coexisten hoy día con una cantidad de sistemas y entidades distintas y altamente fragmentadas que no solo recaban, sino que también procesan, intercambian y transmiten datos personales), representa un cambio radical de escenario y agentes al que debe enfrentarse la reforma del sistema de protección de datos.

Aun así, se trata de una tarea que debe efectuarse. El contenido del sistema actual de protección de datos no es el único que requiere actualización mediante la aclaración de algunos de sus principios, como la transparencia y el consentimiento, o la introducción de otros nuevos, como la «privacidad por diseño», sino que, además, existe la necesidad de establecer una normativa mejorada que cree un marco legal único e integral. En la actualidad, el sistema de protección de datos que se aplica al entorno digital está formado por una compleja mezcla de Directivas europeas (la Directiva de protección de datos general, la Directiva sobre la privacidad y las comunicaciones electrónicas y la Directiva sobre la conservación de datos) que se han aplicado de

manera muy distinta a lo largo de la UE y que, cuando menos, no es lo ideal.

La Comisión Europea presentó el 25 de enero del 2012 una reforma integral del sistema de protección de datos de la UE compuesto por una política sobre comunicación, que desarrolla los objetivos de la Comisión, y dos proyectos legislativos: un Reglamento que establece el marco general europeo de protección de datos y una Directiva que protege los datos personales procesados a los fines de prevenir, detectar, investigar o procesar los delitos penales y otras actividades judiciales relacionadas. La propuesta de la Comisión constituye un paso muy aplaudido que responde no solo a las exigencias del Parlamento Europeo, sino también a la necesidad urgente de adaptar la legislación al entorno digital y cosechar todos los frutos de la revolución digital.

Por tanto, muchos son los cambios que debe acometer el nuevo sistema: en primer lugar, y teniendo en cuenta que el Tratado de Lisboa ya ofrece la base jurídica de la normativa sobre protección de datos para todas las actividades cubiertas por el derecho europeo, existe la necesidad de reafirmar el carácter de derecho fundamental de la protección de datos personales. Como resultado, y con el fin de que dicho derecho sea lo más efectivo posible, se debe incrementar la transparencia del tratamiento, reforzar los mecanismos de concienciación y crear recursos y sanciones más efectivos.

En segundo lugar, y para fomentar la dimensión del Mercado Único Digital, deben explorarse las distintas posibilidades de simplificación y armonización de los sistemas de notificación, aclarar la legislación en vigor, promover la autorregulación e incrementar la responsabilidad de los responsables del tratamiento de los datos personales.

En tercer lugar, el mundo globalizado actual y, especialmente, la naturaleza globalizada de Internet, requiere que se preste la máxima atención a la dimensión global de la protección de datos. A este respecto, debe promoverse el desarrollo de la colaboración internacional con los socios globales mediante el fomento de los principios universales en este dominio, además de aclarar y simplificar las normas de la transmisión de datos.

Por último, existe una evidente necesidad de crear mecanismos institucionales más sólidos que permitan mejorar la aplicación de la normativa de protección de datos en toda la UE. Deben reforzarse asimismo la categoría y las facultades de las autoridades nacionales de protección de datos, al tiempo que se incremente la colaboración y la cooperación entre ellas.

El nuevo sistema de protección de datos propuesto por la Comisión refleja muchos de los anteriores retos, y gran cantidad de sus propuestas proporcionan las mejoras efectivas que se han de aplicar al sistema actual. Por ello, ha tenido muy buena acogida que, por primera vez, el sistema de protección de datos se haya compuesto de un único conjunto de normas consagradas en un instrumento jurídico más adecuado, es decir, un reglamento, que se aplicará directamente en toda la UE sin necesidad de transposición, lo cual en términos concretos significa un gran avance en materia de armonización en toda Europa.

Además, el Proyecto de Reglamento modifica el sistema actual de notificación que obligaba a todas las empresas a comunicar todas las actividades sobre protección de datos a los supervisores de protección de estos (lo cual costaba a las empresas, según la Comisión Europea, 130 millones de euros al año), para exigir ahora que se incremente la responsabilidad y la competencia de quienes procesan los datos personales, por ejemplo obligando a las empresas a que notifiquen en el plazo de 24 horas cualquier vulneración grave de los datos.

Del mismo modo, el concepto de «establecimiento principal», que permitirá a las empresas tratar con una única autoridad nacional de protección en cada Estado miembro de la UE siempre que exista un establecimiento princi-

pal, posiblemente reduzca en gran medida la burocracia de la industria y refuerce los derechos de protección de los datos personales al permitir a las personas acudir a la autoridad de protección de datos de su país. Esto se aplicará incluso aunque sus datos sean procesados por una empresa cuya sede se halle fuera de la UE (las normas europeas se aplican también aunque los datos personales sean manipulados en el extranjero por empresas que operen en el mercado europeo y ofrezcan sus servicios a los ciudadanos europeos).

En cuanto al uso efectivo del derecho fundamental a la protección de los datos personales, cabe destacar que el nuevo proyecto no solo facilitará el acceso a nuestros datos personales, sino que también consagra el derecho a la portabilidad de estos, lo cual, al permitir transferir de manera sencilla los datos personales de un servicio a otro, mejorará sin duda alguna la competencia entre los servicios. En conclusión, tales rasgos tienen potencialmente la capacidad de reforzar la confianza del consumidor en los servicios *online* y mejorar a su vez la competencia, con lo que se conseguiría el tan ansiado estímulo del crecimiento, el empleo y la innovación en Europa.

Es más, tal y como solicitara el Parlamento Europeo en el 2009, la propuesta de Reglamento amplía el ámbito del derecho actual a la protección de datos al conceder a todos los usuarios el «derecho al olvido».

Por último, la propuesta de Reglamento general de protección de datos se ocupa de uno de los aspectos más importantes de un sistema de protección de datos de funcionamiento correcto, esto es, del papel de las autoridades nacionales de protección de datos (APD). De hecho, para poder garantizar el mayor nivel de armonización y una aplicación sistemática del futuro reglamento, hay que definir urgentemente cuál es la APD considerada como la autoridad líder en las actividades de tratamiento efectuadas por los responsables y los encargados del tratamiento de los datos. Del mismo modo, la independencia y las capacidades de las autoridades nacionales de protección de datos deberán aumentarse y, a este respecto, la capacitación de dichas entidades de manera que puedan imponer sanciones administrativas a las empresas que infrinjan la normativa europea sobre protección de datos es un gran avance.

La propuesta de la Comisión, por el momento, sigue siendo tan solo una propuesta. El debate comenzará ahora entre los dos legisladores europeos, el Parlamento y el Consejo. Diversos serán los temas que suscitarán un debate bastante interesante, como por ejemplo, el grado de armonización requerido, la forma en que se estructure la cooperación entre las distintas autoridades nacionales, la capacidad y los niveles de las sanciones que puedan imponer las mismas, el papel de la autorregulación, el acceso a los actos delegados de la Comisión Europea o la manera en que se regulen las transferencias internacionales de datos.

Aparte de todo ello, deberán clarificarse las definiciones y conceptos clave. Al mismo tiempo, las obligaciones y funciones del responsable y del encargado deberán delimitarse de manera adecuada. Además, el concepto del consentimiento deberá adaptarse al entorno digital y, por consiguiente, debería compartir las principales características de este entorno, es decir, debería ser dinámico, contextual y operar en múltiples niveles. De hecho, incluso las definiciones de datos personales y sujeto registrado no están aceptadas de manera unánime.

Teniendo en cuenta que el ámbito y el objetivo de este artículo no permiten una reflexión profunda de todas las características principales que dominarán los debates legislativos que están por comenzar en torno al futuro Reglamento general de protección de datos, considero prudente esbozar lo que en mi opinión serían los principios fundamentales que guiarán el debate entre las instituciones europeas.

No debemos olvidar que el éxito extraordinario de Internet, que ha cambiado nuestra

forma de interactuar en todas las dimensiones de nuestra vida personal, profesional y social, también es el responsable del increíble aumento de la productividad gracias a su carácter innovador. En efecto, la naturaleza constantemente dinámica de Internet en concreto y del entorno digital en general constituye su verdadera esencia, y por tanto los legisladores deberán ser extremadamente cautos a la hora de establecer cualquier normativa clave, evitando que su potencial eterno de contribución al crecimiento y la competitividad, es decir, al bienestar de la población, se vea obstaculizado.

Tal y como se mencionara al principio, el sistema de protección de datos propuesto es una medida muy esperada, y una respuesta a un claro llamamiento a la acción para que una desfasada normativa sobre protección de datos se adaptara al entorno digital garantizando al mismo tiempo la preservación de derechos fundamentales tales como la privacidad. No obstante, para regular ciertos aspectos del entorno digital, los legisladores debemos ser sumamente sensibles a la hora de pulir el marco regulador digital. El «nuevo mundo» que representa el entorno digital cuenta en realidad con un ecosistema muy delicado y frágil basado casi por completo en su capacidad innovadora y, por tanto, dicha naturaleza innovadora debe preservarse.

A modo de ejemplo, parece apropiado reflexionar sobre los retos que se afrontarán en el momento de adaptar el sistema de protección de datos, de forma que no se vea afectada la naturaleza innovadora del entorno digital, al segmento de mayor crecimiento del sector informático, la *cloud computing*.

De hecho, hoy en día el *cloud computing* se ha convertido en uno de los puntos más relevantes de las agendas digitales de todo el mundo. Lo cierto es que no solo cuenta con un valor económico y social de gran importancia, sino que además sus posibilidades son enormes; hoy día, casi no existe organización alguna que no use una base de datos o una red, lo cual en términos comerciales significa que todas las empresas (al igual que todos los gobiernos) son usuarios potenciales.

En todo el mundo las empresas se están dando cuenta de los beneficios en productividad que pueden conseguir al acceder fácilmente a las aplicaciones comerciales de mejor rendimiento o fomentar drásticamente los recursos en infraestructura a un coste muy bajo. Distintos cálculos han estimado que para el año 2014, los ingresos de la nube pueden alcanzar unos 148.800 millones, y que el 60 % de todo el volumen de trabajo de los servidores será virtual.

Las expectativas económicas y comerciales de la «nube» son mucho más que prometedoras, y por tanto se ha creado un modelo de negocio para su desarrollo. Sin duda alguna, y teniendo en cuenta que problemas tales como la privacidad y la seguridad de los datos son de extrema importancia para el desarrollo y el consumo de las infraestructuras en la nube, será crucial instaurar un sistema regulador de protección de datos adecuado que pueda convertirse además en una ventaja competitiva en los futuros mercados globales de servicios en la nube.

Si se consigue el sistema de protección de datos adecuado no solo podrán seguir desarrollándose nuevos servicios de vanguardia en la nube y promover su consumo, sino que además se crearán nuevos mercados sobre privacidad y seguridad que se convertirán en rasgos clave para la oferta de productos. A este respecto, según el Informe Forrester de 2010, se calcula que la «seguridad como servicio» se convertirá en un mercado que ascenderá a 1.500 millones de dólares y, por tanto, los proveedores de servicios en la nube capaces de ofrecer un mayor grado de seguridad y privacidad tendrán la capacidad de atraer a un mayor número de suscriptores, al tiempo que la prestación de servicios de privacidad y seguridad en plataformas en la nube atraerá a usuarios poco convencidos de las garantías de los proveedores de las

plataformas o que no deseen pagar el precio que se les cobre por ello.

En términos prácticos, el resultado final de las negociaciones entre el Parlamento Europeo y el Consejo debería permitir una flexibilidad suficiente a los usuarios de manera que puedan valorar el grado y las características técnicas de la protección de la privacidad y la seguridad que crean más adecuadas para su empresa o uso personal en la nube.

Tal y como se mencionó al principio, el *cloud computing* es solo un ejemplo, debido a su enorme potencial evidente, de los principios fundamentales que deben guiarnos a la hora de reflexionar sobre el futuro sistema de protección de datos. Al adaptar la protección de datos al entorno *online*, no debe olvidarse que la privacidad es un problema contextual que exige mecanismos de aplicación flexibles que permitan a los usuarios tomar decisiones contextuales simples e informadas. Tan solo si se sigue esta vía podrá preservarse el derecho de cada individuo a la privacidad sin tener que renunciar a los beneficios de la innovación y el crecimiento empresarial que representa la era digital.

Hans Graux

Hans Graux es investigador afiliado del Centro Interdisciplinario de Derecho y TIC (ICRI-IBBT, www.icri.be) de la KU Leuven. Es abogado y socio fundador de una empresa con sede en Bruselas denominada time.lex (www.timelex.eu), especializada en Derecho de tecnologías de la información y problemas en las políticas sobre dichas tecnologías.

Jef Ausloos

Jef Ausloos estudió Derecho en la Universidad de Namur (FUNDP) y la Universidad de Leuven (KU Leuven). Hizo un máster en Derecho sobre tecnologías de la información y la propiedad intelectual en la Universidad de Hong Kong, donde además ocupó un cargo de investigador adjunto. En 2011 trabajó como colaborador internacional del Centro de Democracia y Tecnología (www.cdt.org) y para la Fundación Fronteras Electrónicas (www.eff.org) de EE. UU. En la actualidad es investigador doctoral del Centro Interdisciplinario de Derecho y TIC (ICRI-IBBT, www.icri.be) de KU Leuven.

Peggy Valcke

La profesora y doctora Peggy Valcke es profesora de investigación en la Universidad de Leuven (KU Leuven) e imparte clases sobre Derecho de comunicaciones en la Universidad de Bruselas (HU Brussel) y la Facultad Reglamentaria de Florencia (Instituto Universitario Europeo, Florencia). Es profesora invitada de la Universidad de Tilburg y fue profesora invitada de la Universidad Europea Central de Budapest en 2006. Hoy día es directora del Centro Interdisciplinario de Derecho y TIC (ICRI-IBBT, www.icri.be) de la KU Leuven.

3.6 El derecho al olvido en la era de Internet

Hans Graux
Investigador asociado del Centro Interdisciplinario de Derecho y TIC (ICRI-IBBT, www.icri.be) de la Universidad Católica de Lovaina

Jef Ausloos
Investigador doctoral en el Centro Interdisciplinario de Derecho y TIC en la Universidad Católica de Lovaina

Peggy Valcke
Catedrática en la Universidad Católica de Lovaina. Directora del Centro Interdisciplinario de Derecho y TIC en la Universidad Católica de Lovaina

3.6.1 Introducción[108]

La importancia de olvidar, como algo que impulsa las relaciones humanas, ha adquirido cada vez mayor evidencia en los últimos años. En su famoso libro, Mayer-Schönberger[109] ha demostrado mediante una serie de convincentes ejemplos la relevancia que pueden tener las insuficiencias biológicas de los recuerdos humanos a la hora de facilitar las interacciones sociales: las indiscreciones, errores y conflictos pasados se olvidan con el tiempo, garantizando la capacidad de poder pasar por alto casi cualquier imperfección de las propias historias. En ocasiones, el impacto del olvido es negativo, pues podría perderse información relevante que hubiera sido de vital importancia si se hubiera podido recordar. En otros casos, el impacto es positivo: la información que ya no resulta relevante se pierde en la neblina del tiempo, permitiendo dejar atrás las partes menos favorables del propio pasado.

Esta posibilidad de abandonar la historia propia está padeciendo una erosión gradual causada por las tecnologías modernas[110]. Las cuentas de correo, redes sociales y archivos *online* hacen las veces de extensiones perpetuas de los falibles recuerdos. La información ya no se pierde, incluso aunque no se hubiera retenido de manera natural. De esta forma, se guardan los registros de hechos pasados que de otro modo se perderían, pero también conlleva que ciertas partes pequeñas e irrelevantes de las historias propias puedan volver a atormentarnos[111]. ¿Es-

108. Los autores desean dar las gracias a la Dra. Eleni Kosta, investigadora jefe del Centro Interdisciplinario de Derecho y TIC, por sus valiosos comentarios y sugerencias. Cualquier error es responsabilidad única de los autores.
109. Mayer-Schönberger, V., Delete: the Virtue of Forgetting in the Digital Age. Princeton University Press, 2009.
110. McLuhan, M., in: Solove, D. J., The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. Yale University Press, 2007. p. 33.
111. Rosen, J., «The Web Means the End of Forgetting» NYTimes. New York, 21 July 2010. http://nyti.ms/ftHuEt.

tamos perdiendo la capacidad de evolucionar más allá de nuestro pasado? Y, de ser así, ¿se trata de una área en donde debería intervenir la ley?

En este apartado se analiza cómo la sociedad se ha propuesto recrear los efectos de la capacidad natural de olvido imponiendo la obligación de suprimir cierta información. Los paradigmas jurídicos existentes, incluyendo el derecho fundamental a la privacidad y el *droit à l'oubli* (derecho al olvido), existente en algunos países, contrastan con un concepto más reciente: el derecho al olvido. Este concepto se analizará desde la perspectiva de los cuatro factores de regulación de Lessig (las normas, el mercado, el código o tecnología y la ley) con el fin de determinar hasta qué punto la sociedad moderna reconoce y es capaz de lidiar con dicho derecho. Por último, la inclusión reciente del derecho al olvido en la propuesta de Reglamento general de protección de datos[112] se examinará de manera crítica para evaluar su similitud con la normativa y prácticas actuales, los principales retos a los que se enfrentará y cómo se atajarán estos.

3.6.2 La capacidad de olvido: perspectiva desde los derechos fundamentales

En ciertos dominios de la política pública, la capacidad de olvido no solo se considera aceptable y útil para la sociedad, sino que además se estima como algo vital. En el derecho penal, los delitos menores suelen eliminarse de los antecedentes al transcurrir cierto tiempo, al igual que muchas transgresiones cometidas por menores al alcanzar la mayoría de edad. El razonamiento es sencillo: los errores de juicio e infracciones menores de la juventud no deberían impedir la (re)integración futura de la persona en la sociedad general. En cierto momento, en la pizarra oficial se borran todos los incidentes relativamente menores, y no queda ningún registro público que pudiera empañar las oportunidades del autor en el mercado laboral u otras esferas sociales. Se da una segunda oportunidad.

De esta forma, la realidad de la «capacidad de olvido deseable» se ha codificado en ciertos contextos mediante leyes que rigen el mantenimiento y la limpieza periódica de los registros oficiales. Pero la ley se ha aplicado a otras instancias del recuerdo más allá del mantenimiento de registros públicos, a menudo con arreglo a leyes sobre privacidad o los derechos personales. Estos casos suelen girar en torno a personas que se han adentrado temporalmente en el terreno de la exposición pública y han sido incapaces de zafarse de la atención que, después de cierto tiempo, ya no se ha deseado o garantizado. En el lenguaje de la doctrina legal francesa, las reclamaciones efectuadas por dichas personas se han descrito como el ejercicio del derecho al olvido[113].

Un ejemplo bastante ilustrativo del mencionado derecho al olvido podría ser la sentencia del Tribunal de Primera Instancia de Bruselas en 2001[114]. En este caso, un delincuente declarado culpable adujo que, después de haber cumplido su sentencia de cárcel, su derecho al olvido había sido vulnerado por reportajes de televisión que cubrieron su puesta en libertad y recordaron al público los crímenes que había cometido en el pasado, incluyendo la emisión de imágenes de su fuga de prisión en la década de los ochenta. Una variación similar pero más moderna de este escenario tuvo lugar en Alemania, donde dos ciudadanos fueron condenados por asesinato en 1990 después de un notorio juicio. Veinte años después de haber sido puestos en libertad condi-

112. Comisión Europea, «Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la protección de los individuos con respecto al tratamiento de datos personales y la libre circulación de dichos datos (Reglamento general de protección de datos)», COM(2012) 11 final (el Reglamento).

113. Para una reformulación formal y moderna de esta doctrina, véase, por ejemplo la carta del derecho al olvido emitida por el secretario de Estado francés de Planificación Estratégica y Desarrollo de la Economía Digital: http://www.gouvernement.fr/gouvernement/charte-du-droit-a-l-oubli-numerique-mieux-proteger-les-donnees-personnelles-des-interna.

114. Tribunal de Primera Instancia de Bruselas, 20 de septiembre de 2001, Auteurs & Media 2002/1, 77.

cional, uno de ellos acudió a los tribunales alemanes para solicitar órdenes por las que se suprimiera cualquier referencia a su nombre en inglés y alemán en la Wikipedia[115], basándose en una sentencia de 1973 del Tribunal Constitucional de Alemania que afirmaba los derechos a preservar la intimidad de los ciudadanos privados después de haber cumplido sus condenas[116].

En Suiza tuvo lugar otro caso comparable en 1983[117], cuando la Société Suisse de Radio et de Télévision intentó crear un reportaje radiofónico sobre la vida de un asesino que había sido sentenciado a muerte en 1939. En este caso, un descendiente del criminal se opuso al reportaje argumentando que la emisión le perjudicaría personalmente, pues se entrometía en su vida privada. El Tribunal Federal Suizo reconoció que no existía ningún derecho absoluto al olvido *(Vergessen)* que pudiera impedir, por ejemplo, la investigación histórica y científica, pero dictaminó sin embargo que el incremento natural del olvido podría reducirse o eliminarse mediante los medios de difusión electrónicos, de nuevo llamando la atención del gran público sobre ciertos hechos[118]. Como resultado, prohibió que se emitiera el reportaje.

El derecho al olvido se invoca pues principalmente en aquellos casos en los que el pasado de una persona se somete a una exposición pública no deseada, cuando el sujeto que sufre dicha exposición argumenta que esta vulnera sus derechos fundamentales a la privacidad o la personalidad hasta el punto en que cualquier interés público legítimo en tal exposición ya no quede justificado. A este respecto, los debates en torno al derecho al olvido son similares a otros casos en los que los derechos a la privacidad de los personajes públicos entran el conflicto con la libertad de expresión. Evidentemente, la privacidad como tal sigue siendo un concepto que suscita intensos debates, y muchos eruditos han ofrecido sus propias interpretaciones sobre el significado y el ámbito de la privacidad[119]. La reciente sentencia en el caso de Von Hannover contra Alemania (2)[120] dictaminada por el Tribunal Europeo de Derechos Humanos proporciona una extensa perspectiva sobre la jurisprudencia europea anterior en relación con el conflicto entre la privacidad y la libertad de expresión, y describe algunos de los principales factores que se tuvieron en cuenta en tales casos, entre los que se incluyen la contribución de la exposición al debate de interés general, el prestigio general de la persona afectada, su conducta previa, el contenido, forma y consecuencias de la publicación y el contexto[121]. Estos fac-

115. Granick, J., «Convicted Murder to Wikipedia: Shhh!» (org. EFF, 10 de noviembre de 2009) https://www.eff.org/deeplinks/2009/11/murderer-wikipedia-shhh.
116. Schwartz, J., «Two German Killers Demanding Anonymity Sue Wikipedia's Parent» NYTimes (12 de noviembre de 2009), http://www.nytimes.com/2009/11/13/us/13wiki.html.
117. Werro, F., «The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash» en Aurelia Colombi Ciacchi y otros (eds.), Liability in the third millennium (Baden-Baden, F.R.G. 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357.
118. X v. Société Suisse de Radio et de Télévision. BGE 109 II 354 (1983), http://www.servat.unibe.ch/dfr/c2109353.html: «Cambia las cosas, sin embargo, que el olvido, que suele incrementarse de manera natural, no pueda extinguir de forma inmediata el pasado que sigue rememorándose en relación con la vida privada e íntima de un delincuente particular, o que un pasado todavía no extinguido por completo vuelva a sacarse a la luz ante un amplio público a través de los medios de difusión electrónicos, como sería el caso de la emisión del reportaje radiofónico que nos ocupa».
119. Estados Unidos, en especial, disfruta de un extenso historial de doctrina sobre privacidad. Comenzando por el «derecho a no ser molestado» de Warren & Brandeis' de 1890 (Samuel D. Warren & Louis D. Brandeis, 'The right to Privacy' (1890) 4 Harv. L. Rev. 193), y hasta el libro de Alan Westin titulado Privacy and Freedom (New York, Atheneum 1967), donde describe la privacidad como «la reivindicación de todo individuo, grupo o institución de la capacidad de poder determinar por sí mismos el momento, la forma y la extensión en que su información se comunique a otros». Y más recientemente: Daniel Solove, Understanding Privacy (Harvard University Press, 2008), donde el autor describe las distintas formas de privacidad y propone un marco general desde una perspectiva práctica. Véase también: Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life (Stanford University Press, 2010).
120. Von Hannover contra Alemania (2) Appl nos. 40660/08 and 60641/08 (ECtHR, 7 de febrero de 2012).
121. Ibidem, paras. 108 et seq.

tores también suelen citarse en los casos de derecho al olvido, tal y como se ha mostrado en los anteriores ejemplos.

A pesar del interés compartido en la legitimidad de dar a conocer la información personal al público, el debate actual mantenido en torno al derecho al olvido no coincide completamente con los rasgos del derecho al olvido. En lo fundamental, el derecho al olvido forma parte del derecho fundamental de todos a la privacidad (Artículo 7 de la Carta de los Derechos Fundamentales de la UE). Por otro lado, el derecho al olvido se considera un aspecto de la protección de los datos personales (Artículo 8 de la Carta): está relacionado esencialmente con la creación y el mantenimiento de un nivel razonable de privacidad de la información por medio de los mecanismos adecuados de control de los datos personales.

Esta distinción se refleja además en otro enfoque distinto: mientras que el derecho al olvido suele ser invocado como un escudo contra una intrusión desproporcionada de los grandes medios de comunicación (periódicos, noticiarios, reportajes radiofónicos, etcétera) en la vida privada de personas que alguna vez estuvieron expuestas a la opinión pública, el derecho al olvido no tiene la misma tradición ni connotaciones. Las personas que publiquen imágenes, vídeos o declaraciones indiscretos o inapropiados en páginas web públicas podrían padecer esta situación durante mucho tiempo, incluso aunque no exista un interés objetivo u orquestado de los medios de comunicación más importantes. De hecho, basta con que su nombre aparezca en tales materiales al utilizar motores de búsqueda o mecanismos similares de manera que se provoque cierto bochorno, estigma o perjuicio. El derecho potencial a ser olvidado para el más idóneo a la hora de atajar estos y otros problemas. Como tal, formaría parte de un marco jurídico europeo de protección de datos de mayor extensión destinado especialmente a proporcionar una base jurídica para los ciudadanos que ejerzan un mayor grado de control sobre la disponibilidad y uso de sus datos personales.

3.6.3 Factores reguladores de Lessig en relación con el derecho al olvido

Antes de examinar la forma en que la reciente propuesta de Reglamento de protección de datos pretende implantar el derecho al olvido merece la pena examinar hasta qué punto dicho derecho ya ha sido reconocido en la sociedad moderna mediante cualquiera de los cuatro factores reguladores identificados por Lawrence Lessig[122], es decir, las normas, el mercado, el código y la legislación.

Normas

La cuestión sobre el control se ha convertido en un tema que ha adquirido cada vez mayor importancia en la sociedad actual de la información, donde los datos personales se captan y tratan a escala masiva por medio de una cantidad prácticamente infinita de diferentes actores. Los individuos son cada vez más conscientes de su falta de comprensión sobre quiénes procesan sus datos y hasta qué punto. Aunque las actitudes en cuanto a lo que constituye exactamente la «privacidad» distan bastante, la mayoría de los ciudadanos ya parecen percibir la capacidad de controlar lo que ocurre con los datos personales como una norma valiosa. Esta tendencia, indicativa de un enfoque posiblemente más particular sobre la protección de la privacidad por el cual los individuos pretenden ostentar una titularidad más sólida de sus datos, se ha convertido en algo de especial relevancia en la era

122. Lessig, L., Code: Version 2.0 (Perseus Books 2006) 410.

digital[123]. Al final, la idea básica del derecho al olvido (la capacidad de eliminar los datos personales con carácter retroactivo), es meramente una manifestación de un deseo más fundamental de ejercer un mayor control sobre los datos personales propios.

También podría argumentarse, no obstante, que el hecho de olvidar (como tal) ya no se valora como una norma de la sociedad. El debate actual sobre el derecho al olvido podría no ser más que un intento regulador de promover una norma de una «sociedad análoga» que se debilita. Podría decirse que esta norma, tal y como se percibe, está desapareciendo gradualmente para dar cabida a una nueva que enfatiza la divulgación y el mantenimiento de los datos personales. Tal interpretación sugiere que el derecho al olvido que se ha propuesto está condenado al fracaso en la sociedad digital moderna, donde el valor por defecto es el recuerdo.

No obstante, las protestas públicas masivas[124] y el deseo general por conseguir mayor control[125] demuestran las preocupaciones de los sujetos registrados sobre las huellas digitales que van dejando[126] y sugieren que siguen apostando en gran medida por el olvido como una norma válida y valorada. Y lo que es más importante, conducen a creer que esta norma suele desatenderse a menudo y que aparentemente no es tan poderosa como para impulsar el cumplimiento en ausencia de otros factores reguladores. Los examinaremos con mayor profundidad en las siguientes páginas.

Mercado

Internet ha ido evolucionando de manera uniforme desde una red casi por completo «libre» hacia un entorno principalmente comercial. En este nuevo entorno, los datos personales se han convertido en la divisa más importante. El deseo desenfrenado por acumular esta divisa y la capacidad ilimitada de recopilación de datos de las tecnologías modernas han provocado un importante cambio de poderes entre los *usuarios* de los datos y los *sujetos* propietarios de los datos. En Internet, el último está casi indefenso ante el primero.

Incluso aunque el individuo sepa que sus datos están siendo recopilados/utilizados, a menudo no hay mucho que pueda hacerse para prevenir este hecho. Los procedimientos de notificación y descarga podrían eliminar datos de la esfera pública, pero a menudo no

123. Este enfoque sobre la protección de la privacidad fue muy popular a principios de la década del 2000, especialmente al otro lado del Atlántico (Pamela Samuelson, «Privacy as Intellectual Property?» (2000) 52 Stan L Rev 1125; Lessig (n 14), 200 et seq.; Paul Schwartz, «Property, Privacy, and Personal Data» (2004) 117 Harv L Rev 2055.). A pesar de ciertas (y válidas) críticas (como la extensión limitada y la incapacidad/insuficiencia a la hora de tratar con formas más amplias de perjuicios a la privacidad. Véase: Marc Rotenberg, «Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)» (2001) 2001 Stan Tech L Rev 1, 34-35; 91 et seq.; Yves Poullet, «Around the Concept of Privacy: Ethics and Human Rights in the Information Society?» (2008) 14 The European Files, 11.), este enfoque tan protector sobre la protección de la privacidad tiene ciertos méritos importantes. Para un análisis claro y conciso de los derechos de la propiedad como marco regulador de protección de los datos personales, véase: Nadezhda Purtova, «Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence» (2010) TILT Law & Technology Working Paper 2010/017 http://ssrn.com/abstract=1641027, 16 et seq.).

124. Kuner, Ch y otros, «Let›s not kill all the privacy laws (and lawyers)» (2011) 1 IDPL 209. Véase también: Omer Tene, «Privacy: The New Generations» (2010) 1 International Data privacy Law 15, 25; Rosen, «The Web Means the End of Forgetting» (n 3).

125. Un estudio reciente ha demostrado que los usuarios se sienten más cómodos cuando perciben un aumento del control sobre sus datos. Laura Brandimarte, Alessandro Acquisti & George Loewenstein, «Misplaced Confidences: Privacy and the Control Paradox», Privacy Papers for Policy Makers (septiembre de 2010), futureofprivacy.org/wp-content/uploads/2010/09/Misplaced-Confidences-acquisti FPF.pdf.

126. Comisión, «Comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI» COM(2012) 9 final, 25.01.2012, 4 et seq.; Comisión, «Por qué necesitamos una Reforma Europea de Protección de Datos», ec.europa.eu/justice/data-protection/document/index_en.htm.

los consiguen eliminar de los servidores de los usuarios de datos[127]. Las protestas públicas masivas (anteriormente mencionadas) y la cobertura de los medios tampoco han conseguido mejorar mucho el asunto. Y la reivindicación de que la competencia está «a solo un clic» suele ofrecer poco consuelo en este contexto: la efectividad del argumento del mercado libre depende de la transparencia[128] y no justifica los problemas de las externalidades de red y los bloqueos. Es más, los esfuerzos efectuados por los participantes del mercado[129] carecen a menudo de credibilidad, pues su modelo empresarial suele depender de la recopilación y uso de los datos personales. Resumiendo, el lado de los proveedores de servicios del mercado se inclina bastante contra el «olvido» de su moneda más valiosa.

En el otro lado del mercado, los consumidores parecen mostrar una demanda contradictoria de mayores servicios basados en el tratamiento de los datos[130], aunque al mismo tiempo solicitan más protección de su intimidad. A menudo apodado como la «paradoja de la privacidad»[131], este problema ilustra claramente la naturaleza multifacética de la privacidad como concepto. La paradoja contrapone las dos interpretaciones distintas de la noción, más concretamente al deseo de anonimato contra el deseo de controlar los datos personales. Los consumidores no tienen por qué querer necesariamente seguir siendo anónimos, pero quieren conservar cierto grado de control. Se podría decir que el lado del consumidor del mercado *quiere* que sus datos personales se procesen para los fines específicos y limitados que tiene en mente, y que sencillamente *acepta* la gama más amplia (y a menudo confusa) de objetivos que pretenden los responsables del tratamiento de los datos.

Para concluir, parece imposible basarse tan solo en el mercado para otorgar (o devolver) el control a los individuos, pues los proveedores de servicios no cuentan con los suficientes incentivos de mercado como para concederlo. Por otro lado, los consumidores sufren la falta de transparencia y de poder sobre el mercado para cambiar el status quo. El código y la legislación serán necesarios para otorgar cierto equilibrio al mercado.

Código

Dado que el comportamiento por defecto de los servicios *online* está impulsado más directamente por el código que por los otros tres factores reguladores, es importante considerar hasta qué punto se refleja (o debería reflejarse) el derecho al olvido en el código. Una de las ideas más interesantes y citadas habitualmente sobre cómo implantar este derecho es la de adjuntar una «fecha de vencimiento» a los datos personales[132]. Este

127. Los ciudadanos europeos pueden solicitar a Facebook que les envíe todos los datos personales que estén en su posesión: https://www.facebook.com/help/contact.php?show_form=data_requests. En estos informes queda patente que Facebook guarda los registros de todos los datos que se eliminen.

128. Incluso aunque la gente sepa cuál es la empresa que recaba o usa sus datos, nunca queda claro hasta qué punto sucede esto y en qué condiciones (las políticas de privacidad no suelen ofrecer muchas aclaraciones). El argumento adquiere matices cada vez más absurdos si se tiene en cuenta la cantidad de datos recopilados por empresas de las que nunca han oído hablar la mayoría de los usuarios (como agentes de datos tales como Acxiom y ChoicePoint).

129. La capacidad de que se desdibujen o se descarguen fotografías de Google Streetview (Verpixelungsrecht), en: Jeff Jarvis, Public Parts - How Sharing in the Digital Age Improves the Way We Work and Live (Simon & Schuster 2011), 27. Google, «How many German households have opted-out of Street View?» (Blog sobre Política Pública Europea, 21 de octubre de 2010) http://googlepolicyeurope.blogspot.com/2010/10/how-many-german-households-have-opted.html. Véase también la aplicación «ObscuraCam» en Android Market.

130. Un ejemplo claro son las redes sociales y la increíble cantidad de aplicaciones (para *smartphones*) que controlan y gestionan los datos de ubicación, los datos sobre el estado físico, los datos financieros, etc.

131. Andy Greenberg, «The Privacy Paradox», *Forbes*, 15 de febrero de 2008.

132. Mayer-Schönberger (n 1). Una aplicación reciente e interesante sobre este principio es la «aplicación TigerText» para los *smartphones*. Los mensajes enviados a través de esta aplicación se eliminan automáticamente tras un plazo predeterminado (tigertext.com).

concepto cuenta con la considerable ventaja de que los individuos ya no sufrirán la carga de ejercer un papel activo o responsabilidad después de compartir sus datos personales; el olvido de los datos es una característica por defecto, muy parecida al olvido natural de la memoria humana. Pero la puesta en práctica de este principio teórico dista de ser evidente. Por ejemplo, los datos personales podrían «etiquetarse» con una fecha de vencimiento como parte de sus metadatos[133]. No obstante, si se limita a este sencillo mecanismo informativo, el sistema se basaría en gran parte en la voluntad de los usuarios de los datos a la hora de respetarlo según su criterio. Por tanto, como tal (en ausencia de disposiciones legales que exijan el cumplimiento), el efecto del código podría ser limitado. De forma alternativa, podría insertarse en los datos una protección técnica más profunda, similar a la protección DRM de la propiedad intelectual[134]. Aunque se está llevando a cabo una investigación interesante a este respecto[135], estas tecnologías todavía están en fase inicial, y en este momento parece más factible a nivel técnico aplicar un sistema más sencillo (y ampliamente voluntario)[136].

En cualquier caso, no obstante, la viabilidad de tal programa de fechas de vencimiento parece viciada. En primer lugar, parece poco realista que cada persona introduzca una fecha de vencimiento cada vez que se recaben datos personales. Como tal, se corre el riesgo de convertirse en un mero requisito *pro forma* a quien nadie preste verdadera atención, con lo que se convertiría en otra nueva manifestación efectiva del sistema de consentimiento actual de defectuoso funcionamiento[137]. Además, no hay nada que evite que se copien o descifren los datos siempre que sigan disponibles[138]. Los agentes de la privacidad podrían contribuir a una mayor efectividad y atractivo de la capacidad de elección de los usuarios, a controlar todas las transmisiones de datos personales y a permitir que los usuarios gestionen las preferencias (de vencimiento) a lo largo del tiempo según distintos tipos de datos, controladores y contextos[139]. Sin embargo, este software de gestión de datos plantea nuevas dudas sobre la privacidad, pues crea un punto adicional en donde pueden recabarse los datos personales del usuario final[140]. En pocas palabras, aunque estas ideas podrían contribuir ciertamente al cambio de la balanza a favor del sujeto registrado en algunos contextos, la introducción de fechas de vencimiento seguramente no constituya una solución satisfactoria a los problemas sobre

133. Un ejemplo similar es el archivo robots.txt, por el que las páginas web pueden «excluirse voluntariamente» de los motores de búsqueda. Véase también: Jonathan Zittrain, «Privacy 2.0» (2008) Foro Legal de la Universidad de Chicago 65, 101 et seq

134. Ryan Calo, del Centro de Internet y Sociedad de Stanford (CIS), ha propuesto una interpretación más amplia de las disposiciones antielusión en la DMCA (en Europa, Directiva 2001/29/CE). Estas no deberían aplicarse solamente a casos de la propiedad intelectual, sino también cuando se eluda o ignore cualquier «medida técnica» destinada a proteger los datos (personales) (bloqueo/eliminación de cookies, exclusión voluntaria, modo incógnito, etc.). Véase: Ryan Calo, «DRM for Privacy: Part 2» (Opiniones concurrentes, 14 de agosto de 2011) www.concurringopinions.com/archives/2011/08/drm-for-privacy-part-2.

135. Investigadores de la Universidad de Washington trabajan en la actualidad en una tecnología denominada Vanish, que posibilita la autodestrucción de los datos después de un período concreto. «En vez de basarnos en Google, Facebook o Hotmail a la hora de eliminar los datos almacenados »en la nube" (dicho de otro modo, en sus servidores distribuidos), Vanish cifra los datos y después »destruye" la clave de cifrado. Para leer los datos, el ordenador debe reunir los restos de la clave, pero estos se »erosionan" u »oxidan" con el tiempo, y llegados a cierto punto el documento ya no puede leerse.» Si tiene éxito, la tecnología podría aplicarse además a cualquier tipo de datos almacenados en la nube. En: Rosen, «The Web Means the End of Forgetting» (n 3).

136. Mayer-Schönberger también critica la implantación a través de los DRM. Mayer-Schönberger (n 1), 144 et seq.

137. Barocas, S., & Nissenbaum, H. F., «On Notice: The Trouble with Notice and Consent» (2009) http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf.

138. Rosen, «The Web Means the End of Forgetting» (n 3).

139. Mayer-Schönberger (n 1), 172-173.

140. Especialmente en cuanto a la seguridad y quién tiene acceso a ella.

protección de los datos del internauta medio, al menos a corto plazo.

También existen otras soluciones, basadas principalmente en códigos, que sustentan el derecho al olvido. Además de la ingente cantidad de complementos de los exploradores que fomentan la privacidad[141], está surgiendo otra tendencia interesante en Internet, la de los administradores de reputación[142].

Estas páginas web ofrecen un control de toda la información que circule sobre los clientes, defendiendo su reputación por medios legales y técnicos[143] y creando así un planteamiento basado en un híbrido entre código/mercado del derecho al olvido. Dichos servicios demuestran además las posibles amenazas de censura debido a la distorsión de la información en Internet.

Las propuestas descendentes, vagas e inefectivas[144], y la anteriormente mencionada incapacidad del mercado a la hora de permitir que los individuos puedan controlar de manera efectiva lo que ocurre con sus datos personales han provocado una explosión de diversas iniciativas (principalmente) a nivel local por recuperar el control. Desde la perspectiva de las redes sociales, un ejemplo reciente a este respecto es Diaspora[145], una red social descentralizada creada desde sus cimientos teniendo en cuenta la protección de la privacidad. Los usuarios pueden albergar sus propios «servidores Diaspora», concediendo así en esencia a cada usuario el control completo sobre sus datos en su propio segmento de esta nube social. Mediante la eliminación de su propio segmento en la red social, los usuarios pueden controlar de manera efectiva la disponibilidad de sus datos en Diaspora, creando así una réplica limitada del derecho al olvido. Por supuesto, está por ver si dichos planteamientos atraerán a una audiencia lo suficientemente amplia para conseguir una adherencia relevante en el mercado.

En este capítulo se han explicado las soluciones basadas en códigos que pueden ser útiles a la hora de sustentar el derecho al olvido, pero que también tienen problemas para evitar que los datos personales sean copiados por terceros. Dependen completamente de la adopción voluntaria y de la buena fe de los responsables del tratamiento. Por tanto, para conceder (o devolver) el control efectivo a los usuarios, la intervención legislativa parece indispensable.

Legislación

La ley desempeña un papel importante cuando se trata de garantizar una protección suficiente de la privacidad de las personas. Y, de hecho, hasta cierto punto, la Directiva de protección de datos existente ya incluye el derecho al olvido en Europa. Aunque no se menciona de manera explícita, se consigue un efecto similar mediante dos mecanismos importantes previstos en la Directiva: el principio de la proporcionalidad y los derechos de los sujetos registrados.

El principio de la proporcionalidad está presente en toda la Directiva, pero en relación con el aspecto temporal del derecho al olvido, queda afirmado casi de forma clara

141. Véase: https://addons.mozilla.org/en-US/firefox/extensions/privacy-security. Erica Newland, «CDT Releases Draft Definition of »Do Not Track«» (Centro de Democracia y Tecnología, 31 de enero de 2011) http://cdt.org/blogs/erica-newland/cdt-releases-draft-definition-"do-not-track».

142. Reputation.com; reputationsquad.com; les-infostrateges.com; metalrabbitmedia.com; etcétera.

143. ReputationSquad incluso colabora con una compañía aseguradora (Swiss Life) para ofrecer asesoramiento financiero, legal y técnico en caso de que su «reputación digital» sea dañada, por 9,9€/mes. (Véase www.reputationsquad.com/2011/06/reputation-squad-lance-en-partenariatavec-swiss-life-la-premiere-offre-d'assurance-e-reputation.)

144. Por ej.: LRDP Kantor Ltd. & Centro de Reforma Pública, «Estudio comparativo sobre los distintos planteamientos sobre los nuevos retos de la privacidad, en especial a la luz de los avances tecnológicos» (Comisión Europea, 20 de enero de 2010) http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf, 46 et seq.

145. Diasporafoundation.org.

en el Artículo 6.1(e): los datos personales serán «conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente». El Artículo 6(1)(d) especifica además que los «datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados». En conjunto, estas normas exigen a los responsables del tratamiento que eliminen los datos personales si ya no se necesitan para los fines legítimos del tratamiento de datos. Efectivamente, esta obligación puede considerarse de manera que cree un «derecho pasivo a ser olvidado», en forma de una obligación de justificación para los responsables de los datos: si ya no pueden demostrar un motivo legítimo por el que se mantengan los datos personales, entonces deberán eliminarlos.

No obstante, la importancia de este derecho pasivo no debería sobrestimarse: en la práctica, esta norma tiene muy poca aplicación. Es más, los responsables del tratamiento tienen un margen de apreciación importante a la hora de determinar el plazo en que el mantenimiento de los datos personales sirve todavía a objetivos legítimos. Un operario de una red social, por ejemplo, puede asumir una postura (correcta o incorrecta) por la que el mantenimiento de los datos personales proporcionados por sus usuarios durante un plazo indefinido es legítimo si entra dentro de los fines legítimos de las actividades de la red.

Se necesita un marco de derechos más activo, y puede encontrarse parcialmente en los derechos existentes de los sujetos registrados. La Directiva permite a los sujetos registrados solicitar a los controladores de los datos que indiquen cuáles de sus datos personales se están procesando[146] y pidan la «rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos»[147]. Según esta última disposición, los sujetos registrados podrían solicitar hoy día que se eliminaran sus datos personales si ya no son exactos o relevantes para los fines que se indicaran originalmente, o sencillamente si el período razonable de almacenamiento se ha superado de manera evidente (quebrantamiento del principio de la proporcionalidad). Sin embargo, esta posibilidad teórica significa muy poco en la práctica, especialmente si el sujeto registrado ha dado su consentimiento al tratamiento de sus datos para ciertos fines, pues el responsable de dicho tratamiento bien puede replicar que los datos siguen siendo precisos y relevantes para los fines acordados y estando dentro del margen de un mantenimiento razonable. En tal caso, los sujetos registrados seguramente no consigan resarcimiento alguno a raíz del derecho existente de eliminación[148].

Aunque el sistema legal europeo actual establece varios principios y derechos sólidos que sustentan un derecho «diluido» a ser olvidado, las disposiciones específicas contienen puntos de flaqueza que dificultan su efectividad en la práctica. Entre estos se encuentran, en particular, su ineficacia parcial cuando se da el consentimiento y el amplio margen de apreciación que se deja a los responsables del tratamiento por medio de

146. Artículo 12(a) de la Directiva de protección de datos.

147. Artículo 12(b) de la Directiva de protección de datos

148. El derecho independiente de oposición (Artículo 14 de la Directiva) se enfrenta a problemas similares: los sujetos registrados podrían «oponerse en cualquier momento y por razones legítimas y de peso propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento» en los casos en los que el tratamiento de los datos esté justificado según su necesidad de efectuar una tarea en pos del interés público, o según un interés legítimo del controlador de datos. Dado que el ejercicio de estos derechos exige que las oposiciones se basen en «razones legítimas y de peso», seguramente el resultado conseguido tampoco sea satisfactorio.

la dependencia en los fines especificados. El sistema de consentimiento actual ya no cumple con las expectativas de la gente[149], ni ofrece los mecanismos de protección efectivos en casos en que el derecho al olvido sería mucho más útil. La «Opinión sobre el consentimiento» del Grupo de Trabajo del Artículo 29[150] ha enfatizado recientemente que se debería permitir siempre a los individuos la retirada de su consentimiento. No obstante, la retirada tan solo afecta al tratamiento de datos en el futuro, es decir, después de oponerse, y por tanto no sería efectiva para actos de tratamiento de datos que ocurrieran antes.

Es más, el efecto de «filtración» de estas disposiciones es limitado: si el sujeto registrado ejerce su derecho a la rectificación, supresión o bloqueo de los datos, el responsable del tratamiento de los datos deberá enviar una «notificación a los terceros a quienes hayan comunicado los datos [...] si no resulta imposible o supone un esfuerzo desproporcionado»[151]. La Directiva, aun así, no especifica si esta disposición se aplica ni cómo en los casos en que los datos se publican en Internet, lo cual en la práctica significaría que se revelan potencialmente a todos los usuarios de la Red. En estos casos, los responsables del tratamiento podrían sentirse tentados a aducir que no se requiere notificación, pues esta no resultaría efectiva para notificar a todos los receptores reales.

Evidentemente, en los casos en que el tratamiento de datos esté justificado en cierto punto debido a que el sujeto registrado haya otorgado su consentimiento de forma válida, el marco legal no es capaz de ofrecer un grado de control relevante a los sujetos registrados sobre sus propios datos personales. Por ello, el «derecho al olvido», de forma condicional, podría parecer una solicitud legítima a la hora de restablecer el equilibrio de poder. Este es uno de los objetivos que pretende conseguir el nuevo Reglamento de protección de datos. En la sección que sigue se examinará la forma y la extensión en que el Reglamento propuesto es capaz de lograrlo.

3.6.4 Puesta a punto de la normativa: la propuesta de Reglamento de protección de datos

El pasado enero, la Comisión Europea propuso finalmente el esperado proyecto de revisión del marco legal europeo sobre protección de datos (véase *Anexo D*)[152]. Aunque se calcula que la versión final adquirirá rango de ley de aquí a dos años[153], resulta útil evaluar el proyecto actual, que representa los tres años de reflexión, consultas y debates, con el fin de valorar la forma en que ataja los problemas anteriormente descritos.

Los dos objetivos principales del Reglamento propuesto son el fomento del control efectivo de los individuos sobre sus datos personales al tiempo que se proporcione la certeza jurídica y se minimice la carga administrativa para las empresas. Uno de los aspectos añadidos para conseguir el primer objetivo es

149. El Día de los Tontos de abril de 2010, el fracaso del sistema de consentimiento fue demostrado a modo de burla por Gamestation.co.uk después de introducir una «cláusula de alma inmortal» en sus condiciones de servicio. James Temple, «Privacy policies that don't work - and some that might» The Sydney Morning Herald (Sidney, 30 de enero de 2012) http://www.smh.com.au/technology/technology-news/privacy-policies-that-dont-work--and-some-that-might-20120130-1qp4m.html.

150. Opinión sobre el consentimiento, Grupo de Trabajo del Artículo 29 (WP187), 13 de julio de 2011; véase http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf; última visita el 15 de febrero de 2012.

151. Artículo 12(c) de la Directiva

152. Para comprobar la obra completa de la Comisión, véase: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

153. Kuner, Ch., «The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law» (2012) 11 PVLR 06, 2.

la introducción de un «derecho al olvido y a la eliminación» explícito que se fundamente sobre el derecho existente (aunque más limitado, tal y como se comentaba) a la eliminación descrito en el Artículo 12(b) de la Directiva. Según el texto de la Comisión, esa disposición pretende «garantizar que todo individuo que no desee que sus datos personales sigan siendo procesados, y siempre y cuando la organización no disponga de motivos legítimos para mantenerlos, estos sean eliminados».[154]

Fundamentos del derecho propuesto

Antes de profundizar en la disposición real, cabe aclarar brevemente las justificaciones que sustentan el derecho al olvido. El derecho hace las veces de una especie de válvula de seguridad contra problemas imprevistos sobre privacidad. Especialmente en la sociedad actual de la información, resulta prácticamente imposible predecir todas las consecuencias (negativas) del uso de los datos personales. Y aunque puedan preverse unas cuantas, tienden a ser abstractas, distantes e inciertas. Son abstractas porque las intrusiones en la privacidad a menudo afectan a cuestiones sociales, psicológicas y similares. Son distantes porque no se presentan directamente. Y son inciertas porque quizá nunca ocurran, o al menos de manera predecible. Como resultado, incluso aunque un individuo pudiera reconocer a nivel intelectual que dicho uso podría tener consecuencias negativas, el hecho de que se percate podría no ser suficiente para cambiar su comportamiento. Además, los datos personales suelen recabarse y utilizarse sin que pueda controlarlo o ni siquiera saberlo el propio individuo. Y lo que es peor, los esfuerzos que *pueden* hacer las personas para «proteger su privacidad» *online* son a menudo ignorados y pueden burlarse con facilidad. Teniendo todo esto en cuenta, resulta evidente que cargar toda la responsabilidad al sujeto registrado en cuanto a la prevención de cualquier perjuicio posible a la privacidad es injusto e irrealista.

Es más, la misma noción de los «datos personales» es muy ambigua, y no debería considerarse un concepto estático[155]. La información puede vincularse y desvincularse a una persona conforme pasa el tiempo, en relación con los distintos actores y en los diferentes contextos, dependiendo de su uso y de la manera en que se enriquece con datos secundarios. Se necesita un enfoque flexible y casuístico que tenga en cuenta la transformación constante de los «datos» como tal. Podría decirse que el «derecho al olvido» daría a las personas la oportunidad efectiva de (re)evaluar de manera permanente el uso de sus datos según los fines en constante cambio de unos contextos tan dinámicos[156]. Además, reforzaría el control del

154. El discurso de la comisaria europea Viviane Reding por el que presenta la nueva propuesta está disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/827&type=HTML.

155. Véase, por ejemplo, la distinción efectuada entre los datos relacionados con una persona identificada y una identificable: Paul M. Schwartz & Daniel J. Solove, «The PII Problem: Privacy And A New Concept Of Personally Identifiable Information] (2012), 68 NYU Law Review 1814. David Ardia describe la identidad como un continuo con anonimato en un extremo y una revelación total de la identificación personal en el otro. La información online se desplaza permanentemente (hacia delante y atrás) por este eje. Véase: David S. Ardia, «Reputation in a Networked World: Revisiting the Social Foundations of Defamation Law» (2010), 45 Harv. C.R.-C.L. L. Rev. 261, 307.

156. Para más información sobre la privacidad contextual, véase: Nissenbaum (n 8). Servicios tales como 123people.com o «date check» (intelius.com/mobile) reúnen los datos de toda la red y constituyen un gran peligro para una contextualización adecuada. Las redes sociales tampoco aportan herramientas suficientes de contextualización. Véase: Danielle Citron, «Aligning Privacy Expectations with Technical Tools» (Opiniones concurrentes, 10 de abril de 2011) http://www.concurringopinions.com/archives/2011/04/aligning-privacy-expectations-with-technical-tools.html. Jonathan Zittrain conjetura que podrían ofrecerse incluso servicios en el futuro que calculen el atractivo social « a partir de cálculos sociales por minutos (como cuántas veces se ha acercado o evitado a otras personas en fiestas (una clasificación fácil de controlar con la tecnología actual por medio de los móviles y Bluetooth)». También prevé el surgimiento de «brokers de reputación», que proporcionen asesoramiento sobre la «sociabilidad, fiabilidad y empleabilidad» de las personas. Véase: Rosen, «The Web Means the End of Forgetting» (n 3).

individuo sobre su propia identidad[157], haciendo posible una comprobación más efectiva del principio de limitación de los fines y aumentando la responsabilidad de los responsables de los datos[158]. En consecuencia, estos controladores podrían disfrutar de un mayor incentivo a la hora de implantar políticas más orientadas hacia la privacidad, pues los individuos tendrían derecho a exigir una eliminación retroactiva de sus datos.

En resumen, desde la perspectiva política, los beneficios y el atractivo del derecho al olvido parecen evidentes. El siguiente apartado se centra en evaluar hasta qué punto el derecho al olvido (tal y como lo propone el Reglamento) es adecuado para conseguir estos objetivos.

La disposición propuesta

Ámbito

Con el fin de evitar cualquier efecto secundario negativo (y, en particular, de garantizar la protección efectiva de la libertad de expresión), el derecho exige una definición correcta del ámbito de aplicación y ciertas excepciones relevantes. En primer lugar, es importante evaluar la aplicabilidad del Reglamento en su totalidad (Artículo 2). En los casos de tratamiento de datos que no se incluyan en el ámbito del Reglamento (como, por ejemplo, cuando los datos se procesen para uso personal o con fines de seguridad nacional), obviamente, el «derecho al olvido» no se aplicará. Seguidamente, debería evaluarse la aplicabilidad de la disposición en cuestión (en la actualidad, el Artículo 17).

El primer párrafo del artículo relevante describe cuatro situaciones en las que un individuo debería tener derecho a «solicitar al responsable del tratamiento que elimine sus datos personales y se abstenga de seguir divulgándolos»: tienen relación con casos en los que a) el tratamiento de datos quebrante el principio de limitación de los fines; b) el consentimiento al tratamiento de los datos se retire o los períodos legítimos se superen; c) se haya ejercido el derecho a oponerse al tratamiento de datos, y d) el tratamiento de los datos sea ilegal (es decir, cuando no cumpla con el Reglamento).

El impacto práctico del primer motivo, que permite a los usuarios solicitar la eliminación de sus datos cuando ya no se necesiten para los fines a los que se recopilaron, es cuestionable. Tal y como se comentó anteriormente (3.6.3 Legislación), el principio de limitación de los fines ha adquirido mayor ambigüedad dentro de una Internet cada vez más personalizada, donde puede discutirse la relevancia de prácticamente cada dato personal. Especialmente si se tiene en cuenta el texto vago y amplio de las especificaciones de dichos fines. El tercer y cuarto motivos son relativamente claros y concisos. En situaciones en que el sujeto registrado tiene derecho a oponerse al tratamiento de sus datos personales (según el Artículo 19), o cuando el tratamiento de los datos es ilegal en su conjunto, el individuo debería tener siempre claro que puede solicitar la eliminación de sus datos. Aunque es posible que estos tres motivos ya se encontraran implícitos en la Directiva actual, el segundo es más digno de mención, pues establece el «derecho al olvido» en situaciones en que el sujeto registrado retire su consentimiento o cuando haya transcurrido el período de almacenamiento inicial (la idea de la fecha de vencimiento).

La noción básica por la que se otorga a los individuos la posibilidad de terminar de manera unilateral su relación con el responsable/encargado del tratamiento de los datos se ocupa del desequilibrio importante existente en el sistema de protección de datos actual. En la práctica, el tratamiento de datos basado

157. Sobre la importancia del control de cada individuo sobre su reputación, véase: Solove, The future of Reputation: Gossip, Rumor, and Privacy on the Internet (n 2), 33.

158. Véase: Grupo de Trabajo del Artículo 29, «Opinión 3/2010 sobre el principio de responsabilidad» GT 173.

en el consentimiento no suele ofrecer una verdadera opción y control al sujeto registrado. Por este motivo, la propuesta de Reglamento ha restado importancia al consentimiento, por ejemplo permitiendo de manera explícita a los sujetos registrados que lo retiren (Artículo 7[3]). La inclusión del derecho al olvido se basa en esta tendencia por la que se permite a los sujetos registrados ampliar el impacto de esta retirada de los datos personales que en el pasado se hubieran conseguido de forma legítima. La propuesta (considerandos 47-48) exige además que se informe a los sujetos registrados sobre su derecho a la eliminación y que se incluyan modalidades que permitan ejercer dicho derecho.

El segundo párrafo[159] va todavía más allá y propone que el derecho debería acompañar a los datos cuando el responsable del tratamiento de estos los haga públicos (por ejemplo, publicándolos en una página web) o cuando la publicación se delegue a un tercero. En el primer escenario, el responsable del tratamiento original tan solo debe tomar «todas las medidas razonables» destinadas a informar a terceros sobre la solicitud de eliminación del sujeto registrado[160]. En la segunda situación, el responsable del tratamiento original se considerará responsable en cualquier situación.

Aunque no cabe duda de que la idea que subyace a este párrafo (el derecho al olvido debería acompañar a los datos cuando cambien de manos) tiene su valor, debería reformularse. Tal y como está en la actualidad se podría aducir que dicha inclusión es tanto demasiado exhaustiva como no lo suficientemente exhaustiva. Por norma general, no se debería responsabilizar a los responsables del tratamiento ante cualquier uso de los datos personales por parte de un tercero que se suceda sin la implicación o conocimiento de los primeros. Desde esa perspectiva, la ambigüedad de la obligación genérica de tomar «todas las medidas razonables [...] para informar» a los terceros cuando se ejerza dicho derecho es preocupante. Además, tal deber crea inquietudes legítimas en cuanto a un posible efecto disuasorio, especialmente teniendo en cuenta las nuevas y mucho más severas sanciones del Reglamento[161]. De forma similar, la simple afirmación de que los responsables del tratamiento «deberán ser considerados responsables» de la publicación de los datos personales por parte de un tercero cuando lo hayan autorizado empaña la complejidad de los mecanismos subyacentes. ¿Cuándo se «autorizará» la publicación? ¿Y qué implica el hecho de ser «responsable» de manera concreta en términos de deberes u obligaciones? En cuanto a estas cuestiones, el borrador actual deja mucho que desear y podría interpretarse como demasiado exhaustivo.

Desde una perspectiva distinta, esta disposición también podría no ser lo suficientemente exhaustiva. El segundo párrafo del Artículo 17 se centra exclusivamente en los casos en que los datos se han publicado, tanto de manera directa como a través de un tercero. En este sentido, esta contemplación recuerda a las aplicaciones tradicionales del derecho al olvido, tal y como se ha descrito con anterioridad. Sin embargo, no parece haber un motivo a simple vista para este enfoque exclusivo. Se podría argumentar que el derecho al olvido tiene la misma importancia (y quizá mucha más) en situaciones en que los datos se mantengan y procesen sin necesidad de publicarlos, es decir, dentro del contexto de la creación de perfiles (comerciales). Si

159. Véase, asimismo, el considerando 54, que es prácticamente idéntico.

160. En la propuesta filtrada en noviembre todavía no se había incluido la comprobación de «todas las medidas razonables», y el controlador original debía asegurarse de la eliminación de cualquier enlace, copia o réplica que se hubieran hecho públicas.

161. Rosen, J., «The Right to be Forgotten» (2012) 64 Stan. L. Rev. Online 88, http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

los sujetos registrados ejercen su derecho al olvido, parece razonable esperar que el responsable del tratamiento de los datos deba eliminar todos los datos, independientemente de los fines para los que los utilizara[162], e incluso fuera del contexto de la publicación. Un ámbito tan amplio garantizaría que no se cree de forma encubierta un perfil de los sujetos registrados a partir de información de la que quizá no sean conscientes, y que podría no ser (ya) correcta o válida.

A una escala superior, el ámbito de este segundo párrafo es mucho más desconcertante si se tiene en cuenta el Artículo 13 del Reglamento, que incluye unas normas más generales sobre la forma en que los derechos del sujeto registrado pueden acompañar a sus datos. Esta disposición ya afirma que el responsable del tratamiento debe comunicar las solicitudes de eliminación a todos los receptores de los datos personales a quienes se remitieran, a menos que resulte imposible o suponga un esfuerzo desproporcionado. Para evitar el debate en torno a la relación entre el ámbito del Artículo 14 y el del Artículo 17(2), el Reglamento podría obtener mejores resultados si estas disposiciones se armonizaran de manera más explícita. Podría incluso resultar apropiado eliminar el Artículo 17(2) por completo e integrar otras cláusulas relevantes en torno al derecho al olvido en el Artículo 13. Esta oportunidad podría aprovecharse para garantizar que el derecho acompañara a los datos (tan solo) si el responsable del tratamiento los transmite de manera consciente a un tercero, lo cual parece más viable y podría limitar los efectos disuasorios. Cuando se publican los datos, estos pueden copiarse (o procesarse de cualquier modo) por parte de terceros en ausencia de acuerdo con el responsable del tratamiento original, pero dichos terceros deben tener motivos legítimos para procesar los datos.

Por último, cabe mencionar que la Comisión se reserva el derecho a adoptar «actos delegados» por los que se especifiquen los criterios y requisitos para la aplicación del derecho en los sectores y situaciones específicos, pero también por los que se establezcan las condiciones relativas al enigmático segundo párrafo. Evidentemente, resulta difícil evaluar el posible impacto de esta competencia en el estadio actual.

Excepciones

Incluso teniendo en cuenta el ámbito del artículo en su formato actual, persisten los riesgos de abuso. Para evitarlos, el Artículo 17(3) establece ciertas excepciones a la propuesta actual. En los casos en donde la solicitud de eliminación se base en la retirada del consentimiento, los datos personales no deberían eliminarse si existen otros motivos legítimos por los que deba proseguir el tratamiento de estos. Es más, el apartado 3 determina que el responsable del tratamiento podrá optar por retener los datos si es necesario: a) para proteger el derecho a la libertad de expresión; b) por motivos de interés público en el área de la sanidad pública; c) para fines de investigación histórica, estadística y científica, y d) para el cumplimiento, por parte de la Unión o de un Estado miembro, de una obligación legal con respecto al mantenimiento de los datos personales[163].

Los datos personales también podrán retenerse (aunque el controlador debe restringir su tratamiento)[164] en los siguientes casos: a) cuando el sujeto registrado aduzca que no

162. Salvo algunas excepciones (véase más adelante).

163. Dichas leyes deberían, no obstante, «cumplir con el objetivo del interés público, respetar la esencia del derecho a la protección de los datos personales y ser proporcionales al objetivo legítimo perseguido».

164. El uso, en estos casos, debería limitarse al tratamiento «para fines de comprobación, o con el consentimiento del sujeto registrado, o para la protección de los derechos de otra persona física o jurídica o bien para fines de interés público» (Artículo 17, párrafos 4-5).

son correctos (durante un período que permita al responsable del tratamiento verificar la corrección de los datos); b) para fines de comprobación; c) cuando el sujeto registrado se oponga a su eliminación (incluso aunque el tratamiento sea ilegítimo) y solicite la restricción de su uso en cambio, y d) para fines de portabilidad de datos.

Aunque la aplicación de estas excepciones puede no ser definida en la práctica, son absolutamente necesarias para equilibrar el derecho al olvido frente a otros derechos fundamentales, tal y como indica el considerando 139 del Proyecto. En la práctica, podría resultar difícil a los responsables de los tratamientos el hecho de tomar estas decisiones. El apoyo pragmático y rápido de las autoridades nacionales de protección de datos podría mitigar estas cuestiones hasta cierto punto.

Problemas de cumplimiento y efectos disuasorios

En la práctica, el cumplimiento podría resultar una carga para los responsables de los tratamientos de datos. De hecho, se ha alegado que el nuevo derecho podría ejercer un efecto disuasorio sobre el uso de Internet en la UE[165]. La imposición de obligaciones a intermediarios (suelen ser los responsables de los tratamientos en el entorno *online*) a la hora de tomar decisiones complejas en torno a la eliminación de los datos personales podría fomentar una censura preventiva y frenar la innovación[166]. Por ello, es imprescindible que los intermediarios sigan sacando partido del sistema de exención de responsabilidad en vigor de la Directiva sobre el comercio electrónico[167] (Artículos 12-15). Su capacidad debería limitarse a las actividades de tratamiento de datos que ellos mismos hayan iniciado o que hayan organizado a través de encargados del tratamiento de los datos para sus propios fines. Para garantizar una aplicación efectiva y sistemática en toda la Unión, la Comisión ha propuesto además una reestructuración considerable de las autoridades nacionales de protección de datos (denominadas ahora «autoridades de supervisión independientes») y el endurecimiento de los recursos administrativos y judiciales.

Terminología problemática

Teniendo en cuenta el ámbito y el significado actual de la disposición en cuestión, el concepto «derecho al olvido» parece haber sido mal escogido y podría dar lugar a expectativas poco realistas. Desde que Mayer-Schönberger acuñara el término, se ha convertido en un concepto cada vez más promocionado y que se ha abierto camino a pasos acelerados en los debates políticos. No obstante, este término enfatiza de manera excesiva las restricciones u obligaciones de los demás, percepción que ha provocado muchas más protestas de las que lo habría hecho una descripción mucho más precisa[168]. En vez de intentar recrear de manera artificial un fenómeno natural al imponer el deber de «olvidar» a otros, el Reglamento debería ceñirse a un «derecho de eliminación» más concreto que se centrara, por el contrario, en el sujeto registrado. La exención del uso personal (Artículo 2(2)(d)) demuestra, además, de forma evidente, la determinación del Reglamento a no entrometerse en la privacidad de los individuos. Dicho de otro modo, el derecho no se presenta ni debería presentarse como una herramienta de control de la libertad de otros a recibir o transmitir información. Simplemente pretende permitir a los *sujetos*

165. Kuner (n 45), 6.
166. Rosen, «The Right to be Forgotten» (n 53).
167. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior, DO L 178, 17.7.2000, 1-16.
168. Para un examen más profundo sobre la terminología inadecuada, véase: Paul A. Bernal, «A Right to Delete?», Revista Europea sobre Derecho y Tecnología 2 (2011), http://ejlt.org//article/view/75/144.

registrados controlar de forma eficiente lo que hacen con sus datos.

3.6.5 Conclusión

Este capítulo contiene un breve resumen de la situación actual del «derecho al olvido». Tal y como se muestra en la primera sección, el denominado *droit à l'oubli* conseguía objetivos similares cuando se vulneraban los derechos fundamentales a la privacidad o la personalidad. El derecho al olvido que se debate en la actualidad, no obstante, sostiene un planteamiento más práctico y se centra en la privacidad de la información. A la luz de los cuatro factores reguladores de Lessig, se observó que la sociedad ya percibe este derecho, hasta cierto punto, como una norma, pero las otras tres modalidades (el mercado, el código y la legislación) lo manejan de forma insatisfactoria.

Si se observan los fundamentos de derecho que sustentan la disposición en cuestión de la propuesta de Reglamento general de protección de datos, resulta evidente que podrían obtenerse ciertas ventajas si el sujeto registrado dispusiera de unos derechos más sólidos en relación con la eliminación de los datos personales. Sin embargo, una evaluación crítica del borrador actual muestra además sus diversos defectos, entre los que se incluyen la elección desafortunada de la terminología, su ámbito demasiado y no lo suficientemente exhaustivo al mismo tiempo, y la ambigüedad excesiva de las disposiciones relativas a la capacidad del derecho a acompañar a los datos al pasar por distintas manos. Como resultado, los controladores de datos se enfrentarían probablemente a dificultades interpretativas de importancia a la hora de cumplir con el proyecto actual. Este hecho, a su vez, podría provocar efectos disuasorios, especialmente teniendo en cuenta las multas sustanciales que prescribe el texto actual, y sería contraproducente para el objetivo general del Reglamento consistente en proporcionar una mayor certeza jurídica. Así, aunque la idea del derecho al olvido podría valer la pena, el proyecto actual parece necesitar un reajuste importante.

La búsqueda de la humanidad por la memoria permanente y omnisciente está alcanzando su apogeo. Los avances tecnológicos podrían ser imparables en esta sociedad de la información actual tan interconectada y de memoria ilimitada. Lo que la gente *puede* hacer es reclamar cierto control sobre sus datos. El derecho al olvido es solamente un ejemplo (aunque importante) de cómo se puede otorgar (o devolver) dicho control. Tan solo el tiempo dirá si dicho derecho es el más adecuado y el método más efectivo para contribuir a un equilibrio de poderes más equitativo en cuanto a los datos personales.

Ricard Martínez Martínez

Ricard Martínez Martínez es doctor en Derecho y profesor de Derecho Constitucional de la Universidad de Valencia, y ha dedicado su investigación al estudio del derecho fundamental a la protección de datos y a distintas cuestiones relacionadas con las repercusiones de las tecnologías de la información y las comunicaciones en la vida privada. Actualmente preside la Asociación Profesional Española de Privacidad (www.apep.es). Ha sido coordinador del Área de Estudios de la Agencia Española de Protección de Datos. Es autor de distintas monografías dedicadas a esta materia: *Tecnologías de la Información*, *Policía y Constitución*, *Una aproximación crítica a la autodeterminación informativa*, y ha participado como autor o coordinador en distintos comentarios al Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos, y en la monografía *Derecho y redes sociales*, y próximamente publicará la obra *Derecho y Cloud Computing*. Participa como conferenciante y docente en los principales másteres y eventos sobre esta materia en España.

3.7 El derecho a la vida privada en España

Ricard Martínez Martínez
Profesor de Derecho Constitucional de la Universidad de Valencia
Presidente de la Asociación Profesional Española de Privacidad

3.7.1 La protección de la vida privada en la Constitución Española de 1978

El artículo 18 de la Constitución Española (CE) contempla la tutela de la vida privada de modo integral[169]. En la práctica ello supone abordar el conjunto de cuestiones relacionadas con la privacidad tanto desde la perspectiva de los derechos fundamentales entendidos como límites a la acción estatal –inviolabilidad del domicilio, secreto de las comunicaciones y captación de imágenes por sistemas de videovigilancia–, como desde el punto de vista de los daños que para la persona pueden derivar de las revelaciones de datos íntimos, del menoscabo de su honor o el uso inadecuado de su imagen[170], o finalmente la regulación del impacto de las tecnologías de la información en los derechos de la personalidad.

El contenido del art. 18 de la CE, y particularmente el derecho fundamental a la protección de datos admite una interpretación que supera la tradicional concepción de la intimidad, otorgando a su titular el derecho a obtener prestaciones positivas, del Estado y de los particulares. Puede afirmarse con rotundidad que es un derecho de textura abierta que atribuye poderes de control sobre la información personal, y está claramente orientado a ofrecer una esfera de protección frente a los avances tecnológicos.

El derecho a la intimidad

El Tribunal Constitucional español ha caracterizado el derecho a la intimidad como un derecho de ejercicio personalísimo, pero ante todo como manifestación de la dignidad humana[171]

169. En efecto este dispone: «Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de fl agrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráfi cas y telefónicas, salvo resolución judicial. 4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

170. En España la tutela civil de este derecho se regula por la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

171. Véase la STC 53/1985: «Junto al valor de la vida humana y sustancialmente relacionado con la dimensión moral de esta, nuestra Constitución ha elevado también a valor jurídico fundamental la dignidad de la persona, que, sin perjuicio de los derechos que le son inherentes, se halla íntimamente vinculada con (...) al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1). Del sentido de estos preceptos puede deducirse que la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás.» (FJ núm. 8 Caso Despenalización del aborto).

y garantía de la autodeterminación individual. Asimismo, no se trata de una realidad estática, sino que debe ser contemplado a partir del contexto y del momento histórico[172] en el que se inserta.

Si algo caracteriza a este derecho es la multitud de facetas que presenta. Como suele decirse, nadie sabe definir con certeza qué es el derecho a la intimidad pero un juez lo reconoce en cuanto se lo encuentra[173]. Así el Tribunal Constitucional, en la sentencia[174] STC 73/1982, planteó un concepto estricto de intimidad como «reducto» y diferente de la «libertad de relacionarse», lo que prácticamente reducía el espacio de vida privada a la vida familiar en el marco del domicilio, posición que no se ha mantenido en absoluto en la posterior trayectoria jurisprudencial.

En segundo lugar, es un derecho personalísimo sin perjuicio de que puedan derivarse responsabilidades patrimoniales por el uso de la imagen de un fallecido[175]. Ahora bien, el Tribunal entiende que lo que la Constitución tutela es el derecho a la intimidad personal y familiar[176]. En cualquier caso, su titularidad se limita a las personas físicas, excluyendo a las personas jurídicas tuteladas a través de otras técnicas como la protección de secretos industriales y patentes. Si bien, el Alto Tribunal ha extendido a las personas jurídicas la titularidad de la inviolabilidad del domicilio, y del honor[177].

Por otra parte, como el resto de los derechos, la intimidad no es un derecho absoluto, cede en determinadas situaciones y ante concretos valores y derechos constitucionales que se consideran más dignos de tutela[178]. Por último, puesto que su objeto de tutela no es otro que información personal, el significado del derecho a la intimidad no es unívoco. Por ello, puede hablarse de una intimidad familiar, económica[179], corporal[180], o relacionada con la salud[181], la vida sexual[182] (incluidos supuestos de acoso)[183], o la genética.

El derecho a la intimidad y el derecho a la propia imagen

El derecho a la intimidad y el derecho a la propia imagen poseen identidad propia aunque se encuentran directamente interrelaciona-

172. «Intimidad y honor son realidades intangibles cuya extensión viene determinada en cada sociedad y en cada momento histórico, cuyo núcleo esencial en sociedades pluralistas ideológicamente heterogéneas deben determinar los órganos del Poder Judicial.» (STC 171/1990, caso Comandante Patiño).

173. «The Justices might not be able to say what privacy is, but they know it when they see it». Rubenfeld, Jed. «The right of Privacy», en Harvard Law Review, vol. 102, núm. 4, 1989, págs. 737-807 (cita en p. 751).

174. Las sentencias del Tribunal Constitucional citadas en este artículo pueden obtenerse en http://bit.ly/hCy82n.

175. En el Ordenamiento español es posible para los causahabientes el ejercicio de acciones civiles en defensa del honor, la intimidad o la imagen de una persona fallecida, conforme al artículo 4 de la Ley Orgánica 1/1982, aunque en estos casos no existe tutela constitucional ya que los derechos fundamentales se extinguen con la personalidad.

176. «Debe estimarse que, en principio, el derecho a la intimidad personal y familiar se extiende, no solo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen.» (STC 231/1988 FJ núm. 4).

177. El Tribunal Constitucional les ha negado la titularidad de este derecho (STC 37/1985).

178. Véase SSTC 11/1981 y 57/1994 y Aguiar, L. «Dogmática y teoría jurídica de los derechos fundamentales en la interpretación de éstos por el Tribunal Constitucional español», en Revista de Derecho Político núms. 18-19, verano-otoño 1983.

179. Véase SSTC 110/1984, (FJ 5) y 142/1993.

180. En la STC 37/1989 (FJ núm. 7), relacionada con una prueba pericial, subraya, por un lado, la inviolabilidad del cuerpo humano y la necesidad de respetar la dignidad y, por tanto, de practicar este tipo de pesquisas con arreglo a la Ley y con autorización judicial, y por otro, la concepción cultural de la privacidad en este ámbito.

181. Véase STC 20/1992 (caso Arquitecto con VIH), STC 232/1992, sobre publicación de cuidados médicos recibidos por un personaje público, y STC 202/1999 sobre uso de datos de salud por una entidad bancaria.

182. Véase la STC 151/1997.

183. La STC 224/1999 erige el derecho a la intimidad, junto con el principio de no discriminación, en fundamento constitucional frente a las prácticas de acoso sexual.

dos ya que se ordenan a la protección de la vida privada. El Tribunal ha definido el derecho a la propia imagen:

> *Como elemento que tiende a proteger y respetar la privacidad, el derecho a la imagen protege la imagen física, la captación o reproducción de sus rasgos o características externas de forma indebida o sin su consentimiento, no incluyendo por ello la imagen pública profesional. (ATC 300/1989, FJ 2).*

Este derecho, en sentido estricto y conforme a la STC 99/1994, consiste en el «derecho de impedir que otros la capten o la difundan», y en «evitar la difusión incondicionada de su aspecto físico, que constituye el primer elemento configurador de su intimidad y de su esfera personal, en cuanto instrumento básico de identificación y proyección exterior y factor imprescindible para su propio reconocimiento como individuo»[184]. En conclusión, el derecho a la propia imagen constituye un derecho autónomo que comparte con el derecho a la intimidad una función, la de salvaguardar la esfera individual frente a intromisiones ajenas. Ambos derechos, junto con el resto de los del Artículo 18 CE, se ordenan a la salvaguarda de un bien jurídico superior que los comprende a todos: la vida privada[185].

En realidad hay que abordar la vida privada desde un enfoque informacional. En el plano del derecho a la propia imagen es donde más se aprecia esta característica y resulta prácticamente obligatorio distinguir entre la captación, la reproducción y la publicación de una imagen sin consentimiento y la información que esta imagen aporta[186]. En este sentido, debe subrayarse que una de las principales fuentes de información para la especie humana es la visual y las modernas técnicas de videovigilancia[187] permiten, al menos teóricamente, establecer perfiles de personalidad de un sujeto mediante el control de conductas más o menos conscientes que se repiten en el tiempo[188].

El domicilio: un ámbito de intimidad

El Tribunal Constitucional ha incardinado la protección del domicilio en el marco de la tutela de la vida privada. En la STC 22/1984 definía la protección constitucional de la morada en los siguientes términos:

> *La protección constitucional del domicilio es una protección de carácter instrumental, que defiende los ámbitos en que se desarrolla la vida privada de la persona. Por ello existe un*

184. Véase adicionalmente STC 117/1994 sobre difusión de imágenes de una actriz en virtud de un contrato con una revista.

185. Véase la STC 170/1987.

186. La difusión de la imagen de una persona conocida tomada en una situación poco conveniente no solo lesiona su derecho a la propia imagen, puede constituir una intrusión en su derecho a la intimidad cuando revele aspectos de su vida privada. Sobre esta materia Concepción Rodríguez, José Luís. Honor, intimidad e imagen. Un análisis jurisprudencial de la LO. 1/1982. Bosch, Barcelona, 1996.

187. En España el Tribunal Constitucional ha tenido oportunidad de pronunciarse respecto del uso de videovigilancia por la policía. La STC 37/1998 (Caso Ertzainza) consideró que una filmación policial «entrañó una disuasión u obstaculización del libre ejercicio del derecho de huelga, reduciendo su efectividad» debido a «los efectos disuasorios que puede producir en el ánimo de quienes pacíficamente forman parte de un piquete informativo el hecho de ser ininterrumpidamente filmados, sin mediar explicación alguna de este proceder». Posteriormente en la STC 98/2000 consideró discriminatoria la grabación de sonidos, además de imágenes, por el Casino de la Toja en un supuesto de videovigilancia privada.

188. Peter Yost en Science of Surveillance (National Geographic) presenta un escenario de videovigilancia total que se ajustaría bastante a esta realidad. Véase, Lyon David. Surveillance Society: Monitoring Everyday Life (Issues in Society). Open University Press, Buckingham, Philadelfia 2001, Stanley, Jay y Steinhardt, Barry. Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society. American Civil Liberties Union-ACLU. Technology and Liberty Program, 2003, y Martínez Martínez, Ricard. «Los ficheros de datos y archivos de imágenes policiales en la legislación italiana. Análisis de las resoluciones dictadas por el Garante Italiano para la protección de los datos personales» en Revista Española de Derecho Constitucional núm. 60, septiembre-diciembre de 2000.

> *nexo de unión indisoluble entre la norma que prohíbe la entrada y el registro de un domicilio (Artículo 18.2 de la Constitución) y la que impone la defensa y garantía del ámbito de privacidad (Artículo 18.1 Constitución). Todo ello obliga a mantener, por lo menos prima facie, un concepto constitucional de domicilio de mayor amplitud que el concepto jurídico privado o jurídico-administrativo. (FJ núm. 2).*

Además de fijar los perfiles de la inviolabilidad del domicilio, el Tribunal Constitucional define con precisión el ámbito de la vida privada[189] en un pronunciamiento que se ha convertido en un clásico de nuestra jurisprudencia constitucional:

> *El Artículo 18.2 de la Constitución contiene dos reglas distintas: una de carácter genérico o principal, mientras la otra supone una aplicación concreta de la primera, y su contenido es por ello más reducido. La regla primera define la inviolabilidad del domicilio, que constituye un auténtico derecho fundamental de la persona, establecido, según hemos dicho, para garantizar el ámbito de privacidad de esta, dentro del espacio limitado que la propia persona elige y que tiene que caracterizarse precisamente por quedar exento o inmune a las invasiones o agresiones exteriores, de otras personas o de la autoridad pública. Como se ha dicho acertadamente, el domicilio inviolable es un espacio en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima. Por ello, a través de este derecho no solo es objeto de protección el espacio físico en sí mismo considerado, sino lo que en él hay de emanación de la persona y de esfera privada de ella. Interpretada en este sentido la regla de la inviolabilidad del domicilio es de contenido amplio e impone una extensa serie de garantías y de facultades, en las que se comprenden las de vedar toda clase de invasiones incluidas las que puedan realizarse sin penetración directa por medio de aparatos mecánicos, electrónicos u otros análogos.*
>
> *La regla segunda establece un doble condicionamiento a la entrada y al registro, que consiste en el consentimiento del titular o en la resolución judicial.[190] (FJ núm. 5)*

Esta sentencia posee el valor añadido de su modernidad ya que, al igual que la jurisprudencia norteamericana[191], evita los pro-

189. Respecto de la vinculación tradicional de la inviolabilidad del domicilio con la libertad personal véase García morillo, J. El derecho a la libertad personal. Ed. Tirant lo Blanch, col. propuestas, Valencia 1995. Posteriormente este derecho fundamental ha evolucionado situándose en la órbita de la vida privada. Véase Espín Templado, E. «Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio», en Revista del centro de Estudios Constitucionales, nº 8. Enero-abril 1991 y González-Trevijano, P. J. La inviolabilidad del domicilio. Ed. Tecnos, Madrid, 1992.

190. En el mismo sentido, véanse los fundamentos jurídicos quinto de la STC 50/1995 y la STC 133/1995.

191. Véase Kyllo v. United States, 533 U.S., 27 (2001).

blemas derivados de la exigencia de una entrada física, de modo que la intrusión virtual por medios electrónicos vulnera el bien jurídico protegido por el Artículo 18.2 CE. En cuanto a su titularidad, se reconoce a las personas físicas y desde la STC 137/1985, a las jurídicas cuando:

> *La persona jurídica venga a colocarse en el lugar del sujeto privado comprendido dentro del área de la tutela constitucional, y todas las hipótesis en que la instrumentación del derecho a la libertad no aparezcan o sean incompatibles con la naturaleza y la especialidad de fines del ente colectivo. (FJ 3).*

Por último, debe subrayarse que el Tribunal Constitucional ha mantenido una postura abierta e integradora respecto de la inviolabilidad del domicilio. Junto con un concepto estricto de domicilio, ha atendido también la realidad funcional de los espacios habitados[192] y la naturaleza de las intromisiones perpetradas con medios tecnológicos en una concepción que integra el Artículo 18 CE como un todo ordenado a tutelar la privacidad como soporte en el que el individuo desarrolla su personalidad[193].

El secreto de las comunicaciones

El Tribunal Constitucional definió sus notas características en el fundamento jurídico séptimo de la STC 114/1984. En primer lugar, el derecho «consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto», de ahí que se vulnere con «la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas». Así «el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje –con conocimiento o no del mismo– o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado».

Además, «el concepto de «secreto», que aparece en el Artículo 18.3, no cubre solo el contenido de la comunicación, sino también otros aspectos como la identidad subjetiva de los interlocutores e incluso el *comptage* que «permite registrar cuáles hayan sido los números telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma». Se trata de garantizar la comunicación, asegurar «su impenetrabilidad por terceros ajenos a la comunicación misma».

El secreto del Artículo 18.3 CE tiene un carácter «formal», «se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado», opera mediante «la presunción *iuris et de iure* de que lo comunicado es »secreto", en un sentido sustancial». No obstante, el secreto de las comunicaciones no se proyecta sobre los interlocutores sobre los cuales puede pesar la obligación de no revelar lo comunicado vulnerando el derecho a la intimidad.

Otro detalle relevante de la doctrina del Tribunal es que al tutelar el secreto de las comunicaciones no se prejuzga el concreto medio

192. La noción de domicilio la resume el Tribunal Constitucional de modo integral en el fundamento jurídico séptimo de la sentencia 10/2002 «7. (...) el rasgo esencial que defi ne el domicilio a los efectos de la protección dispensada por el art. 18.2 CE reside en la aptitud para desarrollar en él vida privada y en su destino específi co a tal desarrollo aunque sea eventual. Ello signifi ca, en primer término, que su destino o uso constituye el elemento esencial para la delimitación de los espacios constitucionalmente protegidos, de modo que, en principio, son irrelevantes su ubicación, su confi guración física, su carácter mueble o inmueble, la existencia o tipo de título jurídico que habilite su uso, o, finalmente, la intensidad y periodicidad con la que se desarrolle la vida privada en el mismo. (...)».

193. Véase la STC 119/2001 sobre perjuicios derivados para la paz doméstica del demandante como consecuencia de los ruidos generados por la actividad de una discoteca.

tecnológico empleado[194]. El Tribunal Constitucional ha situado el secreto de las comunicaciones en el contexto de la protección de la vida privada y con apertura hacia la evolución tecnológica.

El derecho a la protección de datos personales

En su aproximación a la privacidad el Alto Tribunal ha venido manifestando una clara disposición de atender a su dimensión informacional. Esto se manifiesta con toda claridad en el tratamiento de los datos de carácter personal. En esta materia el primer caso relevante es la STC 254/1993[195]. En ella, el Tribunal oscila entre la afirmación de un nuevo derecho fundamental, el derecho a la libertad informática, o una interpretación evolutiva del derecho a la intimidad[196]. En la práctica el Tribunal Constitucional flirteó con la idea de la autodeterminación informativa, como derecho de control sobre los datos personales, pero finalmente fundamentó su planteamiento en el derecho a la intimidad, atribuyendo a la protección de datos personales la condición de garantía constitucional y afirmando simultáneamente que encarna un derecho fundamental «frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos».

Aunque posteriormente en la STC 143/1994 el Tribunal Constitucional reitera su doctrina sobre el derecho a la intimidad, a partir de la STC 11/1998[197] y finalmente con la STC 292/2000 se consolida la creación jurisprudencial del derecho fundamental a la protección de datos o autodeterminación informativa. El fundamento jurídico quinto de la sentencia afirma que el Artículo 18.4 CE incorpora un nuevo derecho fundamental dotándolo de plena autonomía respecto del derecho a la intimidad:

> *La llamada libertad informática es así derecho a controlar el uso de los mismos datos insertos en un programa informático* (habeas data) *y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4).*

194. Véanse las SSTC STC 81/1998, 70/2002 y 123/2002. En Europa ha generado polémica la conservación de datos de tráfico regulada por la Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas. En España la traspuso la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Esta permite que, con autorización judicial «agentes facultados accedan a datos de tráfico retenidos por un período de doce meses por los operadores como por ejemplo la geolocalización de los terminales móviles. Véase Domínguez Peco, E. (coord.). La protección de datos en la cooperación policial y judicial. Agencia Española de Protección de Datos & Thomson Aranzadi, Pamplona, 2008. En Alemania la trasposición ha sido declarada inconstitucional por la STCFA sobre los artículos 113. a y b de la Ley de telecomunicaciones (Telekommunikationsgesetz) y el artículo 100.g) del Código Penal (Strafprozessordnung). Véase http://bit.ly/trzggS.

195. Véase Lucas Murillo de la Cueva, P. «La construcción del derecho a la autodeterminación informativa» en Revista de Estudios Políticos, Nueva Época, núm. 104, abril-junio 1999. Lucas Murillo de la Cueva, P. «La primera jurisprudencia sobre el derecho a la autodeterminación informativa», en Datos Personales, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, núm. 1, marzo de 2003. Disponible en www.datospersonales.org/.

196. Véase Grimalt Servera, P. «El derecho a controlar los datos personales: algunas consideraciones jurídico-constitucionales» en VV.AA. X años de Encuentros sobre Informática y Derecho, Aranzadi, Pamplona, 1997, pp. 151-172. Lucas Murillo de la Cueva, P. «Las vicisitudes del Derecho de la protección de datos personales», en Revista Vasca de Administración Pública, núm. 58, septiembre-diciembre de 2000. Ortí Vallejo, A. «El nuevo derecho fundamental a la libertad informática (a propósito de la STC 254/1993, de 20 de julio)», en Derecho Privado y Constitución, núm. 2, 1994, pág. 328 y Rebollo Delgado, L. El derecho fundamental a la intimidad. Dykinson, Madrid, 2000, págs. 190-191.

197. Caso Uso indebido de datos sobre afiliación sindical. El supuesto recogido en la sentencia en tanto que afectaba a un colectivo de trabajadores ha generado un conjunto de sentencias coincidentes. SSTC 33/1998 y 35/1998, 45/1998, 60/1998, 77/1998, 94/1998, 104/1998, 105/1998, 106/1998, 123/1998, 124/1998, 126/1998, 158/1998, 198/1998, 223/1998, 30/1999, 44/1999 y 45/1999.

> *Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del Artículo 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 Artículo 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (Artículo 81.1 CE), bien regulando su ejercicio (Artículo 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.*

El Tribunal cierra su argumentación en el fundamento jurídico sexto de la sentencia en el que se define objeto de protección del nuevo derecho que alcanza:

> *a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el Artículo 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.*

Por tanto, se crea un derecho cuyo contenido incluye 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. En definitiva, el poder de disposición sobre los datos personales.

3.7.2 Retos actuales para la vida privada. La evolución del derecho fundamental a la protección de datos en el ordenamiento español

En el último decenio la protección de la vida privada en España se ha caracterizado por un marcado protagonismo del derecho a la protección de datos y una fuerte presencia social de la Agencia Española de Protección de Datos. Este derecho se ha situado de hecho en la primera línea de defensa de la privacidad. Por otra parte, debe subrayarse que España se si-

túa de modo ineludible en el territorio que definen el Convenio nº. 108 del Consejo de Europa, la Directiva 95/46/CE y la Carta Europea de Derechos Fundamentales. Por ello, no puede entenderse el posicionamiento de las autoridades españolas en este campo sino en el contexto de la Jurisprudencia del Tribunal Europeo de Derechos Humanos, el Tribunal de Justicia de la Unión Europea y el Grupo de Trabajo del Artículo 29.

Se trata de un contexto normativo caracterizado por una tutela del derecho fundamental a la protección de datos basada en desarrollos normativos que regulan lo que se ha denominado como mercado de la *privacy*[198] imponiendo prestaciones positivas y garantías a todos los operadores. A ello se une en el caso español un aparato sancionador disuasorio de gran complejidad normativa. Aunque el abanico de cuestiones novedosas que ha planteado este derecho resulta particularmente amplio son destacables los aspectos relacionados con el tratamiento de datos personales de menores, las redes sociales y el derecho al olvido.

Menores

La protección de la privacidad de los menores adquiere una especial relevancia ya que presentan perfiles diversos. El menor es simultáneamente estudiante, «controlado por sus padres», mediante el uso de dispositivos de geolocalización en sus teléfonos móviles, consumidor y destinatario de publicidad segmentada por perfiles de edad, internauta y nativo digital. Y todos y cada uno de estos perfiles, en particular el último, es una fuente generadora de preocupación social.

Sin embargo, el tratamiento de los datos del menor no solo plantea riesgos desde la perspectiva del interesado, sino también para la organización que recaba sus datos y debe atenerse al marco regulador definido por el artículo 13 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

> *Artículo 13. Consentimiento para el tratamiento de datos de menores de edad.*
>
> *1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.*
>
> *2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.*
>
> *3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse*

198. Véase Schwartz, P. M. «Internet privacy and the State» en Connecticut Law Review, vol. 32, 2000, pp. 815-859.

en un lenguaje que sea fácilmente comprensible por aquellos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Esta norma persigue tres objetivos: 1) la protección de los menores; 2) definir un escenario de protección del grupo familiar, y 3) fijar procedimientos para cumplir con los deberes en materia de consentimiento, información y verificación de la edad.

La norma dota de seguridad jurídica al sistema. Evita utilizar conceptos jurídicos indeterminados para definir la capacidad de un menor para disponer de sus derechos de la personalidad[199], como el de la madurez, y apuesta por fijar una frontera clara, los catorce años[200], que únicamente se altera cuando por la complejidad del negocio jurídico de que se trate se prevea la tutela del menor.

Sin embargo, resulta complicado cumplir con dos de sus objetivos: informar de modo comprensible y verificar la edad. Mientras que la primera de las obligaciones únicamente requiere un cambio cultural en los redactores de políticas de privacidad, la segunda de ellas se enfrenta a serias barreras. La primera de ellas es sociológica. Según los informes de la Unión Europea[201], el rango medio de edad de la primera conexión a Internet se sitúa en los nueve-diez años. Además, el efecto emulación convierte las redes sociales, en el caso de España Tuenti, en objeto de deseo de estos menores. Si se añade la inexistencia de un método completamente fiable de verificación de edad, las dificultades para el cumplimiento normativo se incrementan.

En principio, los sitios web que no requieren registro pueden permitir el acceso tras una autodeclaración de la edad en la *homepage*, o integrar software de control de contenidos capaz de ser reconocido por un navegador que tenga activados filtros. No es tan sencillo para los que requieren de registro. Parece razonable estratificar la actuación en este ámbito en niveles:

- Disponer de una política informativa que prohíba el registro de menores que no reúnan los requisitos adecuados.
- Articular procedimientos de registro que no contemplen edades inferiores a las permitidas.
- Incluir en las confirmaciones de alta información legal clara respecto de que quien se registra ha entendido las condiciones y declara ser cierta la edad y demás condiciones exigibles.

Sin embargo, el escollo se encuentra en la implementación de metodologías de verificación de edad como: autodeclaración, uso de tarjetas de crédito, uso de identificadores electrónicos, análisis semántico, biometría, identificación física previa... Todas presentan inconvenientes para verificar con certeza la edad del menor, como subrayan los informes de la propia Comisión[202]. En España, el Docu-

199. Véase de Lama Aymá, A. La protección de los derechos de la personalidad del menor de edad. Tirant lo Blanch. Valencia, 2006.

200. Véase Grupo de Trabajo del Artículo 29. Dictamen 2/2009 sobre la protección de los datos personales de los niños (WP 160) y Grupo de Trabajo del Artículo 29. Dictamen 5/2009 sobre las redes sociales en línea (WP 163).

201. Véase EU Kids Online Final Report (2011). Disponible en http://bit.ly/nLEQyV.

202. Véase European Commission. Information Society and Media Directorate-General. Background Report on Cross Media Rating and Classification, and Age Verification Solutions (Safer Internet Forum 25–26 September 2008). Disponible en http://bit.ly/sRuusT.

mento Nacional de Identidad incorpora una firma electrónica inactiva en el caso de menores. Además, no existe ninguna apertura del sistema a validaciones de identidad, ni se atribuye, como en el caso de los universitarios, una cuenta de correo electrónico a estudiantes menores que previa validación LDAP[203] permitiera verificar atributos. Por ello, en ausencia de un tercero de confianza, las exigencias de las autoridades de protección de datos o de la Comisión resultan de difícil satisfacción. En la verificación del cumplimiento por las redes sociales del Principio Segundo, de los *Safer Social Networking Principles for the EU*, relativo al trabajo para asegurar que los servicios son apropiados para la edad de los destinatarios[204], resulta que solo hay dos casos de cumplimiento muy satisfactorio en la implementación de medidas. Pero ¿qué ocurre si se intenta verificar su eficacia? En la práctica, hay que confiar en la sinceridad del menor y en las técnicas de control interno de los proveedores.

> *Researchers were instructed to create a profile of a 9-year old by providing the child's «real» date of birth at registration. The results of this test showed that 9 of the 11 SNS intended to be age-restricted effectively do not allow sign-up by underage users if they provide their real age. 2 of the intended age-restricted services immediately allowed underage users to register on their services after this first attempt. In the 3 other services which are not age-restricted this is not applicable. Self-declaration of age was, thus, the most common mechanism employed by service providers in order to verify a user's age.*
>
> *9 of the 11 SNS that are age-restricted state in their self-declaration that they employ some mechanism to delete underage users from their websites such as analysis of friends' connections to identify suspicious underage users, user-generated reports, etc. 2 SNSs do not explicitly state in their self-declaration what mechanisms they employ to delete underage users from their services. Within the SNS that are age-restricted the most common age verification mechanism is self-declaration of age[205].*

Ello posee relevancia en un caso como el español, en el que con motivo de un error en la verificación de edad se impuso una multa de 150.000 euros[206]. Por ello, va a ser determinante la capacidad de las organizaciones para desplegar estrategias que acrediten diligencia de modo que sea el menor quien rebase las barreras que se le impongan en el registro falseando su identidad. Así, la demostración de diligencia debería suponer la exclusión de la culpabilidad[207]. Para ello puede ser muy conveniente tener en cuenta la Children's Online Privacy Protection Act norteamericana. Al margen de diferencias como

203. Lightweight Directory Access Protocol (en español Protocolo Ligero de Acceso a Directorios).
204. Véase Implementation of the Safer Social Networking Principles for the EU, disponible en http://bit.ly/jFfESQ.
205. Véase Implementation of the Safer Social Networking Principles for the EU, disponible en http://bit.ly/jFfESQ.
206. Procedimiento Nº PS/00281/2007, (disponible en http://bit.ly/uRYhXG), confirmada por la Sentencia de 26 de noviembre de 2009, de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.
207. Este criterio de exclusión basado en la prueba de la diligencia ha sido aplicado en otro supuesto, por ejemplo por la Sentencia de 10 de febrero de 2011, de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.

la edad mínima para consentir, resulta de interés la metodología denominada *sliding scale mechanism*[208]. En ella las exigencias en la verificación de la edad varían desde el envío de un mensaje de correo electrónico con datos adicionales de comprobación, al uso de impresos o verificaciones de identidad más complejas. Este método en el que se suman pasos adicionales de comprobación o confirmación, parece funcional al estado actual de la tecnología. No obstante, en un futuro debe ser sustituido por mecanismos basados en identificadores electrónicos de los menores o de los padres. En este sentido, cualquier tipo de interoperabilidad con registros públicos, como aquellos que certifican aspectos como el nacimiento o las relaciones de filiación, debería conducir a soluciones confiables.

Protección de datos en las redes sociales.

El desarrollo de las redes sociales ha multiplicado de modo significativo el volumen de tratamientos de datos. Primero, porque potencian nuevas comunidades *online*[209] en las que la interacción y la identidad[210] constituyen un elemento nuclear. Por otra parte, el número de agentes implicados se multiplica. Junto al proveedor del servicio existen terceros proveedores de aplicaciones[211], y los propios usuarios que pueden ser a la vez *betatesters* y desarrolladores. Ello obliga a identificar los principios normativos aplicables[212] y tenerlos en cuenta desde el diseño inicial de las aplicaciones[213].

En Europa la sentencia del Tribunal de Justicia de la Unión Europea en el caso Bodil Lindqvist constituye una referencia necesaria para establecer criterio al aplicar las normas sobre protección de datos en las redes sociales[214]. El Tribunal concluyó que se daban las condiciones para aplicar la Directiva 95/46/CE y existía tratamiento al

> *27. (...) hacer referencia, en una página web, a diversas personas y en identificarlas por su*

208. Véase, COPPA Rulemaking and Rule Reviews, disponible en http://bit.ly/t422Dx y Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule. En Federal Register / Vol. 67, No. 74 / Wednesday, April 17, 2002 / Rules and Regulations. Disponible en http://1.usa.gov/uh07BJ.
209. Véase Castells, M. La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad. Areté, Barcelona, 2001, p. 139.
210. Véase Alamillo Domingo, I. «La identidad electrónica en la red», en Rallo Lombarte, A y Martínez Martínez R (coord.). Derecho y redes sociales. op. cit. pp. 37-53.
211. Véase Denham E.Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act. July 16, 2009. Office of the Privacy Commissioner of canada. PIPEDA Case Summary #2009-008. En http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm (Disp. 16/04/2010), pp. 38 y 94.
212. Frente a quienes vienen afirmando la imposibilidad de acotar jurídicamente el fenómeno de Internet, se afirma la necesidad de aplicar en lo que proceda el derecho preexistente. Véase Martínez Martínez R. «Protección de datos y redes sociales: un cambio de paradigma», en Rallo Lombarte, A y Martínez Martínez R (coord.). Derecho y redes sociales. Civitas, Cizur Menor, 2010, pp. 83-116.
213. Como ha señalado Lessig, el programador tiene la capacidad de definir reglas de funcionamiento del entorno que actúan de modo materialmente normativo y, por tanto, la posibilidad de definir modos de funcionamiento que garanticen el cumplimiento de los principios que el Ordenamiento Jurídico incorpora. Véase Lessig, L. El código y otras leyes del ciberespacio. Taurus, Madrid, 2001 y Lessig, L. Code version 2.0. Basic Books. Perseus Books Group. New York, 2006. Disponible en http://bit.ly/191xCG. ICO. Privacy Impact Assessment (PIA) handbook (Version 2). 2009, Disponible en http://bit.ly/A2cga. Homeland Security (EE.UU) Privacy Impact Assessment EINSTEIN Program. Disponible en http://1.usa.gov/sJIVLU. Treasury Board of Canada Secretariat. Privacy Impact Assessment - Policies and Publications. Disponible en http://bit.ly/mL9PPF. Privacy by Design (http://www.privacybydesign.ca/) y Warren, A. «Privacy Impact Assessments: the UK experience» en 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Madrid, 4-6 de noviembre de 2009. Disponible en http://bit.ly/vaAnLV.
214. La Sra. Lindqvist era una catequista sueca que, a finales de 1998, creó con su ordenador personal varias páginas web relacionadas con los feligreses de su parroquia. En uno de sus contenidos señaló que una de sus compañeras se había lesionado un pie y que se encontraba en situación de baja parcial por enfermedad. Tras ser sancionada por este tratamiento de datos personales y recurrir, un tribunal sueco consultó al Tribunal de Justicia sobre las condiciones de aplicación de la Directiva 95/46/CE. Véase Sentencia del Tribunal de Justicia de 6 de noviembre de 2003 en el asunto C-101/01.

nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un »tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46/CE.

No resultando aplicable la excepción de vida privada[215] siendo «este el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas».

Analógicamente, publicar una opinión en un «muro» o etiquetar una fotografía supone un tratamiento sujeto a la Directiva. Así lo confirma el Grupo de Trabajo del Artículo 29, en el Dictamen 5/2009[216]. El Grupo establece las condiciones de aplicación de la Directiva 95/46/CE, partiendo de considerar que en «sentido jurídico, las redes sociales son servicios de la sociedad de la información». Es evidente que para el funcionamiento de este tipo de servicios resulta necesario tratar datos personales. Por otra parte, el objetivo y los servicios de una red social facilitan tratamientos a los propios usuarios.

Así, no existe duda respecto de la aplicabilidad de la Directiva a los proveedores incluso aunque su sede se encuentre fuera del Espacio Económico Europeo[217]. Además se aplicará a proveedores externos de aplicaciones cuando traten datos y también a usuarios bajo ciertas condiciones:

- Cuando la red social se utiliza como una plataforma de colaboración para una asociación o una empresa.
- Cuando todos los miembros de la Red pueden acceder a un perfil o cuando los datos son indexables por los motores de búsqueda o cuando un usuario decide conscientemente ampliar el acceso más allá de los «amigos» elegidos.
- Por último se plantea no aplicar la excepción doméstica cuando se traten datos de terceros sin su conocimiento o consentimiento, particularmente cuando se trate de datos especialmente protegidos.

Esta posición es compartida por la Agencia Española de Protección de Datos y así se manifiesta en los distintos estudios[218], informes[219], guías[220] y resoluciones publicadas. La Agencia ha tramitado procedimientos sancionadores[221] o tutelas de derechos que afectan a servicios propios de la Web 2.0. En la práctica, se aplican los criterios de Lindqvist y del Grupo apostando por priorizar el ejercicio de derechos de cancelación como método para la resolución de conflictos y re-

215. Las normas de protección de datos personales no se aplican a los tratamientos realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

216. Véase Grupo de Trabajo del Artículo 29. Dictamen 5/2009 sobre las redes sociales en línea. (WP 163). Disponible en http://bit.ly/uwi75f.

217. El Grupo ha señalado que existen tratamientos que no podrían realizarse sin recurrir al uso del propio ordenador del usuario, generalmente mediante la explotación de cookies, con lo que se estarían utilizando medios en territorio europeo. Véase Grupo de Trabajo del Artículo 29. Dictamen 1/2008 sobre asuntos relativos a la protección de datos vinculados a las herramientas de búsqueda (WP148). Disponible en http://bit.ly/fRbSqe.

218. Agencia Española de Protección de Datos. INTECO. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales *online*. Madrid, 2009.

219. En el informe 615/2008, relativo a algo tan común como «la actuación de unos particulares que comparten, utilizando para ello sus páginas web, fotos de sus hijos realizando actividades extraescolares» considera aplicable la legislación sobre protección de datos personales al tratarse de páginas publicadas en abierto. Disponible en http://bit.ly/uMHqMc.

220. Véanse las Recomendaciones a usuarios Internet en su edición de 2009. Disponibles en http://bit.ly/tTgiwo.

221. A título de ejemplo véanse las resoluciones E/03486/2009, A/00275/2011, PS/00137/2011, y TD/01239/2010. Disponibles en http://bit.ly/uwgDP4.

servando el aparato sancionador para los supuestos más graves[222].

El derecho al olvido

Podría definirse el derecho al olvido como la facultad de obtener la eliminación de una determinada información de Internet. En el caso español, el debate en torno a esta nueva figura se ha planteado a partir de distintos conflictos.

- La publicación en boletines oficiales de actos administrativos. Si bien el principio de publicidad rige ciertas actuaciones administrativas, su permanencia puede producir efectos no deseables falseando la realidad presente o desprestigiando de por vida a una persona.
- Los medios de comunicación publican noticias de interés público necesarias, para la formación de la opinión pública libre en una sociedad democrática, en palabras del Tribunal Europeo de Derechos Humanos, pero pueden acabar presentando una imagen falsa de las personas a las que afectan[223] o incluir contenidos desproporcionados o incompletos.
- Los usuarios, lejos de asumir responsabilidad en el control sobre su información, la diseminan en una especie de autobiografía permanente en las redes sociales[224].

Cierran el círculo los buscadores que contribuyen a sistematizar la información disponible, aunque desempeñan un papel neutral y no pueden responder por los contenidos de terceros. Así, si la información no es eliminada en origen ofrecerán una biografía digital que no tiene porqué corresponderse en absoluto con la realidad concreta y actual del individuo afectado[225].

Para abordar la cuestión, resulta necesario recordar que los derechos expresan necesidades humanas que la sociedad entiende como básicas. En la actualidad se puede constatar la dificultad de dar cuerpo al derecho al olvido, pero a medida que la exclusión social basada en la obtención de información en Internet crezca[226], con ella aumentará su reivindicación. Por otra parte, el Derecho posee una cierta elasticidad que le permite adaptarse y esta capacidad, lejos de ser un problema, puede ser una herramienta esencial para garantizar los derechos del individuo[227]. Por ello, corresponde a la tecnolo-

---

222. «Es cierto que la realidad de Internet requiere realizar una interpretación del principio de consentimiento que evite una aplicación estricta que la paralizaría o la convertiría en una red profusa en vulneraciones de datos personales de millones de personas accesibles fácilmente usando un mero buscador y de los que no cabe aportar el consentimiento previo. De ahí que no sea conveniente realizar una interpretación maximalista del requerimiento de consentimiento, sino que debe considerarse el principio según el cual cuando el ordenamiento jurídico ofrece varias soluciones sea más adecuado el agotamiento de otras fórmulas alternativas en el caso de que sea posible, razón por la que el uso del derecho de cancelación de datos tendente al cese del tratamiento de datos personales deba priorizarse. Se trataría de un procedimiento que posibilita la corrección con celeridad del dato incluido con objeto reparador con carácter previo a una tutela por incumplimiento o a la incoación, en su caso, de un procedimiento sancionador, que reviste naturaleza punitiva si no se hiciera desaparecer. Esta premisa no debe obstar para que en determinados supuestos –datos especialmente sensibles o derechos afectados de especial gravedad, así como vulneración del secreto profesional– quepa utilizar el procedimiento sancionador al objeto de sancionar una conducta especialmente grave no amparable en las reglas de Internet como ocurre en el caso denunciado.» Véase PS/00508/2008. Disponible en http://bit.ly/uwgDP4.
223. De algún modo esta situación podría corresponder al Tort de «False Light in the Public eye» norteamericano.
224. Véase Sibilia P. La intimidad como espectáculo. Fondo de Cultura Económica, Buenos Aires, 2008.
225. Véase Kieron O'Hara, Mischa M. Tuffield & Nigel Shadbolt. «Lifelogging: Privacy and Empowerment with Memories for Life», en Identity in the Information Society, Volume 1, Number 1 / diciembre de 2008, Disponible en http://bit.ly/uJ6AdY .
226. Véase la descripción sobre la página Drunken Pirate en Mayer-Schönberger, V. Delete. The Virtue of Forgetting in the Digital Age. Princeton University Press. New Jersey, 2009.
227. En este sentido el Art. 3.1 del Código Civil Español señala que «Las normas se interpretarán según el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas». Y esta elasticidad puede rastrearse en todos los ordenamientos baste con recordar la evolución norteamericana del Right to privacy, desde Warren y Brandeis, de la mano del Tribunal Supremo, o la capacidad del Tribunal Europeo de Derechos Humanos para situar bajo el paraguas de la privacidad no solo la intimidad, el secreto de las comunicaciones, la inviolabilidad del domicilio y el derecho a la protección de datos, sino también el reconocimiento de la identidad de los transexuales, el derecho a un medio ambiente doméstico sano, la protección de la vivienda frente a la acción punitiva del estado o del modo de vida nómada de los gitanos ingleses.

gía respetar el Derecho ya que regula relaciones sociales, no cada nuevo ingenio concreto.

Se ha dicho que todo lo que ocurre en Internet pertenece a una historia que se genera en tiempo real y que los hechos «históricos» no pueden ser borrados. Sin embargo, en una sociedad democrática, historicidad y relevancia histórica no son exactamente lo mismo.

El único auxilio jurídico disponible en estos momentos es el de las facultades y principios que encarnan el derecho fundamental a la protección de datos y desde el punto de vista del afectado los derechos de cancelación y oposición constituyen elementos funcionalmente útiles. La Agencia Española de Protección de Datos en multitud de casos está estimando el ejercicio de estos derechos frente a buscadores, que están siendo objeto de recurso ante los tribunales[228]. Así pues, se dispone de herramientas jurídicas aplicables pero que comportan costes a veces difícilmente asumibles para entornos en cuyo diseño no se ha tenido en cuenta el problema de la privacidad.

El derecho al olvido plantea enormes retos y dificultades, pero con él no está en juego el derecho de un solo individuo sino el de toda la comunidad. Una sociedad sin memoria está condenada al fracaso, pero una sociedad que recuerde todos y cada uno de nuestros hechos, por insignificantes que sean, que tenga en cuenta cada información disponible, y que nos juzgue por ella, por nuestra estupidez, por el menor de nuestros errores, es una sociedad condenada a la intolerancia, a la exclusión y a la discriminación.

228. Véase, por ejemplo, el Procedimiento Nº: TD/01257/2010.

Jorge Pérez Martínez

Doctor ingeniero de Telecomunicación por la Universidad Politécnica de Madrid y licenciado en Ciencias Políticas y Sociología por la Universidad Complutense. Es catedrático de la ETSI de Telecomunicación de la UPM desde 1990, donde imparte docencia e investigación en materias relacionadas con los aspectos socioeconómicos de las tecnologías de la información y las comunicaciones, y política y regulación de las telecomunicaciones. De junio de 1990 a febrero de 1999 fue decano del Colegio Oficial de Ingenieros de Telecomunicación. En la actualidad es miembro de su Consejo de Colegio. De septiembre de 2003 a junio de 2004 fue director general para el desarrollo de la Sociedad de la Información en el Ministerio de Ciencia y Tecnología y consejero de los Consejos de Administración del CDTI y de la Entidad Pública Empresarial RED.ES. Actualmente es director de la Cátedra Red.es en la Universidad Politécnica de Madrid, donde coordina el Grupo de Análisis y Prospectiva del sector de las Telecomunicaciones (GAPTEL). Es asesor del secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Energía y Turismo, y coordinador del Grupo de Alto Nivel de la Agenda Digital para España. Es, asimismo, coordinador del Foro de Gobernanza de Internet en España (IGF España).

Arturo Vergara Pardillo

Doctor ingeniero de Telecomunicación por la Universidad Politécnica de Madrid en 2011, ingeniero de Telecomunicación por la UPM en el año 2006 y especialista universitario de Economía de las Telecomunicaciones por la UNED en el año 2008. Desde el año 2007 al año 2011 disfrutó de una beca de Personal Investigador en la UPM para el desarrollo de su tesis doctoral centrada en la problemática del despliegue de las redes de acceso de próxima generación (NGA). Durante su etapa de investigación ha formado parte del equipo de trabajo del *think-tank* GAPTEL (Grupo de Análisis y Prospectiva del sector de las Telecomunicaciones), ha participado en la elaboración de diferentes informes para la Administración pública, así como en la elaboración de diversos libros, artículos y ponencias científico-técnicas. Desde 2012 es consultor para la Cátedra Red.es y se incorpora al equipo de trabajo de la Agenda Digital para España en la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. Asimismo, es miembro del Grupo de Regulación y de Políticas Públicas del Colegio Oficial de Ingenieros de Telecomunicación y del Foro de Gobernanza de Internet en España, donde colabora activamente.

4. El impacto de la regulación sobre los nuevos servicios

Jorge Pérez Martínez
Catedrático de la Universidad Politécnica de Madrid (UPM)

Arturo Vergara Pardillo
Investigador y consultor

4.1 Introducción

El tercer capítulo de este monográfico tiene como objetivo analizar el impacto que la regulación de protección de datos y de privacidad puede tener sobre la prestación de distintos servicios *online* y sobre los modelos de negocio que los sustentan.

El ecosistema de Internet es un entorno muy dinámico que se puede ver afectado por la imposición de regulaciones extremadamente prescriptivas, garantistas o poco flexibles. Conforme el tratamiento de los datos personales se ha ido desplazando hacia posiciones de mayor relevancia para el desarrollo de nuevos servicios –ya sea para obtener ingresos a través de publicidad o para generar servicios más eficientes y competitivos– la regulación asociada a la protección de los datos personales ha pasado de ser un elemento lateral, con el que era necesario cumplir, a ser un factor fundamental que puede limitar el alcance de la actividad desarrollada y puede imponer sobrecostes a esta.

En este sentido, en los siguientes apartados se analiza –sin pretender ser exhaustivo– las problemáticas actuales de privacidad, el impacto de la regulación actual y el posible impacto que la propuesta de Reglamento de la Comisión Europea podría tener sobre algunos de los servicios más relevantes en el actual ecosistema de Internet, entre los que se encuentran los servicios de *cloud computing*, los servicios de publicidad *online* basada en el comportamiento, las redes sociales, o el ecosistema de aplicaciones móviles.

El capítulo se completa con contribuciones de Facebook, Orange, Microsoft, Telecom Italia y Telefónica, en las que presentan su visión sobre la evolución de este debate y el principal impacto que puede tener sobre la forma en la que se prestan hoy en día diferentes servicios en Internet.

4.2 *Cloud computing*

El *cloud computing* se presenta como un elemento transformador de las tecnologías de la

información que permite a ciudadanos, empresas y administraciones un acceso rápido, flexible y escalable a capacidad de almacenamiento y tratamiento de la información.

Los servicios proporcionados suelen ser virtualizados y se asignan según los requisitos de demanda desde una reserva común compartida entre distintos usuarios. Esto permite, en primer lugar, beneficiarse de importantes economías de escala, y en segundo lugar, trasladar esas economías de escala a los precios finales, consiguiendo ofertas flexibles para los usuarios finales, que evitan realizar inversiones iniciales, los costes de mantenimiento y la necesidad de sobredimensionar el sistema pensando en los picos de demanda. Estas ventajas están impulsando que cada vez un mayor número de organizaciones de todo el mundo estén externalizando estos servicios a proveedores de *cloud computing*.

Los servicios de *cloud computing* se suelen clasificar en tres modelos principales: a) infraestructura como servicio (*Infrastructure as a Service* o IaaS), que representa la provisión de recursos de infraestructura física y recursos hardware como capacidad de tratamiento o de almacenamiento; b) plataforma como servicio (*Platform as a Service* o PaaS), que representa la provisión de herramientas para el desarrollo y despliegue de aplicaciones, como por ejemplo aplicaciones móviles, y c), software como servicio (*Software as a Service* o SaaS), que consiste en la provisión de aplicaciones a usuarios finales a través de Internet, como *webmail* o procesadores de texto *online*.

Entre los principales agentes del *cloud computing* destacan gigantes del mundo de Internet, como Amazon[229] o Google[230], compañías como Microsoft[231] o SAP[232] que están impulsando una alternativa *cloud* a los servicios tradicionales basados en software, empresas como Salesforce[233] o Rackspace[234] que centran su negocio principal en la provisión de servicios de *cloud computing*, y otros actores como IBM, Fujistu, AT&T, Telefónica o BT que están incorporando en sus catálogos diferentes ofertas de servicios de *cloud computing*.

De forma paralela a los servicios orientados al entorno empresarial, la posibilidad de ofrecer servicios en movilidad con independencia del dispositivo o la plataforma utilizada ha facilitado el desarrollo de numerosas aplicaciones orientadas al consumidor basadas en la nube, tanto por parte de agentes más tradicionales como Amazon o Apple como por parte de nuevas empresas como Dropbox, Spotify, Netflix o Hulu.

El mercado de *cloud computing* alcanzó en 2011 los 40.700 millones de dólares y dispone, según la consultora Forrester[235], de un potencial de crecimiento hasta los 241.000 millones

229. Amazon es uno de los principales proveedores de servicios IaaS, ofreciendo dentro de su plataforma Amazon Web Services servicios de tratamiento de información y de almacenamiento. Estos servicios se sitúan como una de las líneas prioritarias de la compañía, que ha aumentado la inversión en esta línea de 373 millones de dólares en 2009 a cerca de 979 millones en 2010.
230. A través del servicio Google Apps, ofrece a empresas en forma de servicios SaaS una versión adaptada de los servicios Google Docs, Gmail, Google Calendar, Google Groups, Google Sites y Google Video. Asimismo, en el área de servicios PaaS, Google ofrece un entorno de desarrollo basado en la nube.
231. Los servicios en la nube de Microsoft se presentan en profundidad en la contribución de Brendon Lynch. Asimismo, también ofrece el servicio Azure (PaaS) con el que pretende atraer a nuevos desarrolladores al ofrecer sus centros de datos como plataforma para el desarrollo y la oferta de servicios.
232. La compañía alemana SAP, líder mundial en el ámbito de los sistemas de planificación de recursos empresariales (ERP) también ofrece soluciones SaaS bajo el nombre de Business ByDesign.
233. Salesforce destaca como líder en el sector PaaS con su servicio Force.com que permite el desarrollo de aplicaciones y su publicación en su tienda AppExchange. Asimismo, Salesforce proporciona soluciones SaaS de gestión de relación con el cliente (CRM).
234. Rackspace, fundada en 1998 en EE. UU. como proveedor de servicios de hosting, ha sabido reconvertirse en uno de los principales actores en el área de los servicios IaaS. Ante la falta de estandarización de los servicios IaaS ofrecidos por distintos fabricantes, Rackspace ha lanzado el sistema operativo en la nube OpenStack.
235. Forrester Research, Sizing The Cloud – Understanding and Quantifying the Future of Cloud Computing, (April 2011).

en 2020, donde destacarán los servicios SaaS. Además de este potencial de crecimiento, la industria del *cloud computing* puede generar un impacto social, y sobre el tejido productivo, que ha sido objeto de diversos estudios. Se ha estimado[236] que más de trescientos mil pequeñas y medianas empresas europeas podrán acceder a capacidades avanzadas de tratamiento mediante menores requisitos de inversión e inferiores costes de mantenimiento, permitiendo la creación[237] de hasta un millón de empleos en Europa, y generando una mejora de la competitividad que puede alcanzar los 149.000 millones de dólares en 2014 a nivel mundial, según la consultora Gartner[238].

Para que estas mejoras económicas y sociales puedan materializarse será necesario avanzar hacia un entorno que facilite el desarrollo y la adopción de los servicios *cloud*. En este sentido, la Comisión Europea inició[239], en 2011, el proceso para definir una Estrategia Europea para el *Cloud Computing* que permitiese a Europa superar las incertidumbres, tanto en materia de privacidad y seguridad como en aspectos técnicos y comerciales, para así desarrollar un mercado dinámico de *cloud computing*. Hasta el momento, el desarrollo de esta estrategia ha involucrado la realización de una consulta pública[240], jornadas específicas de trabajo[241], así como distintos encuentros con la industria[242] y ha permitido el establecimiento de la iniciativa *European Cloud Partnership*[243].

4.2.1 Problemáticas de privacidad en el *cloud computing*

La propia naturaleza deslocalizada de los datos, servidores y aplicaciones en un entorno *cloud*, genera incertidumbres relativas a la privacidad y seguridad de los datos personales. Según un informe[244] realizado por el Foro Económico Mundial en 2010 que implicaba a industria, gobiernos y academia, las principales barreras al desarrollo y adopción de servicios *cloud* se agrupan en cuestiones de gobernanza de los datos, seguridad y entorno empresarial.

Por su parte, las respuestas a la consulta pública realizada por la Comisión Europea[245] recogen la incertidumbre generada por el marco regulador en materia de privacidad y protección de datos, señalando como principales barreras al desarrollo de una mayor actividad de *cloud computing* en Europa la falta de claridad del marco regulador, la inseguridad jurídica generada en términos de responsabilidades y obligaciones, y los costes asociados a la adaptación a las distintas implementaciones de las Directivas actuales.

En el ámbito de la Gobernanza de los datos, que se relaciona directamente con las problemáticas de privacidad presentadas en este libro, el Foro Económico Mundial distingue tres problemáticas principales, las generadas por la localización de los datos, las formadas por cuestiones de privacidad y confidencialidad, y las relacionadas con la propiedad y los derechos de los datos en la nube.

---

236. Etro, F. «The Economic Consequences of the Diffusion of Cloud Computing» in The Global Information Technology Report 2009-2010. World Economic Forum (2010).
237. Kroes, N. «Ensuring the Cloud happens with Europe, not to Europe». Speech/12/238. Brussels, 27 March 2012.
238. Gartner, Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2009-2014, (June 2010).
239. Ver Neelie Kroes, «Towards a European Cloud Computing Strategy World Economic Forum Davos», speech 11/50, 27 January 2011. Disponible en: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/50.
240. http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf
241. http://ec.europa.eu/information_society/events/cf/daa11/item-display.cfm?id=5999
242. Ver informes de encuentros con industria, pequeñas y medianas empresas, operadores de telecomunicación y proveedores de servicios de hosting, y con los consumidores. http://ec.europa.eu/information_society/activities/cloudcomputing/library/index_en.htm
243. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/38
243. World Economic Forum, Advancing Cloud Computing: What to do now? Priorities for Industry and Governments (2011), World Economic Forum in partnership with Accenture.
245. Ver http://ec.europa.eu/information_society/activities/cloudcomputing/docs/ccconsultationfinalreport.pdf

Transferencia internacional de datos personales

La primera problemática se refiere a las limitaciones producidas por la localización de los datos en distintas regiones geográficas sometidas a diferentes marcos jurídicos. La resolución de las inconsistencias jurídicas genera incertidumbres entre usuarios, gobiernos y proveedores de servicios *cloud*. Los usuarios manifiestan su preocupación por la capacidad de otros gobiernos de demandar un acceso a sus datos. Por su parte, la preocupación de los gobiernos radica en la pérdida de capacidad de supervisión y de control de los datos en la nube, lo que puede derivar en el establecimiento de condicionantes a la localización de los datos –por ejemplo, obligaciones para que los proveedores de servicios *cloud* almacenen los datos dentro de las fronteras nacionales, o imponer condiciones especiales junto con la necesidad de autorización para la transferencia de datos transfronteriza, elemento fundamental para el desarrollo del *cloud computing*.

En el caso europeo, la transferencia de datos personales fuera de las fronteras está limitada salvo para casos de países que garanticen un nivel de protección adecuado, o en el caso del cumplimiento de cláusulas específicas como es el acuerdo de Puerto Seguro con EE. UU. *(Safe Harbour)*. A diferencia de los grandes actores en este segmento como Amazon, Apple, Google o Microsoft, no es tan claro que actores de menor tamaño como Pro Softnet o Dropbox dispongan de servidores fuera de su mercado natural ni hayan obtenido Acuerdos de Puerto Seguro[246]. La existencia de este tipo de barreras puede limitar el desarrollo de centros de datos en mercados menores, al dificultar la capacidad de alcanzar economías de escala, principal beneficio del *cloud computing*. Esto se percibe por los proveedores de servicios *cloud* como una barrera a la innovación que proporciona a los agentes con mayor tamaño una ventaja competitiva adicional.

Consistencia y armonización de los marcos reguladores

El segundo elemento señalado es la preocupación de los usuarios sobre la privacidad y confidencialidad de sus datos una vez subidos a una plataforma *cloud*. La existencia de legislación específica trata de solventar estas incertidumbres, sin embargo, como se ha puesto de manifiesto a lo largo del libro, surgen problemas de armonización y de consistencia entre los distintos enfoques y legislaciones aplicadas.

En este sentido, algunos de los agentes señalan que para el caso del *cloud computing* la solución a los desafíos de regulación deberá recaer en un mayor uso de mecanismos de mercado y de autorregulación, como la privacidad desde el diseño, la aplicación del principio de responsabilidad o mecanismos de certificación de privacidad que permitan acercar, o hacer más compatibles, los distintos marcos reguladores.

Clarificación de los roles de responsable del tratamiento y encargado del tratamiento

El tercer elemento señalado por el Foro Económico Mundial se refiere al reparto de responsabilidad entre el prestador de los servicios de *cloud* –habitualmente un agente intermediario– y el responsable del tratamiento, que es quien utiliza el servicio *cloud* como parte del tratamiento de los datos personales de los afectados.

El marco europeo solo distingue dos tipos de agentes involucrados en el tratamiento de los datos personales: el «responsable del tratamiento»[247], que es quien determina los fines

246. En el caso de Dropbox, este alcanzó el cumplimiento del acuerdo Safe Harbour con la UE en febrero de 2012 (http://blog.dropbox.com/?p=972). Hasta ese momento no cumplía con los requisitos para realizar transferencias de datos personales entre Europa y EE. UU., lo que forzó a dicha empresa a instalar servidores para prestar servicio en Europa o a limitar su actividad en Europa a usos puramente domésticos (excepción de uso doméstico del Artículo 3 de la Directiva de protección de datos).

247. Conocido también como el «controlador de los datos», derivado de la traducción del término en inglés *data controller*.

y los medios del tratamiento de datos personales; y el «encargado del tratamiento»[248], quien trata datos personales por cuenta del responsable del tratamiento. Ambas categorías de agentes se ven sometidas a obligaciones y responsabilidades distintas marcadas en la Directiva de protección de datos que imponen diferentes limitaciones y costes adicionales. La problemática en este caso se basa en si el agente de *cloud* será considerado como responsable o encargado del tratamiento, caso en el que contraería responsabilidades sobre los datos personales que pueden impedir el desarrollo de sus servicios, máxime cuando en la mayoría de las ocasiones los datos almacenados o procesados en las infraestructuras del operador de *cloud* son transparentes para este sin tener acceso a ellos.

En un informe[249] elaborado por el Foro Digital del CEPS[250], se argumenta que en ocasiones los proveedores de servicios *cloud* no deberían ser considerados responsables, sino meros «auxiliares», ya que son los usuarios de los servicios *cloud*, en este caso los responsables originales del tratamiento, los que mantienen el control sobre los datos personales de los afectados.

Asimismo, a pesar de que habitualmente también se considera a estos proveedores como encargados del tratamiento, en muchas ocasiones solo proporcionan recursos para terceros –por ejemplo, servicios de IaaS o SaaS en los que no conocen el tipo de información o datos procesados–, por lo que deberían ser considerados como intermediarios neutrales, deteniéndose la responsabilidad en aquellos proveedores que tienen control y conocimiento sobre los datos personales[251]. La clarificación entre los diferentes roles posibles y el tipo de regulación impuesta tendrá efectos relevantes sobre la evolución de la industria del *cloud.* Los agentes involucrados señalan que una sobrerregulación en las etapas iniciales de evolución de la industria puede tener un impacto negativo en la innovación y en la capacidad de responder a las necesidades de los usuarios.

Problemáticas de seguridad en el *cloud computing*

La confianza de usuarios y empresas en la seguridad de los servicios *cloud* se sitúa como uno de los elementos principales que frenan la adopción de estos. En este sentido, los temas de seguridad señalados por el Foro Económico Mundial se centran en: a) mejorar la seguridad de los datos combatiendo el acceso no autorizado mediante la mejora de la gestión y verificación de identidades y el uso de encriptación; b) asegurar la integridad y la disponibilidad de los datos, mejorando la resistencia de las infraestructuras y avanzando hacia una mayor transparencia en la gestión de las violaciones de datos, y c) asegurar que los datos son eliminados una vez no son necesarios o cuando los responsables del tratamiento lo consideren oportuno.

La mejora de la seguridad y confianza vendrá necesariamente asociada al desarrollo de un marco legal más claro y apropiado para los casos de *cloud computing.* Por ejemplo, el establecimiento de condiciones de notificación sobre violaciones de datos para todos los agentes.

Asimismo, una parte muy relevante del debate de la seguridad en el ámbito del *cloud computing* está asociada al desarrollo de estándares, códigos voluntarios de conducta o esquemas de certificación. En este sentido, la colaboración entre los distintos organismos de estandarización mundiales y la industria es clave para una rápida mejora de la confianza en los servicios de *cloud computing*.

248. Conocido también como el «procesador de los datos», derivado de la traducción del término en inglés data processor.
249. Renda A. y Guido L. The economics of cloud computing. Working Group 4. CEPS Digital Forum.
250. Centre for European Policy Studies.
251. Argumento planteado en Hon K., et. al., Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law. The Cloud of Unknowing, Part 3 (2011), Legal Studies Research Paper No 84/2011. Queen Mary University of London, School of Law.

Problemáticas de entorno empresarial en el *cloud computing*

Finalmente, cuestiones de interoperabilidad, portabilidad de los datos, niveles de servicios o la falta de madurez del ecosistema *cloud* son algunos de los elementos señalados por el Foro Económico Mundial que generan incertidumbre en el entorno empresarial y que pueden causar una fuerte dependencia de proveedor. Si bien estos elementos exceden el objeto y contenido de este texto, es importante señalar que algunos de ellos son tratados en el mismo marco regulador que otros elementos de privacidad y seguridad. Y que, en cualquier caso, deberán ser considerados en el desarrollo de cualquier medida reguladora o legislativa que tenga como objetivo el impulso al desarrollo de la industria *cloud*, y a la adopción de sus servicios.

4.2.2 Impacto de la revisión del marco regulador europeo

La revisión de la Directiva de protección de datos iniciada por la Comisión Europea supone una gran oportunidad para establecer un entorno que no solo sea amigable para el desarrollo del *cloud computing*, sino que sea proactivo. Las medidas determinadas en este proceso tendrán un impacto directo sobre los costes, las limitaciones y los requisitos de los distintos modelos de negocio de *cloud* que se establezcan o presten servicios en el espacio europeo.

La propuesta actual de la Comisión permitiría resolver algunos de los problemas que el marco actual impone sobre el desarrollo de negocios *cloud*, como es la falta de armonización de la normativa en Europa, lo que incrementa los costes al obligar a una adaptación de los servicios y de los requisitos de privacidad en cada país, o como es el desarrollo de un marco más coherente y equivalente sobre obligaciones de transparencia y notificación ante situaciones de violación de los datos personales, lo que permitirá mejorar la confianza de los usuarios en los servicios *cloud*.

Sin embargo, el Reglamento propuesto mantiene barreras e incertidumbres que tienen un impacto relevante sobre el desarrollo del *cloud computing* en Europa. Atendiendo al análisis realizado por el *Cloud Legal Project*[252] de la Universidad Queen Mary (Londres), la propuesta de la Comisión Europea no resuelve las siguientes problemáticas:

- El ámbito de aplicación del Reglamento hace probable que la mayor parte de los datos en la nube sean considerados datos personales para propósitos de la legislación de datos, haciendo más probable que los proveedores de servicios *cloud* se vean sometidos a cargas innecesarias. Un modelo que valorase los riesgos asociados al uso de los datos junto con la probabilidad de identificación de los sujetos se ajustaría mejor a la naturaleza tecnológica y logística de los modelos de negocio/tecnología *cloud* y a su uso.
- La naturaleza de los proveedores de servicios *cloud* no encaja bien con el modelo de responsable del tratamiento (controlador) y encargado del tratamiento (procesador) empleado en la regulación actual y en la propuesta de la Comisión. Muchos proveedores de servicios *cloud* proporcionan recursos de infraestructura o herramientas que emplean de forma autónoma los usuarios de la nube o plataformas intermedias, que actúan como un intermediario pasivo. Su clasificación como encargados del tratamiento implica un conjunto de car-

252. El Cloud Legal Project (CLP) es una iniciativa de tres años impulsada por el Centre for Commercial Law Studies (CCLS) de la Universidad de Queen Mary para estudiar los aspectos legales y de regulación que generan el cloud computing. Su objetivo principal es reducir la incertidumbre en relación con dichos aspectos legales y de regulación mediante la difusión de estudios académicos. Los estudios realizados pueden encontrarse en: http://www.cloudlegal.ccls.qmul.ac.uk/index.html.

gas y requisitos adicionales que pueden influir negativamente sobre el modelo de negocio de estos agentes, salvo que se introduzca una exención para este tipo de agentes intermediarios.

- En relación con la jurisdicción aplicable, si bien el Reglamento elimina la fijación de la jurisdicción a partir de la localización de los equipamientos –poco apropiado para un entorno en la nube– y utiliza un criterio de oferta de servicios, introduce el concepto de establecimiento principal cuya aplicación práctica es incierta. Esto significa que seguirá existiendo incertidumbre sobre la aplicabilidad o no de la regulación de protección de datos para aquellos casos en los que usuarios externos al Espacio Económico Europeo utilicen un proveedor de servicios *cloud* o un centro de datos dentro del Espacio Económico Europeo.
- La transferencia de datos personales fuera de las fronteras de la UE supone uno de los principales elementos facilitadores para un desarrollo y un uso eficiente de los servicios *cloud*. La propuesta de Reglamento impone como requisito adicional a los ya existentes la necesidad de aprobación por parte de los organismos reguladores correspondientes, creando mayores cargas para aquellas empresas europeas que utilicen servicios *cloud* que involucren la transferencia de datos personales a terceros países.
- Finalmente, se señala que la propuesta de Reglamento no consigue resolver la incertidumbre generada en relación con el concepto de «interés público» en el Artículo 44 referido a las excepciones aceptadas para permitir las transferencias de datos fuera de las fronteras europeas. Asimismo, se señala la necesidad de una mayor clarificación de las transferencias de datos a terceros países en los casos en los que se hayan reclamado datos personales para actividades relacionadas con asegurar el cumplimiento de la ley *(enforcement)*.

Asimismo, la nueva propuesta introduce dos nuevos elementos que pueden tener un impacto negativo en los modelos de negocio del *cloud computing*.

- El primero de ellos es el incremento de la burocracia y de los requisitos de obligado cumplimiento para los encargados del tratamiento (clasificación habitual que recibirán los proveedores de servicios *cloud*), como la realización de evaluaciones de impacto o la obligación de establecer delegados de protección de datos.
- El segundo elemento introducido es la mayor capacidad de las autoridades supervisoras y la necesidad de aprobación previa al tratamiento de datos en determinados contextos, como puede ser en relación con la transferencia de datos a terceros países.

Todos los agentes involucrados en el desarrollo de servicios en la nube han reconocido la importancia del marco regulador de protección de datos en la evolución y el éxito del *cloud computing*. El establecimiento de marcos que generen mayores costes asociados con la regulación o dificultades a la adopción o a un uso flexible podrá mermar la capacidad competitiva de Europa para desarrollar y utilizar eficazmente estos servicios, afectando negativamente al beneficio económico y productivo que el uso de servicios en la nube genera a ciudadanos, empresas –en especial a la pequeña y mediana– y a la propia Administración.

Será importante que el modelo regulador adoptado permita la apertura, interoperabilidad, uso de estándares globales y la protección de los datos en relación con el *cloud computing*. Asimismo, la protección de la privacidad de los usuarios de un modo transparente y equilibrado solo será beneficiosa si permite

generar confianza y alcanzar el equilibrio adecuado entre la defensa de la privacidad individual y unas reglas amigables para el desarrollo de actividades empresariales, de forma que los beneficios del *cloud computing* puedan ser aprovechados por los ciudadanos y empresas europeas. Los proveedores de servicios necesitan unas reglas de juego homogéneas en Europa que les permitan operar con economías de escala para impulsar la innovación y promover la adopción masiva de nuevas aplicaciones y servicios.

4.3 Publicidad *online*

La publicidad *online* se sitúa como una de las principales fuentes de ingresos para un gran número de modelos de negocio asociados a servicios en Internet y como un elemento central y clave para el desarrollo del ecosistema de Internet. La evolución tecnológica y el propio desarrollo de Internet han permitido pasar de los primeros *banners* genéricos a una oferta de publicidad mucho más segmentada, incluyendo entre otros formatos, publicidad en el móvil, publicidad embebida en las propias aplicaciones y publicidad en las búsquedas.

Asimismo, la mayor capacidad de captura y tratamiento de información sobre los usuarios permite una publicidad más orientada a los intereses de los usuarios, o publicidad basada en el comportamiento. Este tipo de publicidad se basa en la observación del comportamiento del individuo durante el tiempo, estudiando las características de sus acciones (patrones de visitas a sitios web, interacciones, palabras clave, producción de contenido, localización, etc.) para elaborar un perfil específico que permita ajustar la publicidad servida a dicho usuario a los intereses identificados.

A diferencia de otros modelos de publicidad, como la contextual[253] o la segmentada[254] que utilizan información estática o parcial del individuo, la publicidad basada en el comportamiento permite proporcionar al anunciante una visión más detallada del usuario y de su «vida *online*». Las principales ventajas de este tipo de publicidad radican en que los individuos reciben una publicidad más útil para sus intereses y que los anunciantes realizan una mejor selección de su audiencia, permitiendo a los sitios web incrementar su valor e ingresos, elementos clave para la sostenibilidad de la inversión en Internet.

Los principales agentes involucrados en la provisión de publicidad son los proveedores de redes publicitarias (del inglés *advertising network providers*, también conocidos como *ad networks*), que conectan a los anunciantes con múltiples páginas web o interfaces (como aplicaciones móviles) que entregan la publicidad a los usuarios finales. Entre estos agentes se pueden encontrar Google AdSense o Yahoo! Advertising solutions. La publicidad mediante *banners* y en sitios web alcanzará los 11.000 millones de dólares en 2011 y se espera que crezca un 20 % CAGR (tasa de crecimiento anual compuesto) hasta 2016, alcanzando los 27.600 millones de dólares. De estas cifras de inversión *online* en EE. UU., eMarketer afirma que Google captura más del 40 %, mientras que Yahoo o Microsoft se limitan a una cuota del mercado estadounidense del 11 y del 6 %, respectivamente[255].

Asimismo, resultan relevantes los agentes basados en la inserción de publicidad en las búsquedas, como Google AdWords, Mi-

253. La publicidad contextual se basa en la actividad actual que está desarrollando el usuario en un momento dado, como pueden ser las búsquedas realizadas o las páginas visitadas en dicha sesión. Este tipo de publicidad se adapta a las acciones del usuario en un único momento y no tiene en cuenta el historial o el perfil del usuario.

254. La publicidad segmentada se basa en un conjunto de características conocidas del usuario como pueden ser la edad, el sexo, la localización, la profesión, etc. proporcionadas por el propio usuario.

255. http://www.emarketer.com/blog/index.php/tag/online-ad-revenues/

crosoft AdCenter o e-Bay Advertising. De acuerdo con Forrester, la inversión en publicidad en buscadores en EE. UU. será de 18.800 millones de dólares en 2011, y se espera que crezca un 12 % CAGR hasta los 33.300 millones en 2016. Por otra parte, el éxito de las redes sociales ha impulsado la inversión en publicidad en ellas hasta alcanzar los 6.000 millones de dólares en 2011, entre las que destaca principalmente Facebook[256] con más de un 67 %.

4.3.1 Problemáticas de privacidad en la publicidad *online*

La relación con la privacidad surge de la utilización de tecnologías de monitorización del comportamiento para la elaboración de perfiles de usuario que permitan personalizar la publicidad entregada. Estas tecnologías se basan habitualmente en el uso de *cookies* de seguimiento, que son instaladas por los *ad networks* en el navegador o equipo de usuario la primera vez que este accede a una página web que proporciona anuncios de dicha red publicitaria. La *cookie* de seguimiento permite al *ad network* reconocer el acceso del usuario a las páginas web enlazadas en su red, y a partir de dicho comportamiento elaborar un perfil de usuario para la provisión personalizada de publicidad.

Los perfiles de usuarios se generan mediante la combinación de perfiles explícitos, creados según los datos proporcionados directamente por los usuarios –por ejemplo, durante el registro en un servicio web–, y perfiles predictivos, que se crean a partir de técnicas de *data mining* de los datos de comportamiento almacenado. Asimismo, en la creación de los perfiles de usuario se utiliza información adicional como puede ser la localización –por ejemplo, la obtenida a partir de la dirección IP, información disponible por la integración de otros servicios web del mismo proveedor o por integración o acuerdos con terceros, o bases de datos de comportamiento adquiridas por el *ad network*.

De esta forma, la prestación de servicios de publicidad basada en el comportamiento genera distintas cuestiones relacionadas con la privacidad y con el tratamiento de los datos personales que pueden afectar a la efectividad de aquella y, consecuentemente, a los modelos de negocio de anunciantes, proveedores de redes publicitarias y a modelos de negocio de servicios *online* que se basan principalmente en la publicidad.

Legislación aplicable

Según un análisis[257] realizado por el Grupo de Trabajo del Artículo 29, el uso de técnicas de monitorización del comportamiento *online* está sujeto tanto al cumplimiento de la Directiva sobre la privacidad y las comunicaciones electrónicas como de la Directiva de protección de datos.

La revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas de 2009 modificó el Artículo 5 de confidencialidad de las comunicaciones en su apartado tercero para requerir el consentimiento informado del usuario como requisito para poder almacenar información o acceder a información previamente almacenada en el terminal del usuario. De esta forma, la instalación de *cookies* o tecnologías similares y el uso posterior para obtener acceso a información sobre el usuario[258] deberá cumplir con dicho Artículo.

Por su parte, en los casos en los que la información capturada mediante este tipo de técnicas permita la identificación del individuo, se considerarán datos personales y, por tanto, los agentes involucrados estarán sujetos a la Di-

256. http://www.socialmediaportal.com/News/2011/01/Social-media-ad-spend-to-hit-6-billion-worldwide-in-2011.aspx
257. Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising (2010).
258. El Artículo 5(3) es de aplicación a cualquier tipo de información, sean o no datos personales.

rectiva de protección de datos. En este sentido, la opinión del GT29 es que la utilización de este tipo de técnicas de monitorización suele involucrar el tratamiento de datos personales, ya sea porque se utiliza la dirección IP de los sujetos, o porque la información obtenida está relacionada con las características de una persona o de su comportamiento.

La inclusión de las *cookies* en el ámbito de aplicación de la Directiva, cuyo plazo para su implementación en la legislación nacional fue mayo de 2011[259], y la posible consideración de los agentes como responsables del tratamiento de los datos, podrá generar implicaciones en el funcionamiento y la efectividad de los modelos de negocio de provisión de publicidad *online*, como se presenta en los siguientes apartados.

Roles y responsabilidades de los distintos agentes involucrados

La aplicación de la Directiva de protección de datos en los casos de publicidad *online* basada en el comportamiento tiene implicaciones en forma de obligaciones y responsabilidades para los diferentes agentes involucrados –las redes de publicidad, los anunciantes y los espacios web que publican los anuncios– que pueden tener un impacto sobre el modelo de negocio de estos.

Si bien en el caso de las redes de publicidad es bastante claro que se ocupa el rol de responsable del tratamiento de los datos (con las obligaciones y responsabilidades asociadas, como son los derechos de acceso, rectificación y borrado de los datos personales), no lo es tanto para anunciantes y sitios web que publican los anuncios.

En relación con los espacios web que publican los anuncios, el GT29 considera que son estos agentes quienes inician la cadena de tratamiento de los datos personales, al redirigir el navegador de los usuarios hacia las redes de publicidad –que almacenan o acceden a la información disponible en el terminal de usuario–. Por tanto, en opinión del GT29, estos agentes tienen cierta responsabilidad en el tratamiento de los datos, que dependerá de la implementación nacional de la Directiva de protección de datos y de las leyes nacionales. Esta responsabilidad no cubierta bajo la figura de responsable o de encargado del tratamiento puede generar incertidumbre en los responsables de los sitios web y reducir su voluntad a incorporar publicidad. En aquellos casos en los que el sitio web no se limite a la redirección, sino que activamente recoja ciertos datos (como la dirección IP, nombre, edad, etcétera.) y los envíe a las redes de publicidad, el sitio web podrá ser considerado responsable conjunto del tratamiento de los datos personales, y verse sometido a las obligaciones y responsabilidades pertinentes.

Por su parte, los anunciantes pueden ser considerados responsables del tratamiento de los datos personales si al recibir la visita desde uno de los anuncios provistos a través de la red de publicidad, capturan información de la clasificación del usuario y la combinan con el comportamiento de este durante la visita o con los datos de registro.

Problemática del consentimiento

La revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas realizada en 2009 introdujo la obligación de obtener el consentimiento previo de los usuarios para poder almacenar o acceder a información almacenada en el terminal de usuario, así como proporcionar información clara y completa sobre el objeto del tratamiento de la información.

Estos requisitos, que implican un mecanismo de consentimiento positivo u *opt-in*, su-

259. La implementación de la Directiva ha sido desigual en Europa, por ejemplo, en el caso de España esta directiva se implementó en marzo de 2012.

ponen un cambio relevante frente al funcionamiento de los mecanismos de monitorización del comportamiento *online*, que en general realizan la instalación de *cookies* en los navegadores configurados para no rechazarlas[260] y permiten mecanismos de *opt-out* en los que los usuarios se pueden dar de baja de los servicios voluntariamente accediendo a la web de las redes de publicidad que controlan estos mecanismos. No obstante, esta interpretación no es compartida por todos los agentes[261], y el proceso de implementación de la Directiva puede generar diferencias entre los enfoques adoptados a nivel nacional y aumentar la incertidumbre para los agentes.

Este cambio de enfoque ha recibido el rechazo frontal de la industria de la publicidad y los medios[262], considerándolo muy perjudicial para la experiencia de usuario –al ver interrumpida constantemente su navegación– así como para el atractivo de la Internet europea y su capacidad de innovación y de generar valor y beneficios para usuarios y empresas, actuando en detrimento de la economía digital y de los ambiciosos objetivos de la Agenda Digital para Europa.

En términos del impacto sobre el negocio de la introducción de la obligación de consentimiento previo, se ha evaluado esta en un 65 % de disminución de la efectividad de la publicidad *online* sobre el cambio de intención de compra. Esta disminución de la eficiencia puede generar una tendencia negativa en la inversión publicitaria en Internet[263] y frenar la aparición de modelos de negocio innovadores sustentados en los ingresos por publicidad.

Asimismo, y como se presenta en el siguiente apartado, el desarrollo de códigos de autorregulación basados en mecanismos de *opt-out* ha sido rechazado por el Grupo de Trabajo del Artículo 29 como sistema para cumplir con la Directiva sobre la privacidad y las comunicaciones electrónicas, lo que convierte la problemática del consentimiento previo, y la implementación y ejecución de esta Directiva en uno de los elementos críticos para el desarrollo del negocio de la publicidad y para muchos modelos de negocio de aplicaciones y servicios de Internet basados en publicidad.

Autorregulación

El desarrollo de códigos de autorregulación se ha planteado como una de las principales opciones para avanzar hacia modelos que permitan una defensa de los derechos de los usuarios equilibrada con la necesaria flexibili-

260. La opinión 2/2010 del Article 29 Data Protection Working Party sobre publicidad basada en el comportamiento considera que el uso de un navegador configurado para aceptar cookies no representa el consentimiento informado que requiere el Artículo 5(3) de la Directiva sobre la privacidad y las comunicacioines electrónicas. Para que el consentimiento pueda darse a través de la configuración del navegador, el GT29 considera que deben darse las siguientes condiciones: a) que el navegador esté configurado para rechazar por defecto todas las cookies de terceras partes y que obligue al usuario a aceptar de forma activa la configuración y la transmisión continuada de información a un tercero, y b) que el navegador, en combinación con las redes de publicidad, presente de forma visible, clara y comprensible la información necesaria para hacer de dicha decisión una decisión informada. Asimismo, el GT29 considera que los navegadores deberían estar configurados por defecto para rechazar el almacenamiento y la transmisión de cookies de terceras partes. En este contexto, el desarrollo de estándares técnicos como el Do-Not-Track puede suponer un impulso relevante para resolver las problemáticas de privacidad relacionadas con la publicidad online.

261. Ver apartado 2.2.4 de Goldfarb, A. & Catherine E. Tucker. «Privacy Regulation and Online Advertising» (2011), Managment Science, 57(1), 57 – 71. Disponible en: http://ssrn.com/abstract=1600259

262. En 2009 se presentó una posición conjunta al Parlamento durante el proceso de revisión del Marco Regulador Europeo (ver http://www.epceurope.org/issues/epc-joint-industry-position-on-the-european-parliament-amendments-regarding-cookies-e-privacy-directive.pdf). Posteriormente, la industria europea se opuso frontalmente a la interpretación realizada por el Grupo de Trabajo del Artículo 29 en su opinión 2/2010 sobre la obligatoriedad del consentimiento previo (ver http://www.iabeurope.eu/public-affairs/e-privacy-directive/europe%E2%80%99s-data-privacy-regulators%E2%80%99-latest-opinion-on-cookies-is-out-of-step-with-online-businesses-and-their-consumers.aspx)

263. Según Forrester, la inversión en publicidad en Europa Occidental es una cuarta parte inferior a la de EE UU. Esta diferencia es más notable si se tiene en cuenta el mayor número de usuarios de Internet en Europa (373 millones frente a 213 en EE. UU.). La combinación de una regulación de publicidad más estricta junto con el mayor número de contenidos en páginas estadounidenses pueden justificar parte de esta diferenciación en inversión publicitaria.

dad que permita la innovación característica en Internet. En este sentido, los agentes involucrados en la provisión de publicidad *online* han impulsado códigos de conducta que permitan facilitar la gestión de la privacidad y del consentimiento. No obstante, las opiniones publicadas por el Grupo de Trabajo del Artículo 29 a tal respecto mantienen la necesidad de cumplir de forma estricta con la Directiva sobre la privacidad y las comunicaciones electrónicas, siendo el desarrollo de códigos de autorregulación por parte de la industria un elemento recomendable pero no suficiente.

El principal ejemplo de esta situación es el código de buenas prácticas[264] publicado por la Alianza Europea de Estándares de Publicidad (*European Advertising Standards Alliance*, o EASA por sus siglas en inglés) en abril de 2011. La recomendación permitirá identificar los anuncios de las redes de publicidad adscritas al código[265] mediante un icono paneuropeo que dirigirá a los usuarios a un sitio web donde estará contenida la información relativa a la política de privacidad, los usuarios podrán comprobar por qué redes de publicidad están siendo monitorizados con el objeto de recibir anuncios *online* personalizados, y tendrán la opción de dejar de recibir publicidad personalizada según su perfil (recibiendo en esos casos publicidad sin segmentación previa). Sin embargo, en su opinión 16/2011, el Grupo de Trabajo del Artículo 29 considera que dicha propuesta no cumple con los requisitos establecidos en el Artículo 5(3) de la Directiva sobre la privacidad y las comunicaciones electrónicas ni constituye un mecanismo auténtico de *opt-out*[266].

El enfoque europeo respecto a la autorregulación –la validación o no del cumplimiento de las propuestas realizadas por la industria– difiere del enfoque que se está llevando a cabo en EE. UU., donde la FTC ha manifestado[267] su apoyo al impulso de códigos de autorregulación y su involucración en el desarrollo de estos. Esta diferenciación entre los modelos europeo y estadounidense puede generar incertidumbre a los agentes que operan en Europa a la hora de invertir esfuerzos en el desarrollo de nuevos códigos de autorregulación. En este sentido, debería evitarse la pérdida del incentivo al desarrollo de autorregulación del tipo *do-not-track*, fuertemente impulsada por la FTC, ya que puede suponer una buena oportunidad para avanzar hacia estándares globales que permitan asimismo cumplir con los principios marcados en las Directivas si se recibe el suficiente apoyo por parte de los reguladores.

4.3.2 Impacto de la revisión del marco regulador europeo

El proceso de diálogo abierto sobre la propuesta de Reglamento de la Comisión Europea puede suponer una oportunidad para limitar las incertidumbres identificadas sobre las problemáticas de privacidad e impulsar mecanismos de consentimiento que impulsen la competitividad del espacio europeo en Internet. No obstante, y como se ha planteado anteriormente, las principales problemáticas derivan de la aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas, cuya modificación no se contempla en el actual proceso de revisión.

Esta Directiva, y la interpretación realizada por el Grupo de Trabajo del Artículo 29, pueden tener implicaciones negativas en términos de inversión en publicidad y en la compe-

264. Disponible en: http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download

265. EASA estima que a mediados de 2012 el 70% de la publicidad online basada en el comportamiento seguirá este código de autorregulación.

266. Según la opinión 16/2011 del Grupo de Trabajo del Artículo 29, la baja de los usuarios de la recepción de publicidad personalizada se realiza mediante la instalación de cookies que avisan a dichas redes de que no se les proporcione dicho tipo de publicidad. Sin embargo, esto no impide a las susodichas redes seguir procesando los datos de comportamiento de los usuarios que se han dado de baja.

267. FTC. Protecting Consumer Privacy in an Era of Rapid Change. Recommendation for Business and Policymakers (2012). Disponible en: http://ftc.gov/os/2012/03/120326privacyreport.pdf

titividad de la industria europea. Sin embargo, será necesario analizar esta evolución y las distintas implementaciones nacionales de la Directiva ya que hasta el momento no ha transcurrido el suficiente tiempo como para clarificar cuál será el efecto producido.

El proceso de debate abierto deberá tener estos aspectos en cuenta y, si procede, plantear la matización de las obligaciones de consentimiento, ya sea a través de un mayor impulso de la autorregulación del tipo *do-not-track* –avanzando hacia lo que podría ser un futuro estándar global– u otros mecanismos que equilibren la protección del derecho individual a la privacidad de los datos personales, con los riesgos y beneficios totales del tratamiento de datos para la provisión de publicidad personalizada.

En términos del impacto de la propuesta de Reglamento, los principales factores señalados por la industria europea[268] de publicidad se centran en los siguientes puntos:

- El incremento de las cargas administrativas y los costes asociados que se generan al considerarse la información utilizada para la monitorización del comportamiento como datos personales. La amplitud en la definición de los datos personales considerada en la propuesta de la Comisión implicará que en la mayoría de los casos los agentes involucrados serán considerados responsables del tratamiento cuando en muchos casos el objetivo no es la identificación de los afectados. En ese sentido la industria solicita la consideración de una nueva categoría de datos que refleje esta situación y equilibre las obligaciones con los riesgos existentes.
- La posible ambigüedad generada, para el caso de la publicidad *online* basada en el comportamiento, por la redacción del Artículo 20, que no permite la toma de medidas legales o que impacten a dicha persona (por ejemplo, relacionado con aspectos como el rendimiento laboral, la salud, la situación económica, el comportamiento o sus aficiones) basándose exclusivamente en el uso de perfiles de usuario generados mediante el tratamiento automático de datos personales.
- La obligación de consentimiento explícito para el tratamiento de los datos.

4.4 Redes sociales

Las redes sociales representan una nueva generación de plataformas colaborativas y de interacción social entre individuos. Este tipo de redes, que agrupan a usuarios con intereses y objetivos comunes y que permiten la comunicación con otros usuarios (conocidos o desconocidos), han alcanzado más de 2.400 millones de usuarios[269] y copan cada vez una mayor parte del tiempo que los usuarios dedican a Internet.

El contenido principal de las redes sociales es proporcionado por los propios usuarios a través del desarrollo de sus perfiles de usuarios, fotografías, vídeos, comentarios o recomendaciones. El número de usuarios, el tipo y la cantidad de información disponible sobre ellos, la visibilidad de los datos y la capacidad de la plataforma para integrar dicha información con terceras partes o aplicaciones suponen algunos de los elementos más relevantes que determinarán el éxito de una red social. Las redes sociales presentan claros efectos de red, cuanto mayor sea el número de usuarios y cuanto más ricos y completos sean los perfiles creados, más capacidad tendrá la red so-

268. Como ejemplo se puede observar la respuesta de la delegación de Reino Unido de la IAB (Internet Advertising Bureau) a la petición de comentarios y evidencias realizada por el gobierno de Reino Unido sobre el impacto de la propuesta de la Comisión Europea. Disponible en: http://www.iabuk.net/sites/default/files/EC%20Data%20Protection%20Rules%20-%20IAB%20UK%20response%20to%20MoJ%20Call%20for%20Evidence.pdf

269. http://vincos.it/social-media-statistics/

cial de conseguir nuevos usuarios, y más valor presentará como plataforma publicitaria o como plataforma para la prestación de aplicaciones o servicios complementarios.

En este sentido, la gestión de la privacidad supone uno de los elementos claves para las redes sociales, no solo por la necesidad de cumplir con las obligaciones legales pertinentes, sino por la propia percepción de los usuarios en relación con el uso y visibilidad de sus datos, que puede situar las políticas de privacidad empleadas como un factor competitivo entre diferentes redes sociales.

Las problemáticas de privacidad en las redes sociales se han incrementado respecto a otro tipo de servicios *online* debido a la facilidad con la que los usuarios revelan información personal, así como a la falta de percepción de estos sobre los riesgos involucrados y a la dificultad de algunos usuarios para configurar de forma adecuada estas herramientas. Una muestra de la cada vez más creciente percepción de estas problemáticas fue recogida por el eurobarómetro en 2011[270], que señalaba que si bien un 74 % de los europeos considera la facilitación de información personal como un aspecto creciente en la vida moderna, el 72 % considera que está proporcionando demasiada información personal *online*. En relación con las redes sociales, el 54% de los usuarios se declara informado de las condiciones de la recogida de datos y del uso posterior de estos, pero solo un 26 % siente que controla sus propios datos.

4.4.1 Problemáticas de privacidad en las redes sociales

Los proveedores de redes sociales son considerados responsables del tratamiento bajo la Directiva de protección de datos, y como tales se ven sometidos a un conjunto de obligaciones y requisitos específicos que, en ocasiones, puede resultar en conflictos con la propia naturaleza de estas plataformas.

Las principales problemáticas de privacidad han sido analizadas en distintos informes a nivel europeo, entre los que se pueden destacar los elaborados por ENISA *(The European Network and Information Security Agency)* en 2007 ofreciendo información y recomendaciones sobre seguridad en redes sociales[271], en 2010 analizando el impacto para la seguridad y la privacidad del uso de las redes sociales desde redes móviles[272], o en 2012 examinando las problemáticas de recogida y almacenamiento de datos en el caso de las redes sociales[273]. Por su parte, el Grupo de Trabajo del Artículo 29 de la Directiva de protección de datos publicó en 2009 su opinión sobre las obligaciones que recaen sobre los proveedores de redes sociales para cumplir con la regulación europea de protección de datos[274]. Mientras, a nivel internacional destaca el informe adoptado por el International Working Group on Data Protection in Telecommunications en 2008, conocido como el *Memorándum de Roma*[275]. A continuación se presentan algunas de las principales problemáticas asociadas con la privacidad en las redes sociales.

Asimismo, la mayor parte de las redes sociales basan parte de sus ingresos en la publicidad *online*, ya sea prestada a través de plataformas publicitarias propias o de acuerdos con redes de distribución de publicidad. La posible integración de los datos personales y otra información de los usuarios en la prestación de publicidad basada en el comportamiento plan-

270. Special Eurobarometer 359, Attitudes on Data Protection and Electronic Identity in the European Union, June 2011.
271. ENISA, Security Issues and Recommendations for Online Social Networks, November 2007.
272. ENISA, Online as soon as it happens, February 2010.
273. ENISA, Study on data collection and storage in the EU, February 2012.
274. Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, WP 163. June 2009.
275. International Working Group on Data Protection in Telecommunications (IWGDPT), Report and guidance on Social Network Services ("Rome Memorandum»), 2008.

tea otro tipo de cuestiones de privacidad presentadas anteriormente, y que deberán añadirse a las presentadas a continuación, más específicas de las redes sociales.

Recogida de datos personales

Una de las principales problemáticas de privacidad en las redes sociales es el tipo y la cantidad de información recogida por estas. En ese sentido, existe un desacoplo entre el principio de minimización de datos, que requiere a los responsables del tratamiento que limiten los datos recogidos a aquellos «adecuados, pertinentes y no excesivos en relación con los fines para los que se recaben y para los que se traten posteriormente»[276], con la naturaleza de aquellas, que tratan de recoger la mayor cantidad de datos para permitir la construcción de perfiles más ricos y precisos que incrementen su valor como plataforma bilateral.

Un número significativo de redes sociales[277] requiere que los usuarios proporcionen datos de género, fecha de nacimiento o localización durante en el proceso de registro. Este tipo de datos son considerados datos sensibles por la Directiva de protección de datos y su requisito obligatorio para el alta en los servicios ha sido considerado excesivo por algunas asociaciones en virtud del principio de minimización, lo que ha llevado a diferentes quejas y procesos formales[278].

Almacenamiento y eliminación de datos personales de los usuarios

Otro de los aspectos más problemáticos es el relacionado con el tiempo que una red social mantiene almacenados los datos de los usuarios y con la capacidad de estos de eliminar definitivamente una información que previamente se ha publicado en las redes sociales.

Según la Directiva de protección de datos, los datos personales deberán ser «conservados [...] durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente»[279]. Este principio es de aplicación tanto a la información «subida» por los usuarios a la red social –como fotografías, comentarios o datos sobre el propio usuario– que este puede querer conservar de modo indefinido mientras siga siendo usuario de la plataforma[280], como a otro tipo de datos relacionados con el comportamiento del usuario, como búsquedas realizadas, accesos, comunicación con otros usuarios, etcétera.

Asimismo, algunas de las redes sociales de mayor éxito –como Facebook o Google+– se encuentran establecidas en EE. UU., lo que hace más complejo el tratamiento de las cuestiones de protección de datos en el ámbito Europeo. Dichas empresas deben adherirse al tratado de puerto seguro para poder transferir datos personales de ciudadanos europeos fuera de las fronteras de Europa; sin embargo, los principios establecidos en este tratado no incluyen la obligación de eliminar los datos tras un período de tiempo, lo que ha generado problemáticas en la aplicación del principio de almacenamiento planteado en la Directiva, y ha impulsado el desarrollo del derecho al olvido en la propuesta de Reglamento de la Comisión Europea.

---

276. Artículo 6(1)(c) de la Directiva de protección de datos.
277. El informe ENISA (2012) analizó los requisitos en materia de datos personales necesarios para operar en 27 redes sociales en distintos países europeos, obteniendo que al menos 17 de ellas requerían datos de fecha de nacimiento o de género (14 de ellas) para el registro inicial como usuario.
278. Por ejemplo, la asociación Europe v. Facebook ha presentado 22 quejas formales frente a Facebook Ireland por diferentes temas relacionados con la privacidad.
279. Artículo 6(1)(e) de la Directiva de protección de datos.
280. Por ejemplo, Facebook planteó en su respuesta a la consulta pública de la Comisión Europea sobre la revisión del marco regulador de protección de datos, que sus usuarios utilizan Facebook como una plataforma de almacenamiento de contenido a largo plazo, y que la eliminación de dichos datos sin el permiso de los usuarios podría generar un perjuicio relevante para ellos y para el funcionamiento y la reputación de la propia red social.

Visibilidad de los datos y configuración por defecto

La visibilidad de la información proporcionada por los usuarios supone uno de los principales riesgos para su privacidad, y la configuración que la plataforma proporcione para los distintos niveles, ya sean contactos o amigos del usuario, otros usuarios de la red social o información disponible desde fuera de la red social –por ejemplo, accesible desde buscadores, se ha situado como un elemento de conflicto potencial con usuarios y supervisores de protección de datos.

Los riesgos para la privacidad pueden surgir de un uso no deseado por terceras partes de los datos personales que se hacen visibles por los propios usuarios. Como ejemplo se puede mencionar el caso de la aplicación *Girls Around Me*[281], que en EE. UU. permitía la localización de mujeres en una determinada zona a partir de la información publicada en la red social Foursquare en combinación con la información pública de los perfiles de Facebook. Si bien Foursquare ha limitado el acceso de dicha aplicación a su interfaz de programación de aplicaciones (API), y Apple la ha retirado de su tienda de aplicaciones, este caso supone un ejemplo de una utilización no legítima de datos personales hechos públicos por los usuarios en el contexto de una red social. Asimismo, se pueden dar casos de copia de la información o de las fotografías publicadas y su *republicación* fuera del ámbito de control de los usuarios.

Aunque la legislación europea prohíbe el tratamiento de datos personales sin el consentimiento de los usuarios, la mayor disponibilidad de datos públicamente visibles y la falta de percepción de los usuarios de los riesgos asociados con dicha visibilidad suponen una problemática de privacidad añadida. En este sentido, el Grupo de Trabajo del Artículo 29 señala dos elementos relevantes para reducir los riesgos y problemáticas de privacidad en las redes sociales: a) que los proveedores de redes sociales proporcionen a los usuarios una adecuada información sobre los distintos niveles de visibilidad de la información publicada y de los riesgos asociados a la privacidad de dicha información, y b) que la configuración de privacidad por defecto que implementen las redes sociales minimice los datos visibles en los niveles con mayor riesgo, como por ejemplo los datos públicamente disponibles.

Por un lado, la red social se beneficiará –en general– de una mayor visibilidad de los perfiles de sus propios usuarios debido a la existencia de externalidades de red, mientras que por otro, los supervisores de protección de datos presionan para que la configuración por defecto sea más restrictiva al considerar necesario un consentimiento explícito[282] para permitir un ámbito de visibilidad de la información más amplio. Si bien los usuarios pueden cambiar de forma activa los distintos niveles de visibilidad de sus datos, es previsible que un número significativo de ellos utilice la configuración por defecto, por lo que este elemento puede suponer un factor de divergencia entre los intereses de las redes sociales y un mayor enfoque hacia la privacidad de la información.

Integración con terceros

Las redes sociales pueden actuar como plataformas en las que terceras partes prestan servicios y en las que el acceso a la información de los usuarios depende de los permisos prestados y de las API implementadas. Existe un gran abanico de aplicaciones disponibles y en desarrollo entre las que se incluyen

281. http://www.bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/

282. En su opinión 15/2011 sobre definición de consentimiento, el Grupo de Trabajo del Artículo 29 cuestiona, en el caso de las redes sociales, que pueda considerarse consentimiento a que un usuario no cambie la configuración de visibilidad (por defecto) a un ámbito más restrictivo.

juegos, aplicaciones de gestión de perfiles desde dispositivos móviles, aplicaciones que gestionan los chats o sistemas de mensajería de diferentes redes sociales (por ejemplo eBuddy), aplicaciones que integran las preferencias de los usuarios en la propia red social (Spotify), etcétera.

Las principales problemáticas pueden derivar de la falta de transparencia sobre el uso de los datos personales, de una falta de proporcionalidad en los permisos requeridos por terceros, o de la ausencia de una granularidad suficiente en el acceso a los datos en las API proporcionadas por la red social a las aplicaciones de terceros, y fundamentalmente, de la falta de mecanismos de consentimiento que permitan diferenciar los permisos prestados, evitando que los usuarios se vean obligados a prestar acceso a terceros a información no relevante para la aplicación solicitada, tener que aceptar ser objeto de una publicidad segmentada o aceptar la explotación o venta posterior de los datos como único modo de poder utilizar una determinada aplicación.

En su opinión 5/2009, el Grupo de Trabajo del Artículo 29 considera que en los casos en los que sea la red social la entidad que medie para prestar el acceso a los datos de los usuarios, esta deberá asegurar que dichas aplicaciones cumplen con la Directiva de protección de datos y con la Directiva sobre la privacidad y las comunicaciones electrónicas, incluyendo que se proporcione una información clara y suficiente a los usuarios y que el acceso se limite a los datos necesarios. Mientras, en el caso de que sea el usuario el que haya mediado para que una aplicación tercera tenga acceso a sus datos, la responsabilidad recaerá exclusivamente sobre las terceras partes.

Usuarios de las redes sociales como responsables del tratamiento de datos personales

El Grupo de Trabajo del Artículo 29 señaló, en su opinión 5/2009, varios casos en los que los usuarios de las redes sociales pueden ser considerados asimismo como responsables del tratamiento[283] de sus propios datos o de datos de terceros publicados en las redes sociales. Esta circunstancia puede generar problemáticas en la aplicación de la normativa de protección de datos, y supone un elemento diferencial de las redes sociales frente a otros servicios *online*.

Las casuísticas principales responden a situaciones que exceden la exención de «actividades domésticas» implementada por la Directiva de protección de datos, como son: a) el uso de las redes sociales para actividades empresariales, colaborativas, comerciales, políticas, etcétera; b) en aquellos casos en los que la información del perfil se encuentra en una esfera de visibilidad abierta a todos los usuarios de la red social o indexable desde buscadores externos[284], y c) cuando se produce el tratamiento o publicación de datos de terceras partes.

4.4.2 Impacto de la revisión del marco regulador europeo

Uno de los principales desafíos para una defensa equilibrada de la privacidad en las redes sociales radica en que la mayor parte de la información disponible en ellas se publica bajo la iniciativa de los propios usuarios y basándose en su consentimiento. La regulación «tradicional» de privacidad se centra en la definición de reglas para proteger a los ciudadanos frente a usos injustos o poco proporcionados del trata-

283. En estas situaciones se considera que el usuario de la red social es un responsable de tratamiento de datos que está proporcionando dichos datos a otro responsable (la propia plataforma de red social) y a terceros (otros usuarios de la red social). En estos casos el usuario tendrá que cumplir con todas las obligaciones de un responsable del tratamiento, incluido el requisito de obtener el consentimiento del afectado para la publicación o tratamiento de sus datos.

284. El Grupo de Trabajo del Artículo 29 recuerda que, si bien estos casos no estarían exentos por la cláusula de «actividades domésticas», sí podrían estarlo por otras, como por actividades periodísticas, artísticas o literarias.

miento de datos, y el gran incremento de datos personales publicados por iniciativa de los propios usuarios genera nuevas y complejas problemáticas.

La revisión del marco regulador europeo y el debate que está siguiendo a la propuesta de la Comisión suponen una gran oportunidad para alinear la defensa de los derechos de los usuarios con mecanismos más flexibles que faciliten el desarrollo de los servicios prestados por las redes sociales. La propuesta de la Comisión incorpora cambios relevantes en el marco regulador que afectan a las problemáticas de privacidad presentadas y que abren nuevos elementos de debate. Los aspectos más relevantes de dicha propuesta que impactan sobre las redes sociales son los siguientes:

- La modificación del ámbito de aplicación del Reglamento, pasando a afectar las disposiciones previstas a todas las empresas que presten servicio en Europa. En el caso de las redes sociales este cambio resulta muy relevante al estar un gran número de ellas establecidas fuera de las fronteras europeas.
- La introducción del derecho al olvido, que puede generar dificultades técnicas para su aplicación en las redes sociales debido a la gran visibilidad que pueden alcanzar los contenidos publicados. Asimismo, puede plantear otro tipo de dificultades al poder ser los propios afectados responsables o responsables conjuntos del tratamiento. Según el despacho de abogados Hogan Lovells International[285], será necesario un análisis más detallado para determinar si el proveedor de la red social es el responsable de implementar los mecanismos técnicos necesarios para ayudar al afectado (y responsable del tratamiento) a obtener el borrado de sus datos personales en terceras plataformas.
- La introducción del derecho de portabilidad, que puede tener un impacto significativo sobre las redes sociales dado el gran volumen de datos almacenado en ellas. Algunos argumentos[286] que señalan la necesidad de una revisión de esta propuesta consideran que el derecho a la portabilidad queda fuera del ámbito de aplicación de un Reglamento de protección de datos y que debería tratarse en un ámbito de defensa de la competencia y tan solo tras un análisis que señale fallos de mercado.
- El establecimiento de la privacidad por defecto, que puede afectar al modo en el que se gestiona la visibilidad de los perfiles en las redes sociales. Concretamente, la propuesta de Reglamento establece en su Artículo 23 que «[...] por defecto, los datos personales no sean accesibles a un número indeterminado de personas», pudiendo repercutir en el ámbito de visibilidad de los perfiles –especialmente en las búsquedas realizadas en entornos externos a la plataforma– obligando a los proveedores de servicios de red social a prestar una información más completa a sus usuarios si buscan ampliar dicho ámbito de visibilidad.
- La prohibición del desarrollo de perfiles, que podrá afectar a la capacidad de monetizar la inteligencia obtenida del tratamiento de los datos y limitar, en cierta medida, el desarrollo de nuevos servicios que utilicen las redes sociales como plataforma para su prestación.

4.5 Aplicaciones móviles

Las aplicaciones móviles se encuentran en un mercado naciente y dinámico con una alta ca-

285. Hogan Lovells, Response of Hogan Lovells International LLP to the Ministry of Justice's call for evidence on the EU Data Protection Proposals. 2012.

286. Hogan Lovells (2012).

pacidad de trasladar los beneficios de la innovación a los usuarios finales. Este mercado ha experimentado un crecimiento explosivo en los últimos tres años y medio, pasando de cerca de las 600 aplicaciones disponibles en el lanzamiento de las tiendas de aplicaciones de Apple y Android, al más de medio millón de aplicaciones en el *App store* de Apple y más de 380.000 aplicaciones disponibles en *Android Market* en 2012[287]. Las aplicaciones están disponibles para diferentes dispositivos, y hasta el momento se han descargado más de 28.000 millones de ellas.

Este ecosistema, formado por operadores de telecomunicaciones, fabricantes de terminales, desarrolladores de sistemas operativos, desarrolladores de aplicaciones móviles, plataformas de Internet, anunciantes, etcétera, es altamente competitivo, y la capacidad de elección del usuario y su opinión, reflejada en los propios *app markets*, es prioritaria para determinar qué aplicaciones tienen éxito y cuáles no.

El rápido crecimiento del mercado proporciona oportunidades y beneficios muy significativos para los usuarios, pero también puede generar cuestiones relacionadas con la privacidad. Las aplicaciones móviles pueden acceder a un amplio abanico de información sobre el usuario, como datos de geolocalización muy precisos, número telefónico, agenda de contactos, registros de llamadas, identificadores de usuario y del terminal, así como otra información almacenada en el dispositivo entre la que se pueden encontrar vídeos o fotografías.

El manejo de los datos personales y de otra información asociada a los individuos es uno de los factores competitivos en este mercado por tres motivos principales. En primer lugar, por la capacidad de innovación que supone, ya que un uso adecuado de la información accesible puede permitir el diseño de aplicaciones novedosas capaces de atraer a los usuarios. En segundo lugar, por la capacidad de mejorar la monetización de las aplicaciones móviles, en muchos casos basadas en el uso de publicidad cuya eficiencia aumenta con la personalización basada en el comportamiento, y en otros casos mediante la puesta a disposición de los datos a terceros. Y en tercer lugar, por la propia imagen y confianza percibida por los usuarios en las aplicaciones, cuya adopción tiene una fuerte dependencia en la opinión de otros usuarios al verse reflejada durante su compra o instalación la puntuación otorgada y los comentarios realizados por otros usuarios (sean estos buenos o malos).

De esta forma, si bien los distintos agentes tienen incentivos para realizar un uso intenso de los datos personales en las aplicaciones móviles, el rechazo a dichas prácticas o la desconfianza de los usuarios puede suponer una desventaja competitiva relevante. No es por tanto de extrañar que, pese a lo incipiente de este mercado, ya se hayan producido algunas problemáticas relacionadas con la privacidad de los datos personales[288]. De hecho, es previsible que estas aumenten conforme se vaya perfeccionando el uso de los datos en el ecosistema de las aplicaciones móviles y según siga aumentando el número de usuarios de *smartphones*, *tablets* y otros dispositivos similares.

4.5.1 Problemáticas de privacidad en las aplicaciones móviles

Transparencia y control sobre la información recogida y procesada

Los usuarios de aplicaciones móviles toman frecuentemente decisiones relacionadas con la privacidad, como elegir qué aplicaciones ins-

287. FTC. Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (2012).

288. Por ejemplo, la polémica surgida en 2011 por el almacenamiento de los datos de localización producido en terminales de Apple y algunos de los basados en el sistema operativo Android. Ver http://www.huffingtonpost.com/2011/05/10/senate-panel-apple-google-location-data-privacy_n_860155.html

talar, basándose en la información proporcionada en las plataformas de aplicaciones sobre los permisos de acceso[289] requeridos y los comentarios u opiniones de otros usuarios.

En este sentido, resulta muy importante que los desarrolladores de las aplicaciones pongan a disposición de los usuarios la política de privacidad seguida, en la que se indique el tipo de información recogida, para qué se usa, si se recoge información de geolocalización, si se comparte dicha información con terceros para proporcionar publicidad, así como información sobre los derechos de los usuarios (como el *opt-out*) entre otros.

El desarrollo de códigos de autoconducta puede definir directrices para saber: a) cómo proporcionar a los consumidores una adecuada información sobre las prácticas de privacidad de la aplicación móvil, considerando las limitaciones inherentes a los dispositivos móviles como el tamaño de la pantalla, y b), cómo conseguir que colaboren los distintos participantes en el proceso de desarrollo y entrega de las aplicaciones para asegurar que esta información se entrega al usuario. En este sentido, se puede señalar que existen múltiples directrices que plantean cómo se debe realizar esta entrega de información, como el código planteado por el GSMA[290], o la propuesta de política de privacidad planteada por el MMA[291].

Asimismo, para disminuir las problemáticas de privacidad resulta necesario que durante el proceso de instalación de las aplicaciones, el usuario tenga la información suficiente sobre los permisos requeridos y la política de privacidad empleada para poder dar un consentimiento informado. Para incrementar el control del usuario, algunas plataformas móviles permiten que el usuario modifique el acceso que las aplicaciones tienen a diferente información, como por ejemplo los datos de geolocalización. Este tipo de control podrá mejorar con el desarrollo de iniciativas como el *do-not-track*.

En un ecosistema tan complejo como el de las aplicaciones móviles, resulta muy relevante la distribución de las responsabilidades en relación con la privacidad de los datos personales entre los desarrolladores de estas, los sistemas operativos que les dan acceso a los distintos recursos, los fabricantes de terminales y los operadores móviles. En este tipo de entornos, resulta relevante que los distintos intermediarios entre el usuario y la aplicación implementen protecciones para salvaguardar frente a un mal uso de los datos personales (como la solicitud de consentimiento al acceso a los recursos previo a la instalación, o la disponibilidad de una opción fácil de ejecutar que bloquee el acceso de las *apps* a los datos de localización), pero el hacerles responsables del uso de los datos personales realizados por terceros puede suponer un importante impacto negativo en el dinamismo de este mercado. En este sentido, el establecimiento de foros entre los diferentes agentes involucrados para avanzar hacia códigos de autoconducta puede suponer un marco adecuado para resolver una gran proporción de las problemáticas de privacidad de las aplicaciones móviles.

Monitorización de la actividad del terminal

Otra de las problemáticas relacionadas con la privacidad en las aplicaciones móviles es la referida a la posibilidad de monitorizar el comportamiento que los usuarios realizan de sus terminales. Si bien esto puede resultar legítimo para diagnosticar y mejorar el funcionamiento de los propios dispositivos, sistemas operativos o aplicaciones, la monitorización

289. Entre estos permisos a la API del sistema operativo se encuentra el acceso a comunicación de datos, agenda de contactos, localización, registro de llamadas, memoria, etcétera.

290. GSMA, Privacy Design Guidelines for Mobile Application Development (2011), Global System for Mobile Communications Association.

291. MMA, Mobile Application Privacy Policy Framework (2011), Mobile Marketing Association.

de las llamadas, mensajes o del uso de las aplicaciones puede resultar sensible para determinados usuarios. En esta área, el desarrollo de códigos de autorregulación puede permitir que los principales operadores y plataformas móviles alcancen unos compromisos adecuados sobre transparencia y limitaciones de la recogida de información en los nuevos dispositivos (*smartphones*, *tablets*, etcétera).

Utilización de los datos personales para la prestación de publicidad

No hay duda de que la publicidad basada en el comportamiento y en la localización puede ser útil para los usuarios y aportar valor a las empresas y los desarrolladores. Sin embargo, este uso plantea cuestiones relativas a la granularidad de los datos recogidos, al tiempo que son retenidos y, en definitiva, sobre qué prácticas son consideradas apropiadas para el uso de información muy precisa sobre geolocalización por terceras partes en un contexto de análisis de datos y de publicidad basada en el comportamiento y en la localización.

4.5.2 Impacto de la revisión del marco regulador europeo

La fase inicial en la que se encuentra el mercado de aplicaciones móviles y su continua evolución hacen difícil comprender el impacto que tendrá la revisión del marco regulador europeo de protección de datos para su desarrollo futuro. No obstante, el potencial económico y de generación de empleo deberá tenerse en cuenta en el proceso de debate que está siguiendo a la propuesta de la Comisión Europea, para que el Reglamento de protección de datos aprobado permita a Europa competir en el mercado global de aplicaciones móviles sin desventajas manifiestas fruto de reglas muy diferenciadas respecto a los estándares globales.

Este mercado ha pasado de una facturación de 3.800 millones de dólares en 2008 a unas expectativas de ingreso de 76.000 millones en 2015[292]. En torno al 88 % de las empresas involucradas en el desarrollo de aplicaciones móviles son pequeñas o en muchos casos individuales[293]. El establecimiento de marcos muy prescriptivos o que introduzcan muchas obligaciones de costoso cumplimiento dificultará el desarrollo del mercado –especialmente para las pequeñas empresas, principales generadoras de empleo que en EE. UU. han impulsado este mercado hasta cerca del medio millón de empleos[294].

En este sentido, la utilización de los estándares de autorregulación ya disponibles y en desarrollo, y la presencia de medidas que permitan asegurar su cumplimiento, pueden permitir el tratamiento de la mayor parte de las problemáticas de privacidad en el mercado de las aplicaciones móviles sin impactar negativamente en su desarrollo. Asimismo, es importante que la regulación adoptada sea igual para todos los agentes involucrados en el mercado de las aplicaciones móviles, independientemente de que sean o no operadores de telecomunicación.

292. http://www.slideshare.net/joelrubinson/an3---us---appeconomy20112015
293. http://Republicans.EnergyCommerce.house.gov/Media/file/Hearings/CMT/100511/Reed.pdf
294. http://www.technet.org/new-technet-sponsored-study-nearly-500000-app-economy-jobs-in-united-states-february-7-2012/

Richard Allan

Richard Allan es actualmente director de Política Pública en Facebook EMEA. Se unió a Facebook en junio de 2009, y desde entonces encabeza las labores relativas a la política pública de la empresa en Europa. Antes de unirse a Facebook, Richard había sido director europeo de Asuntos Gubernamentales para Cisco desde septiembre del 2005. En abril de 2008, el Gabinete de Reino Unido nombró a Allan presidente de la Comisión Especial sobre el Poder de la Información, donde trabajó para mejorar el uso de los datos del gobierno. La Comisión Especial terminó su labor en mayo de 2009 con la publicación de un informe cuyas recomendaciones fueron muy bien acogidas por el gobierno británico.

Allan escribe y habla sobre una amplia serie de asuntos relacionados con la política tecnológica, y ha sido visitante académico del Oxford Internet Institute. Fue elegido miembro del Parlamento de Sheffield Hallam en 1997 y reelegido en 2001 antes de ceder su puesto en 2005. Allan se especializó en cuestiones sobre política tecnológica en el Parlamento y fue portavoz principal de varios proyectos de ley, incluyendo la Ley de Protección de Datos, la Ley sobre la Regulación de las Competencias de Investigación y la Ley de Comunicaciones. Fue presidente del Comité Informativo del Parlamento en 1997 y miembro de los Comités de Contabilidad Pública y Coordinación del Parlamento en 2001.

Entre 1991 y 1997, trabajó como profesional informático en el servicio público de salud británico, diseñando y creando sistemas de gestión de la información. Es licenciado en estudios anglosajones, escandinavos y celtas en arqueología y antropología, y cuenta con un máster en tecnología de la información.

5. Contribuciones para «El impacto de la regulación sobre los nuevos servicios»

5.1 Facebook: La posición de Facebook sobre la privacidad y la seguridad

Richard Allan.
Director de Política Pública en Facebook EMEA

5.1.1 Introducción

El cometido de Facebook consiste en proporcionar a la gente la capacidad de compartir y de convertir el mundo en un lugar más abierto y conectado. Con cientos de millones de usuarios activos en el mundo entero, el impacto que ejerce en la vida de las personas, desde su participación activa en el diálogo político hasta historias personales de familias que se han vuelto a encontrar, no tiene precedentes.

Su capacidad de conexión es lo que atrae a la gente a Facebook, tanto por la posibilidad de encontrar a viejos amigos como por mantener el contacto con la familia, planificar eventos o compartir momentos especiales. Además, es una plataforma de diálogo político. Los ciudadanos ya pueden hablar directamente con sus líderes, nacen nuevos movimientos políticos *online* y una única voz puede llegar a millones de personas.

Lo que no se ha documentado tan bien hasta hace poco es el papel de las redes sociales, y en especial el de Facebook, a la hora de sustentar el crecimiento económico a nivel mundial. Facebook ha engendrado un nuevo ecosistema laboral en EE. UU., donde ha creado unos 235.000 puestos de trabajo tan solo en el ámbito de las aplicaciones. Empresas de todos los tamaños están volviendo a definir la forma en que se conectan y venden a sus clientes en la red social. Y no se trata de un fenómeno aislado de EE. UU. Un estudio reciente de Deloitte[295] estimó que Facebook generó más de 15.000 millones de euros de valor añadido en la UE en 2011, sustentando más de 230.000 empleos. La propia economía de las aplicaciones de Facebook en el ámbito europeo se estima en más de 1.900 millones de euros y sustenta más de 29.000 puestos de trabajo. A su vez, las empresas utilizan el servicio para conectarse con sus clientes,

295. http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/Industries/TMT/uk-tmt-media-facebook-europe-economic-impact.pdf

crear una publicidad más efectiva y crear la identidad de la marca.

El potencial que tienen Facebook y, en conjunto, el ecosistema *online* para fomentar el crecimiento económico depende de la capacidad de compartir la información de forma sencilla, de manera que puedan crecer nuevos modelos empresariales sin obstáculos legislativos innecesarios. Es importante la asociación con los reguladores con el fin de crear un entorno que promueva la inversión y la innovación y proporcione un marco legislativo coherente y estable. Al mismo tiempo, hay que continuar capacitando a los usuarios de forma que puedan controlar sus datos y conectarse y compartir de manera informada.

5.1.2 Enfoque de la protección de datos basado en principios

Es esencial que todos los servicios de Internet, tanto en Europa como en EE. UU., disfruten de seguridad y previsibilidad en lo que respecta a la regulación en materia de protección de datos. La interoperabilidad total entre la UE y EE. UU. y otros regímenes es indispensable para poder promover la innovación, que a su vez es de gran importancia para el fomento del empleo.

Facebook se alegra de que uno de los objetivos de la Comisión Europea al proponer el nuevo marco legislativo sobre Protección de Datos[296] consista en el estímulo del crecimiento y el empleo. Este aspecto también se refleja en el *Libro Blanco* del Ministerio de Comercio de EE. UU.[297] relativo a la privacidad de los datos de los consumidores, que busca tanto cumplir con las expectativas de estos en los contextos en que utilizan los servicios *online*, como promover la innovación que ha estimulado el crecimiento de Internet durante las últimas dos décadas.

Cualquier marco legal sobre protección de datos debe conseguir un adecuado equilibrio entre el fomento de la innovación y la aportación de una transparencia razonable y control significativo de los datos de los consumidores dentro del contexto de los distintos servicios y modelos empresariales. Se puede contar con una regulación sobre privacidad sólida y un sector digital próspero. Dicho marco legislativo debería basarse en principios y centrarse en fomentar mejores prácticas por parte de las empresas en vez de establecer unas normas técnicas detalladas que no soportarán el paso del tiempo y podrían resultar frustrantes y costosas, tanto para los proveedores de servicios como para los usuarios.

La política de privacidad de Facebook se guía por tres principios: control, transparencia y responsabilidad. Estos principios reflejan el prolongado compromiso adquirido frente a sus usuarios.

Control para el usuario

La esencia del producto Facebook consiste en compartir y conectar. Esos son los motivos por los que la mayoría de la gente se une a Facebook y más de la mitad de sus 845 millones de usuarios activos vuelven a visitar el sitio cada día.

Facebook cree que la gente debería controlar el contenido compartido en su cuenta y escoger la audiencia con la que lo comparten. Con los «controles en línea» introducidos en agosto de 2011, cada uno puede escoger fácilmente los ajustes de privacidad todas y cada una de las veces que publique contenidos mediante la decisión de la audiencia para la que estos serán visibles. Además, también puede ver las publicaciones anteriores y cambiar los ajustes de privacidad de manera individualizada.

Los ajustes de cuenta iniciales recomendados de Facebook se han escogido de manera

296. http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
297. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

que las personas puedan encontrar y conectarse fácilmente con sus amigos, al tiempo que protegen la información más sensible. Facebook quiere dejar claro qué información se considera pública y cómo pueden controlar las personas que usan Facebook de manera exacta el contenido que comparten y con quién en el momento que decidan hacerlo.

Uno de los elementos centrales del control de los usuarios es su derecho a eliminar sus propias cuentas o contenidos concretos que hayan publicado en su historial. Facebook ofrece esta posibilidad a sus usuarios y defiende los derechos de las personas a eliminar su propio contenido. Cuando la cuestión de la eliminación se vuelve más polémica es cuando alguien quiere eliminar y ejercer control sobre el contenido que otras personas han publicado. Este hecho puede dar lugar a conflictos con el derecho a la libertad de expresión de la otra persona, y por ello debe estudiarse detenidamente.

Control y consentimiento

Las propuestas de la Comisión Europea incluyen un aumento de los requisitos para la obtención del consentimiento del sujeto registrado a la hora de legitimar el procesamiento de los datos. Aunque el consentimiento es un principio importante, hay que garantizar que no conduce a requisitos demasiado preceptivos que impliquen mecanismos molestos e innecesarios de solicitud de consentimiento para actividades concretas. De ser así, se correría el riesgo de inundar a los usuarios con casillas de verificación y avisos. Esto, aparte de afectar a la experiencia del usuario, conduciría inevitablemente a una posible «devaluación» del principio de control, y podría hacer más complicada la toma de decisiones de los usuarios en lo relativo a cuándo otorgar consentimiento y cuándo denegarlo.

Tal y como se ha afirmado, es importante tener en cuenta que servicios como Facebook se han diseñado para que la gente pueda conectarse y compartir información. La auditoría[298] efectuada por el Comisario de Protección de Datos de Irlanda (CPD) sobre las prácticas de privacidad de Facebook en 2011 aceptó que en el caso de una red social, el usuario otorga el consentimiento al registrarse en el servicio. Ese consentimiento, combinado con la cantidad de información que Facebook ofrece en su página sobre la forma en que se usa la información y el nivel de control concedido a los usuarios para gestionar sus datos, constituye un ejemplo convincente de cómo puede obtenerse el consentimiento de manera firme y muy fácil para el usuario.

Facebook cree que el consentimiento debería obtenerse cuando sea importante, y que el contexto desempeña un papel clave en ello. Para los servicios en los que la gente ejerce un control específico cada vez que comparte los datos, la proporción de información contextual representa un modelo efectivo de obtención de un consentimiento valioso.

Transparencia y todavía más transparencia

Facebook ha adquirido el compromiso de ser transparente respecto a la información que las personas almacenan en su servicio, y a este respecto, ha sido líder en la creación de herramientas en Internet que proporcionen a las personas la capacidad de ver y controlar lo que comparten.

Facebook se ha esforzado al máximo por garantizar que su política de uso de datos[299] se explique de forma clara y comprensible, con información adaptada a los distintos grupos de edades. En ella, la gente puede conocer los tipos de información que recibe Facebook y cómo se utiliza; conocer los ajustes de

298. http://dataprotection.ie/viewdoc.asp%3FDocid=1175%26Catid=66%26StartDate=1+January+2011%26m=n
299. facebook.com/about/privacy

privacidad que ayudarán a controlar la información de las personas en Facebook; averiguar las formas en que se comparte la información del usuario con los juegos, aplicaciones y páginas web que no pertenecen a Facebook; ver cómo se envían anuncios sin compartir la información del usuario con los publicistas, y comprender cómo se adecuan los anuncios al contexto, como ocurre con las historias del tipo servicio de noticias.

Facebook siempre está buscando maneras de mejorar en esta área, y este es un compromiso constante frente a sus usuarios y los reguladores. De hecho Facebook, tras la auditoría de 2011, se ha comprometido a trabajar estrechamente con la Oficina del CPD de Irlanda para encontrar la forma de mejorar la información que se proporciona a las personas en cuanto a cómo pueden controlar su información al utilizar las aplicaciones.

La responsabilidad es nuestro cometido

En primer lugar, Facebook es responsable frente a sus usuarios y siempre está encantado de escuchar las actualizaciones propuestas por las personas en relación con la política de privacidad y otros documentos reglamentarios. En mayo de 2012, unos 800.000 usuarios se habían suscrito a las actualizaciones de la página de Privacidad de Facebook y más de 2 millones de usuarios se habían suscrito a la página de gestión del sitio.

Facebook también es responsable frente a los legisladores. A continuación se incluyen dos casos del año pasado que demuestran el compromiso formal de Facebook frente a los legisladores de EE. UU. y la UE:

- Acuerdo del comisario federal de Comercio[300]: Este fue el último de una serie de acuerdos sobre ajustes de privacidad con empresas importantes de tecnología avanzada, y forma parte de los esfuerzos de la FTC por fijar las normas de aplicación en toda la industria para las empresas líderes en control de privacidad. Para Facebook, este acuerdo ayuda a formalizar compromisos claros respecto a prácticas sólidas en materia de privacidad. Como resultado, Facebook seguirá dando prioridad a la privacidad y aplicando medidas adicionales de protección, que incluyen un programa de privacidad revisado y análisis regulares realizados por externos sobre las prácticas de privacidad. Facebook designó a dos directivos de privacidad (uno para la política y otro para el producto) tras este análisis.
- Auditoría del CPD de Irlanda: Facebook fue sometido a una auditoría profunda y detallada realizada por la Oficina del CPD de Irlanda en relación con sus prácticas y políticas, y que se publicó el 21 de diciembre de 2011. Los informes de auditoría no suelen publicarse, pero en este caso el CPD y Facebook acordaron desde el principio que para fomentar la transparencia deberían publicarse todos los resultados de la auditoría en su totalidad. Se dedicaron muchísimos recursos a garantizar que el CPD contara con toda la información necesaria para efectuar una auditoría integral. Esta implicó tres meses de análisis riguroso, y el informe final demostró que Facebook cumple con los principios europeos sobre protección de datos y con la legislación irlandesa. Además, identificó áreas en que podría mejorarse, y Facebook está trabajando para aplicar las recomendaciones durante la primera mitad de 2012.

Facebook cree que un enfoque basado en la responsabilidad es muy útil especialmente para las empresas globales de Internet. Dicho

300. http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf

esto, resulta relevante que dicho enfoque no se añada sencillamente a la carga reglamentaria de las empresas que estén dispuestas a responsabilizarse.

En el contexto de la UE, las empresas podrían tener que responder formalmente ante la Autoridad de Protección de Datos (APD) del Estado miembro donde estén constituidas («sede principal»). Si una empresa está dispuesta a responder ante su APD nacional así como a implantar unas buenas políticas y prácticas que comparta con otras APD, entonces debería someterse a un régimen más sencillo por el que no requiera la reautorización para sus operaciones. Esto implicaría, además, la necesidad de implantar un sistema vinculante de reconocimiento mutuo de las decisiones tomadas por la APD del país de constitución y las APD de los otros Estados miembros. Dicha aplicación del principio de la responsabilidad aportará el nivel suficiente de armonización en la UE, muy ansiada y necesaria para conseguir un verdadero mercado único digital en Europa.

Mercado Único Digital europeo: mayor armonización

Facebook es líder entre los proveedores de servicios de Internet globales en materia de transparencia y predisposición a la hora de colaborar con las APD europeas, y seguirá haciendo uso de este constructivo enfoque para cumplir con sus obligaciones frente a los usuarios.

Hemos acogido de buena gana el sistema de «ventanilla única» propuesto por la Comisión Europea así como su iniciativa para conseguir una mayor armonización de la legislación europea sobre protección de datos y en especial de la jurisdicción de las APD. Desde 2010, los usuarios de Facebook en Europa han recibido este servicio desde Facebook Ireland Ltd, que cumple con la legislación irlandesa sobre protección de datos y tal y como se ha mostrado con anterioridad, ha sido supervisada por el CPD de Irlanda.

Facebook cree que la aplicación de un principio de «ventanilla única» sólido y veraz en Europa es extremadamente importante para poder demostrar el cumplimiento de la ley y garantizar una certeza legal para las empresas que operen a escala europea y global.

La armonización de los principios legales relativos a la protección de datos en la UE puede contribuir al objetivo de conseguir un verdadero mercado único digital europeo sin otros obstáculos artificiales. Las personas registradas en Facebook obtienen el mejor valor del servicio al poder compartir sin restricciones geográficas. Esta capacidad de llegar a tanta gente del mundo entero es el motivo por el cual las empresas que usan Facebook pueden crecer promoviendo sus empresas con las páginas gratuitas de Facebook, publicitándose o desarrollando aplicaciones en la plataforma abierta.

5.1.3 Conclusión

La privacidad está en el núcleo de todo lo que hace Facebook. Está integrada en los productos desde su fase de diseño, y existen equipos especiales de expertos en privacidad que analizan el impacto que estos productos podrían ejercer sobre la privacidad de los usuarios. La gente es dueña y controla la información que comparte en Facebook, y así seguirá siendo siempre.

Mientras el debate en Europa y EE. UU. se intensifica, Facebook mantendrá su firme compromiso con reguladores y políticos con el fin de conseguir un marco de protección de datos viable que equilibre en gran medida los requisitos reglamentarios relativos a la protección de datos al tiempo que posibilite un sector digital próspero e innovador.

Eric Debroeck

Vicepresidente sénior del Grupo de Asuntos de Regulación en France Telecom-Orange desde mediados de 2004. De 2000 a 2004 fue director de «servicios de operadores nacionales», la unidad de negocio a cargo de las actividades comerciales al por mayor con los competidores nacionales. Anteriormente estuvo a cargo de diferentes puestos de gestión en France Telecom en áreas de estrategia corporativa, regulación nacional y europea. Eric Debroeck se graduó en la École Polytechnique y en la École Nationale Supérieure des Télécommunications.

5.2 Orange Telecom: la opinión de Orange sobre la regulación de la privacidad y la seguridad

Eric Debroeck
Vicepresidente sénior del Grupo de Asuntos de Regulación en France Telecom - Orange

5.2.1 La protección de las personas, los servicios innovadores y el desarrollo económico deberían impulsar el nuevo planteamiento legislativo global

Uno de los cambios sociales más importantes provocados por la tecnología digital concierne a los planteamientos de los individuos en torno a la privacidad: mientras que en la década de los sesenta la privacidad era una cuestión que afectaba tan solo a los famosos, unas pocas décadas después la gente se encontró viviendo en un tiempo en que los ordenadores almacenaban continuamente registros de todo tipo de cosas, convirtiendo la privacidad en un problema generalizado.

Hoy día son múltiples los dispositivos que generan una cantidad ingente de datos, y estos se comparten a través de servicios *online* y plataformas conectadas. Cada día, una comunidad enorme de personas utiliza nuevos servicios basados en la publicidad para almacenar fotografías, publicaciones y blogs y disfrutar de servicios de comunicación[301]. Empresas tales como Google, Amazon, Apple y Facebook, que comercian con los perfiles de sus clientes, han hecho de la minería de datos personales un negocio muy rentable.

Grupos enormes de personas han comenzado a comerciar con los datos personales para medios de comunicación, conexiones sociales y servicios de almacenamiento basados en la publicidad. Uno de los resultados del éxito de estas empresas es que los europeos se ven igualmente afectados por prácticas que no cumplen en su totalidad con la normativa europea sobre protección. En la actualidad, los europeos no siempre sienten que controlan al completo sus datos personales, y no están lo suficientemente informados sobre su derecho a la privacidad.

Debido a este nuevo contexto, la normativa sobre privacidad está sometida a un proceso de revisión. En Europa, la Comisión está redactando un Reglamento general de protección de datos unido a una directiva sobre los poderes policiales y las medidas penales relacionados con la protección de datos; en EE. UU., con la administración de Obama, una «carta de derechos» sobre protección de datos debería refle-

301. Enero de 2012: hay 800 millones de personas conectadas a Facebook en el mundo entero.

jar los principios trazados en el enfoque europeo. Conforme maduran los servicios y los modelos de negocio basados en los datos se establecen en el entorno del *cloud computing*, los legisladores se enfrentan al reto de mejorar el nivel de convergencia y armonización que requiere la economía digital global.

La función de los legisladores es la de proporcionar un marco jurídico global adecuado para la innovación que posibilite la prestación de servicios innovadores y el desarrollo de nuevos modelos de negocio, así como la de seguir fomentando la confianza entre los usuarios y la certeza jurídica. La función de los agentes responsables de Internet consiste en proporcionar herramientas de gestión de la privacidad transparentes y fáciles de usar. Estas herramientas permitirán a los individuos controlar si se usan sus datos y la forma en que se procesan, y les alentará a dar permiso con respecto al uso de sus datos personales por parte de los proveedores de servicios y los publicistas en especial.

5.2.2 Planteamiento de Orange centrado en el consumidor

Orange cree que hoy día los consumidores son conscientes de que su información personal se ha convertido en un activo, y que lo que necesitan son herramientas que les ayuden a protegerse al tiempo que se comercia de forma transparente con este valor en tanto en cuanto así lo permitan. La percepción de las personas del valor de sus datos y de la privacidad que desean varía, y quienes utilizan servicios avanzados *online* han cambiado su posición de sujetos registrados vulnerables a sujetos protegidos y a cierto grado de madurez, lo cual implica que pueden ejercer control sobre sus propios datos y tener cierto poder frente a las empresas. Este cambio es esencial a la hora de crear formas reales y sostenibles en que los individuos puedan controlar el uso de sus datos personales.

Orange comparte el punto de vista del Foro Económico Mundial[302] en lo relativo al concepto de la orientación hacia el usuario final, en el sentido de que los consumidores son participantes atentos y esenciales para la creación e intercambio de valores en servicios y experiencias. Grandes grupos de consumidores comparten su opinión en torno a los servicios a través de foros y redes sociales, y son conscientes de su poder en el mercado si actúan de forma colectiva. Un enfoque centrado en el consumidor pretende integrar distintos tipos de datos personales cumpliendo con cuatro principios clave:

- Transparencia: del tipo de datos, de la finalidad del tratamiento y de quién puede acceder a ellos.
- Confianza: la confianza de los individuos en su disponibilidad, fiabilidad, integridad y seguridad se gestiona de manera correcta.
- Control: la capacidad de los individuos de gestionar de forma efectiva hasta qué punto se comparten sus datos personales.
- Valor: los individuos comprenden el valor originado a partir del uso de sus datos y la forma en que se les compensa por ello, y son conscientes de su poder en el mercado tanto a nivel individual como colectivo.

La transparencia y la confianza son puntos fuertes en la relación de Orange con el consumidor, una visión positiva que los servicios móviles de Orange, en concreto, han cuantificado en muchas ocasiones.

Orange está progresando en la actualidad en cuanto al control y el valor. El planteamiento de Orange es extremadamente cauto, y se basa en solicitar la autorización de autoridades específicas sobre privacidad para las ofertas de

302. «Datos personales: el surgimiento de una nueva clase de activos».

Orange que impliquen a consumidores dispuestos a participar en la elaboración de perfiles. Este diálogo con el responsable del tratamiento concede a Orange la garantía de que se ha alcanzado un elevado nivel de transparencia y que se han aplicado las medidas de seguridad adecuadas a la hora de procesar los datos personales. Orange ha lanzado recientemente Preference, una oferta por la que se crean perfiles de clientes a cambio de retribuciones, basada en un planteamiento estrictamente voluntario. Antes de su lanzamiento comercial, la oferta se presentó a la Autoridad de Protección de Datos de Francia para que emitiera su autorización formal de manera que se estableciera que la información proporcionada a los clientes era clara, precisa y transparente.

Además de los principios del Foro Económico Mundial, la estrategia de privacidad de Orange incluye otros principios basados en observaciones prácticas:

- Proporcionalidad: el grado de protección depende del tipo de datos personales, los límites y el contenido de lo que se considera privado difieren según las culturas y los mismos individuos, pero se comparten ampliamente algunos aspectos básicos. Todo el mundo admitiría que una imagen médica personal almacenada en una aplicación sanitaria informatizada requiere un mayor nivel de protección que la fotografía de una mascota publicada en una red social. Los individuos son conscientes de dichas distinciones y no adoptarían las nuevas tecnologías, tales como el almacenamiento de imágenes médicas en la nube, si no se tratara y gestionara la privacidad como corresponde.
- Protección de menores: los niños requieren protección especial porque son menos conscientes de los riesgos y las consecuencias del tratamiento de sus datos personales. Desde el 2005, Orange participa en varias iniciativas destinadas a proporcionar las directrices que deben seguir los padres así como información sobre las herramientas disponibles para proteger a sus hijos en la Red. Orange ha desarrollado un sencillo software de control parental[303] gratuito. Recientemente, Orange respondió de forma positiva a la llamada del comisario de la Agenda Digital[304] por la que se solicitaba a la industria la asunción de mayor responsabilidad a la hora de implantar medidas que permitieran que los niños siguieran utilizando sus servicios y equipos de forma segura, y ha contribuido a la creación y firma de los principios sobre TIC.

5.2.3 Orange ofrece servicios que protegen la intimidad

Orange desarrolla soluciones acordes con el nivel de seguridad que exigen las aplicaciones específicas, puesto que un planteamiento responsable por parte de la industria resulta esencial para conseguir la confianza de los individuos. Hace poco, Orange obtuvo una autorización específica[305] del gobierno francés para una aplicación de sanidad digital en la nube basada en una normativa muy estricta. Orange cree que dichas aplicaciones ayudarán a fomentar la confianza en las aplicaciones en la nube.

Durante los cuatro últimos años, Orange Healthcare ha ofrecido soluciones sanitarias digitales mediante la transmisión y alojamiento seguros de información médica para distintos agentes sanitarios. Orange da su importancia a las condiciones de seguridad y privacidad de los datos médicos de sus soluciones digitales de sanidad.

303. http://www.orange.com/sirius/protection_enfants/protectiondesenfants_VA/article_7.html
304. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/703&format=HTML&aged=0&language=EN&guiLanguage=en
305. Art. L. 1111-8 del Código de Sanidad Pública francés.

Un servicio de Orange denominado Imagerie Médicale Partagée permite acceder a imágenes médicas personales almacenadas en la nube. La autorización del gobierno ofrece al cliente la garantía de que su información personal altamente confidencial se está tratando con el mayor respeto a la confidencialidad, seguridad, integridad y control de acceso.

Orange cuenta con varios proyectos relativos a los datos personales de nuestros clientes que brindan la oportunidad de organizar dichos datos desde el punto de vista del cliente, aprovechando la nube para otorgar a los datos personales una dimensión de multidispositivo y poder tratar finalmente los servicios sobre los datos personales desde hogares digitales.

5.2.4 El marco legal de la privacidad necesita mejorarse

En Europa, el debate sobre la revisión de la Directiva de protección de datos ha progresado durante los últimos años, y se han sacado a la luz elementos concretos como los mencionados en las notas de prensa de la Comisión[306]: la armonización y mejor aplicación de la normativa en toda la UE; la transparencia de forma que los ciudadanos sepan exactamente el motivo por el cual se recopilan sus datos; y la equidad, de forma que los ciudadanos no se vean forzados a compartir sus datos. La Comisión se enfrenta al reto de conseguir un equilibrio entre la protección de los ciudadanos y el impacto de la normativa en las empresas, con el fin de evitar un posible impacto negativo sobre los emprendedores e innovadores.

Orange comparte el punto de vista de la Comisión en cuanto a que la aplicación de la Directiva de protección de datos a empresas extracomunitarias que buscan clientes europeos no resulta satisfactoria hoy día: la normativa sobre protección de datos funcionará solamente si se hace cumplir. Es más, la diversidad de normas nacionales sobre privacidad ha dado lugar a una situación compleja e insostenible tanto para los individuos como para las empresas europeas. El objetivo general de la revisión de la Directiva de protección de datos debería consistir en crear una situación de igualdad de condiciones real para todos los agentes del ecosistema de Internet, incluyendo a los agentes *Over the Top* puros de Internet, así como en conseguir una armonización real de las normas en toda la UE. El lema debería ser: «Mismo servicio, mismos usuarios, mismas normas», independientemente de la ubicación geográfica del proveedor de servicios.

La protección de la privacidad de los europeos solo podrá garantizarse si se logra un verdadero mercado interno de protección de la privacidad y los datos. Tal y como ha mencionado la industria en varias ocasiones, aumentar la armonización de las leyes nacionales de los Estados miembros es un propósito fundamental de esta revisión.

Sin embargo, una normativa estricta sobre el consentimiento no sería apropiada para los servicios *online*: la privacidad es un problema contextual que exige unos mecanismos de aplicación flexibles. La aplicación rigurosa de una normativa sobre consentimiento inequívoca hubiera podido evitar la explotación comercial de los directorios telefónicos. Las personas necesitan tomar decisiones contextuales sencillas e informadas, y no verse obligadas a tratar con mecanismos que exigen su consentimiento de manera sistemática. El consentimiento explícito debe seguir siendo excepcional y limitarse a datos personales de alta confidencialidad, como la información sobre la salud, religión u orientación sexual de las personas.

306. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1462

Se deberían proteger los datos cuando se envíen a otro país por medio de cargas proporcionales y procedimientos eficientes. Los esfuerzos deberían centrarse en reducir la complejidad y los costes asociados a la normativa actual para la transmisión de datos a nivel internacional. En concreto, en situaciones complejas como la del *cloud computing*, donde múltiples responsables y encargados del tratamiento operan en diversos países, las estrictas estipulaciones actuales de la Directiva de protección de datos podrían afectar de manera negativa a las empresas europeas.

Los individuos necesitan comprender las implicaciones de la privacidad cuando pretendan publicar y compartir su información personal *online*. La capacidad de controlar sus datos está directamente relacionada con su conciencia sobre la normativa en materia de privacidad: la formación es, evidentemente, el factor clave que permite a los individuos protegerse a sí mismos. La normativa sobre protección de datos no será efectiva si los sujetos registrados no son conscientes de cuáles son sus derechos y, por tanto, no se encuentran en posición de asumir su parte de responsabilidad.

5.2.5 Conclusión

La relación entre los proveedores de servicios y los clientes debería basarse en principios compartidos a nivel global, como los que propone el Foro Económico Mundial.

Orange, dado su papel clave en la prestación de diversos servicios *online* sobre protección de datos, desde los servicios de alta seguridad hasta las innovaciones responsables para los mercados de masas, cree que el tratamiento de datos personales es esencial para proporcionar eficiencia y calidad a la economía de los servicios *online*.

La revisión de la Directiva de protección de datos brinda una oportunidad excelente para mejorar la legislación sobre privacidad y así proporcionar una protección mejorada a los europeos y garantizar una certeza jurídica a las empresas. La capacidad de Europa a la hora de permitir un desarrollo sólido del tratamiento seguro de los datos personales por parte de los servicios *online* es un elemento clave para su futuro económico. El alcance global de los servicios de Internet exige un marco legal convergente.

Brendon Lynch

Brendon Lynch es el director general de Privacidad en Microsoft Corp., donde ha estado los últimos seis años. Es responsable del enfoque de todos los aspectos de privacidad de Microsoft, incluyendo la creación de políticas de privacidad y su implementación en la compañía; su ámbito abarca la creación de tecnologías de protección de datos y privacidad para los consumidores y la supervisión de la comunicación y los compromisos con el público exterior.

Antes de unirse a Microsoft, Lynch lideró la Privacidad y Solución de Riesgos en los Negocios en Watchfire (ahora parte de IBM), proveedor de seguridad en páginas web, privacidad, y creador de software accesible y de calidad. Antes de entrar en la industria del software en 2002, pasó nueve años en Europa y Norteamérica trabajando en PricewaterhouseCoopers, donde prestaba servicios de consultoría, en relación con privacidad y gestión de riesgos. Lynch ha sido miembro del Consejo de certificación de la Asociación Internacional de Profesionales de la Privacidad (IAPP) desde que se fundó y es un profesional certificado de esta asociación.

Lynch es licenciado en Sistemas de información de empresas por la Universidad de Waikato, en su país de nacimiento, Nueva Zelanda.

5.3 Microsoft: los desafíos de privacidad del *cloud computing* global y el Office 365 de Microsoft

Brendon Lynch
Director general de privacidad en Microsoft Corp.

5.3.1 *Cloud computing*: desafíos

El *cloud computing* ha evolucionado rápidamente desde su situación de servicio de nicho a una alternativa popular al modelo tradicional de uso del software y almacenamiento de datos en instalaciones o equipos personales.

El *cloud computing* proporciona un acceso escalable y a medida a una amplia gama de aplicaciones, servicios *online* y de almacenamiento. Como resultado, tanto las empresas globales como los emprendedores acuden a la nube con el fin de acelerar la innovación, lanzar nuevos negocios y recortar los costes. Las agencias del gobierno, los proveedores de servicios públicos y las instituciones de enseñanza están migrando a la nube para poder servir mejor a sus usuarios y reducir el gasto informático, especialmente como respuesta a la reducción de presupuestos.

Sin embargo, el *cloud computing* también plantea muchos e importantes desafíos a la privacidad. Según el modelo tradicional de tecnologías de la información, las organizaciones son responsables de todos los aspectos de la protección de datos, desde la forma en que usan la información personal hasta cómo almacenan y protegen los datos en sus propios ordenadores. No ocurre así con el *cloud computing*, pues la información suele circular fuera del origen y se remite a centros de datos que poseen y gestionan los proveedores de la nube. Este hecho plantea diversas dudas en torno a la responsabilidad sobre la protección de los datos.

La naturaleza global de muchos servicios en la nube también supone un desafío. Por ejemplo, en un paradigma en la nube, los datos creados en Francia que usen software alojado en Irlanda podrían almacenarse en Países Bajos y accederse desde EE. UU. Dicha complejidad geográfica plantea muchas cuestiones sobre la soberanía de los datos; ¿quieren saber los reguladores y los clientes de la nube quién podría acceder a sus datos en la nube y bajo qué circunstancias?

Otra consideración política importante es la segregación de los datos. En los servicios «públicos» de *cloud computing*, los datos de clientes múltiples se almacenan y procesan en la misma ubicación física y, a menudo, en los mismos servidores. Por tanto, los proveedores de la nube deben tomar las medidas necesarias para segregar a nivel lógico todos esos datos y protegerlos contra cualquier uso inapropiado o pérdida, además de restringir y controlar el acceso a la información por parte de sus empleados y suministradores.

Un aspecto importante del modo en que pueden ayudar los proveedores de la nube a atajar muchas de estas cuestiones es ofrecer una mayor transparencia. Los proveedores de la nube pueden crear confianza comunicándose de forma clara con los clientes y reguladores en cuanto a la forma en que se utilizan y reutilizan sus datos, y proporcionando información sobre sus planteamientos relativos al acceso, compartición y almacenamiento de estos.

5.3.2 El planteamiento de Microsoft sobre el *cloud computing*: el ejemplo del Office 365

Microsoft entiende que la protección estricta de la intimidad es esencial para poder generar confianza en el *cloud computing* y permitir que este servicio emergente exprima todo su potencial. Ha invertido en la creación de sistemas y centros de datos sensibles a la privacidad y que ayuden a proteger la intimidad del individuo, desde el desarrollo de software hasta la entrega del servicio, operaciones y asistencia.

Microsoft ofrece varios productos basados en la nube, incluyendo el Office 365, que reúne el software de correo electrónico y colaboración con funciones de almacenamiento y tratamiento escalables. Dado que Microsoft sabe que la privacidad y la seguridad son importantes para los clientes de la nube, el Office 365 (lanzando en junio de 2011) se creó desde su base teniendo en cuenta una sólida protección de los datos.

Microsoft ofrece a los clientes del Office 365 información que define la forma en que gestionan y utilizan los datos de clientes. Funciona desde una sencilla perspectiva, que consiste en utilizar los datos principales del cliente tan solo para el mantenimiento, prestación y seguridad de los servicios del Office 365: los servicios por los que paga el cliente.

A través del Centro de Confianza del Office 365, Microsoft proporciona a sus clientes los recursos necesarios que les ayudarán a comprender las políticas y las prácticas sobre protección de datos del servicio. Por ejemplo, los clientes que desean saber dónde almacena el servicio los datos pueden acceder a las páginas de «Fronteras geográficas» del Centro de Confianza, donde podrán encontrar la información sobre la circulación de los datos entre los centros de datos primarios y los de respaldo, además de otros detalles sobre el proceso de asignación de la ubicación primaria de almacenamiento de datos para cada cliente. En la página «Terceros» del Centro de Confianza del Office 365, Microsoft identifica además a los subcontratistas que pueden acceder a los datos del cliente y las circunstancias en que pueden hacerlo.

Para proporcionar un mayor ahorro y eficiencia al cliente, Microsoft ofrece una versión pública en la nube «multiarrendamiento» del Office 365 que consolida los datos de clientes múltiples en centros regionales de datos. Microsoft no escatima en recursos para garantizar que estos despliegues públicos en la nube del Office 365 no solo fomenten la privacidad y la seguridad, sino que también separen el almacenamiento y tratamiento de datos a nivel logístico entre las cuentas.

El Office 365 ayuda además a los clientes a rastrear el acceso a sus datos principales. Microsoft conserva un registro de accesos a cada uno de los componentes del Office 365 (desde SharePoint Online hasta Exchange Online), que están disponibles para los clientes previa solicitud. Además, la empresa, junto con otras entidades externas, realiza auditorías con el fin de confirmar que solo se accede a los datos para los fines comerciales correspondientes.

Para poder dar cabida a las particulares exigencias sobre protección de datos de la legislación europea, Office 365 ofrece, además, la oportunidad a los clientes que cuenten con usuarios europeos de formalizar acuerdos de tratamiento de datos con las cláusulas contractuales estándares publicadas por la Comi-

sión Europea. La predisposición de Microsoft a la hora de firmar estos acuerdos significa que esta empresa garantiza por contrato que Office 365 cumple con los requisitos sobre privacidad y seguridad establecidos en las cláusulas modelo.

Office 365 se diseñó teniendo en cuenta los desafíos que presenta el *cloud computing*. Microsoft entiende que, a menos que se muestre receptiva a las dudas de los clientes y reguladores en relación con la protección de los datos en las nubes públicas, no se ganará la confianza necesaria para que sus servicios en la nube puedan cubrir las necesidades de sus clientes.

5.3.3 En qué manera pueden colaborar la industria y el gobierno con el fin de aprovechar el potencial del *cloud computing*

El *cloud computing* ofrece tanto a las empresas como a las personas las ventajas de un mayor poder de elección, más flexibilidad y ahorro de costes. Los reguladores y legisladores de todo el mundo pueden ayudar a exprimir todo el potencial del *cloud computing* mediante la resolución de incertidumbres jurídicas, jurisdiccionales y reglamentarias en torno a la tecnología.

Para poder desarrollar la eficiencia de los servicios en la nube y ofrecer el rendimiento y la fiabilidad que esperan los clientes, los proveedores de la nube deben ser capaces de gestionar los centros de datos en múltiples ubicaciones y de transferir los datos entre ellos. La circulación libre de los datos permite a los proveedores de la nube maximizar la eficiencia y ofrecer un mayor rendimiento y fiabilidad. Las ventajas tecnológicas del *cloud computing* están limitadas por la normativa que restringe las transmisiones de datos transfronterizas, o bien crean cierta inseguridad al no articular claramente las normas que se aplican a dichas transmisiones.

Además, las obligaciones jurídicas contradictorias siguen restringiendo los servicios de *cloud computing* así como su asimilación. Las distintas normas sobre privacidad, mantenimiento de datos y otras cuestiones han creado ambigüedades y otros problemas jurídicos de importancia.

Microsoft apoya las iniciativas que faciliten el flujo de información, fomenten la confianza y estimulen la innovación. Mientras aumentan los flujos globales de datos, nosotros abogamos firmemente por una mayor armonización e interoperabilidad de la normativa, políticas y estándares sobre privacidad a nivel mundial.

A la vez que los gobiernos desarrollan políticas destinadas a resolver los problemas de privacidad y seguridad asociados a tecnologías emergentes tales como el *cloud computing*, también deberían preservar su apoyo a la innovación y adopción tecnológicas. Colaborando, el gobierno y la industria pueden llegar a crear los principios apropiados en materia de privacidad que sustenten la protección de los datos en la nube.

Francesco Nonno

Francesco Nonno es director de Privacidad, Antimonopolio y Asistencia al Cliente de Telecom Italia. Con una licenciatura en Económicas, la experiencia laboral de Francesco comprende un largo período en el que trabajó como asesor para empresas de telecomunicaciones y una importante experiencia en la Autoridad Nacional de Reglamentación, donde ocupó varios cargos.

Stefano Tagliabue

Stefano Tagliabue trabaja en el Departamento de Privacidad de Telecom Italia y cuenta con años de experiencia en la gestión de cuestiones de privacidad y seguridad en la industria de las telecomunicaciones. Además, tiene experiencia en sistemas de auditoría y gestión medioambiental de las tecnologías de la información, y es auditor certificado de sistemas de la información (CISA) y un profesional certificado en materia de seguridad de los sistemas de información (CISSP).

5.4 Telecom Italia: el *cloud computing* exige un nuevo enfoque legislativo

Francesco Nonno
Director de Privacidad, Antimonopolio y Asistencia al Cliente de Telecom Italia

Stefano Tagliabue
Miembro del Departamento de Privacidad de Telecom Italia

El *cloud computing* constituye una innovación que está transformando la industria y la forma en que los consumidores y las empresas gestionan sus datos. Concede a los consumidores la oportunidad de almacenar sus datos de manera económica dentro de un espacio virtual al que puede accederse a través de cualquier equipo del usuario. Las empresas también pueden hacer uso del *cloud computing* para servicios esenciales para su misión con el fin de incrementar su flexibilidad y reducir los gastos fijos.

La adopción del *cloud computing* y sus servicios relacionados está superando un veloz proceso de aceleración entre las empresas: en el mundo entero, IDC calcula que este mercado alcanzará un valor notable de casi 40.000 millones de euros para el 2014. Los mercados más maduros, los de Norteamérica y Europa, representan la mayor cuota de mercado, y se espera que el de Europa occidental en concreto crezca con mayor rapidez, con una tasa de crecimiento compuesto anual entre 2010 y 2014 del 34,6 %, en comparación con el aumento global estimado, situado en el 25,8 %. Esto significa que Europa, que sumaba en 2010 el 25,8 % del mercado mundial, alcanzará el 31,4 % en 2014.

En el mercado italiano, es posible detectar la diferencia entre los planteamientos de los servicios en la nube de las pequeñas y medianas empresas (pyme) y los de las grandes empresas. Las pymes suelen estar más interesadas en las soluciones de software como servicio (SaaS), principalmente debido a que no requieren adaptaciones complejas del software y no cuentan con las destrezas técnicas adecuadas para desarrollar sus propias aplicaciones. Por el contrario, el componente de servicios de infraestructura predomina en el mercado de las grandes empresas, que suelen necesitar aplicaciones personalizadas y cuentan con gran capacidad técnica. En cualquier caso, muchos estudios recientes coinciden en predecir un crecimiento sostenido de los servicios de la nube en Italia.

Dicho en pocas palabras, las diversas ventajas del *cloud computing* incrementan el atractivo de esta tecnología a ojos de las empresas que desean acelerar la prestación de sus servicios y mejorar la eficiencia de sus servicios informáticos. No obstante, los servicios *cloud* no solo ofrecen numerosas ventajas, sino que también implican nuevos desafíos para la privacidad y la seguridad que exigen nuevos plan-

teamientos y actitudes a todas las partes implicadas: los proveedores de servicios, los clientes y las autoridades reguladoras.

El marco regulador cumple un papel esencial a la hora de permitir que todas las oportunidades sociales y económicas asociadas al *cloud computing* puedan prosperar, y los legisladores deberían evaluar la forma en que la normativa actual y futura, en un amplio espectro de sectores, podría afectar al desarrollo de los servicios en la nube. No es tarea fácil, pues la rápida evolución de la tecnología y los modelos empresariales plantea dudas con respecto al tipo de servicios, la estructura de precios, la calidad de los servicios y las soluciones técnicas que mejor cubran las necesidades de los clientes.

Por ello es importante que, con el fin de no restringir el potencial del *cloud computing*, las acciones políticas no se trasladen en regulación prematura. Es más, puesto que la tecnología y las aplicaciones del *cloud computing* evolucionan con gran velocidad, las políticas reguladoras deben ser lo suficientemente flexibles y adaptables para permitir soluciones técnicas y de mercado innovadoras.

También es cierto que, ya que la difusión del *cloud computing* promoverá en gran medida las transmisiones internacionales de datos, su éxito depende también de la circulación libre y segura de los datos a través de las fronteras nacionales. Los servicios en la nube tan solo conseguirán desplegar todo su potencial de desarrollo económico y social si se crea un entorno seguro y fiable para todos, tanto para las personas como para las empresas. La conformidad, la transparencia, la confianza y la responsabilidad, al igual que una infraestructura fiable, son esenciales a este respecto.

De ello se desprende que la protección y la seguridad de los datos son algo clave a la hora de debatir las políticas sobre el *cloud computing*, y que deben tratarse a nivel global. Los consumidores aceptarán de buena gana los servicios en la nube si pueden estar seguros de que sus datos personales están protegidos de la misma forma por toda la UE y a escala internacional.

La normativa actual para las infraestructuras informáticas no se creó teniendo en cuenta los nuevos escenarios creados por las tecnologías de la virtualización. Hoy día, muchas de las directrices industriales se derivan de la tecnología, que se está convirtiendo cada vez más en el motor impulsor de estos tipos de servicios. En este momento, no existe un conjunto de normas reconocido a nivel internacional en materia de tratamiento de datos dentro del ciberespacio, incluso a pesar de que la Comunidad Europea y los grupos de trabajo internacionales están trabajando en la definición de las normas sobre infraestructura y seguridad del mercado de los servicios en la nube.

Es más, dada su naturaleza técnica, el *cloud computing* no está limitado por fronteras nacionales ni legislativas. El marco legislativo actual referente a la privacidad y la seguridad de los datos no proporciona homogeneidad y coherencia a los distintos países ni a nivel internacional ni europeo. Las diferencias en la ubicación geográfica de los datos y en las entidades que participan en actividades de almacenamiento y tratamiento dentro del entorno *cloud* constituyen la base del desequilibrio legislativo que caracteriza los problemas sobre privacidad correspondientes. Por ejemplo, las futuras prescripciones que aporte la Autoridad sobre Privacidad italiana para los servicios en la nube tan solo serán vinculantes dentro de la misma Italia.

Esta normativa nacional podría exigir a los proveedores la aplicación de medidas organizativas, técnicas y sobre seguridad, incluso más estrictas que la misma legislación de otros países, creando pues desequilibrios y posibles desventajas competitivas con los proveedores europeos. De hecho, Europa disfruta de una ventaja obvia sobre otras regiones, pues cuenta con un Sistema de Protección de Datos centrado en el interés de los ciudadanos europeos;

no obstante, este no debería imponer restricciones excesivas a los proveedores europeos. El desequilibrio regulador podría provocar, tanto para los proveedores europeos existentes como para los futuros, un incremento de gastos y del plazo de entrada al mercado de los servicios en la nube, generando, pues, una desventaja competitiva en términos de gastos –tanto de establecimiento como gastos periódicos del servicio–. Finalmente, esta situación podría causar el desplazamiento de una porción importante del mercado nacional hacia otros proveedores que no estén sujetos a estas normas, lo cual conduciría paradójicamente, al contrario de lo esperado por las autoridades reguladoras, a un nivel de protección inferior de las empresas europeas que, en su calidad de responsables del tratamiento, confiarían los datos personales a dichos proveedores.

Cabe mencionar que, si se echa un vistazo al uso del *cloud computing*, puede percibirse una diferencia relevante entre las aplicaciones de las empresas y las de los consumidores. Las empresas recurren al *cloud* para gestionar sus datos y aplicaciones, que a menudo incluyen los datos de sus clientes (de los cuales son responsables del tratamiento), mientras que los consumidores suelen utilizar los servicios de la nube para almacenar sus propios datos junto con datos relativos a sus relaciones.

Los distintos usos plantean diferentes cuestiones que deben tratarse por separado.

Si nos centramos en los servicios *cloud* para el mercado comercial (servicios de la nube para empresas y el sector público), para poder superar este desequilibrio regulador, las próximas directrices legislativas de la UE deberían ocuparse, en primer lugar, de los responsables del tratamiento, es decir, de las empresas que usan estos servicios independientemente del proveedor escogido y del país donde se procesen los datos. De hecho, el responsable del tratamiento de los datos personales está obligado por ley a adoptar (y asegurarse de que sus proveedores de servicios subcontratados adopten) las medidas organizativas y de seguridad apropiadas para la protección de los datos personales, además de las medidas de seguridad mínimas que prescribe la ley.

Puesto que las condiciones de servicio, la política de privacidad y las ubicaciones escogidas por los proveedores de servicios en la nube podrían afectar significativamente a los intereses de los usuarios finales en materia de privacidad y confidencialidad, el cliente (el responsables del tratamiento de los datos) debería verificar la fiabilidad del proveedor de servicios y sus socios además de si cumplen con estos requisitos antes de confiar el tratamiento de los datos a un tercero.

Según esto, unas directrices vinculantes que prescriban un conjunto común de medidas a aplicar por parte de todos los responsables de los tratamientos que deseen hacer uso de estos servicios deberían:

- eximir a los responsables del tratamiento de la ardua obligación de identificar las medidas a adoptar, considerado que la mayoría de los responsables de los tratamientos de datos personales que recurren a los servicios de *cloud computing* buscan además una forma de simplificar el uso de las tecnologías de la información y puede que no cuenten con las destrezas necesarias para efectuar un análisis de riesgos;
- crear los criterios de obligado cumplimiento a adoptar sin someterse a negociaciones técnicas y comerciales en las que los responsables de los datos individuales no tendrían: a) la fortaleza para comparar los proveedores de servicios y poder exigir los requisitos técnicos concretos, ni b) la motivación económica para solicitar la personalización de los servicios estándares ofertados;
- imponer de forma indirecta las medidas adecuadas de tratamiento de datos que se respeten con independencia del proveedor escogido de los servicios de *cloud*

computing, pues esta obligación se transferiría al proveedor a través de los contratos de servicios;
- crear un conjunto común de normas que aplicar por parte de todos los proveedores de servicios que deseen operar en el mercado (nacional/europeo) relevante, independientemente de la nacionalidad de la sede social o de sus centros de datos;
- definir un conjunto de normas que no cree un desequilibrio en el mercado.

Según la Autoridad de Protección de Datos italiana, una gestión de contratos adecuada y precisa podría apoyar al usuario y al proveedor a la hora de definir los procedimientos y parámetros operativos para la evaluación del servicio, aparte de identificar las medidas de seguridad a adoptar. Sin embargo, es importante evaluar la idoneidad de las condiciones contractuales para la prestación del servicio en la nube en relación con las obligaciones y responsabilidades en caso de pérdida de los datos almacenados en la nube así como las consecuencias del cambio a otro proveedor.

Bajo esta perspectiva, los contratos de nivel de servicios (SLA, del inglés *Service Level Agreement*) para los servicios en la nube deberían contemplar la adopción de las medidas anteriormente mencionadas. Esto podría conseguirse mediante:

- la predisposición del proveedor a la hora de superar auditorías por parte del responsable del tratamiento de los datos;
- la certificación de los servicios de la nube prestados por cada proveedor, emitida por una entidad externa independiente;
- la certificación de la infraestructura *cloud* por parte del proveedor, que permita y garantice el nivel de aplicación del servicio de la nube (plataforma como servicio, aplicación como servicio), también cuando lo preste un socio del proveedor.

Las medidas físicas e informáticas de seguridad deberían aplicarse basándose en este modelo, incluyendo la adopción de modelos específicos de SLA. Deberían diseñarse las medidas de seguridad informática apropiadas para los sistemas de registros de auditorías, aparte de protocolos de comunicación segura, separación lógica de los datos pertenecientes a distintos clientes y protección perimetral de componentes de red, de almacenamiento y de tratamiento de datos. La seguridad física debería abarcar las cuestiones derivadas de los controles de acceso físico (al registrar cada acceso) y de los controles ambientales (por ejemplo, el suministro eléctrico ininterrumpido, los sistemas de prevención de incendios, etcétera.).

En nuestra opinión, el responsable del tratamiento de los datos debería solicitar cláusulas contractuales que contemplaran:

- su derecho a efectuar actividades de auditoría;
- una declaración de conformidad por parte del proveedor;
- la definición de una política de gestión de datos por parte del proveedor.

Por último, los proveedores deberían contar con una política definida y un marco de gestión del riesgo informático y de las reclamaciones gubernamentales que incluya las normas actuales y prácticas de excelencia con el fin de garantizar:
- análisis regulares de riesgos;
- una definición de las políticas y directrices;
- la identificación de medidas técnicas y organizativas;
- auditorías y controles.

Pero otro panorama surge si se observan los servicios de la nube para el mercado de consumo, que incluyen, por ejemplo, el almacenamiento y distribución de archivos multimedia, y que ofrecen a menudo servicios de redes sociales al mismo tiempo.

De estos servicios se derivan varios problemas relativos a la privacidad. ¿Cómo garantizar un entorno seguro para los niños y menores sin restringir su acceso al espectro completo de servicios de la nube y sus redes sociales? ¿Tienen los suscriptores el derecho a procesar los datos relacionados con terceros tales como imágenes de amigos o familiares? ¿Es realmente posible aplicar el «derecho al olvido» cuando el cliente opta por cancelar su suscripción a un servicio? Estas son solamente unas cuantas dudas que se deben tener en cuenta. Pero, además, la posible creación de perfiles de los clientes para fines comerciales y publicitarios plantea otras cuestiones de importancia que afectan a la forma en que podría equilibrarse mejor el derecho de las personas a controlar sus datos personales y las ventajas de recibir publicidad relacionada con sus intereses y preferencias.

Desde estas perspectivas, puede comprobarse que, en el caso de los servicios de la nube para el mercado de consumo, el marco regulador podría considerar al consumidor de servicios de la nube como una persona a quien debe proteger la ley y no como el receptor de obligaciones y requisitos. Por tanto, la ley debería proporcionar un conjunto de normas básicas que deberían respetar todos los operarios, independientemente de su nacionalidad o de la tecnología que usen.

Y lo cierto es que la normativa europea sobre privacidad está evolucionando hacia esta dirección. La propuesta reciente del Reglamento general de protección de datos europeo afirma de forma explícita que «el tratamiento de datos personales está al servicio del hombre; los principios y normas relativos a la protección de las personas en lo que respecta al tratamiento de sus datos de carácter personal debe, cualquiera que sea la nacionalidad o residencia de las personas físicas, respetar las libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal». En consecuencia, la UE propone que este Reglamento debería aplicarse al tratamiento de los datos personales de sujetos registrados que residan en la UE por parte de responsables del tratamiento que no residan en ella, en especial cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios o el control de la conducta del consumidor.

Carlos López Blanco

Carlos López Blanco, nacido en Valladolid en 1959, es licenciado en Derecho por la Universidad de Valladolid, diplomado en Alta Dirección de Empresas por el IESE y abogado del Estado. Durante los años 1984 a 1989 prestó servicios como abogado del Estado en la Administración en el País Vasco y los ministerios de Educación, Justicia y Economía y Hacienda. En 1989 pasó al sector empresarial desempeñando la Secretaría del Consejo de Administración de Construcciones Aeronáuticas. En 1992 fue nombrado para el mismo cargo en IBM España y desde 1995 al 2001 ocupó la Secretaría General de Airtel, después convertida en Vodafone España. Del 2002 a 2004 fue secretario de Estado de Telecomunicaciones y para la Sociedad de la Información. Del 2004 a 2007 ha sido presidente de ENTER, Centro de Análisis de la Sociedad de la Información y las Telecomunicaciones del Instituto de Empresa y consejero de Ericsson España e Ydilo, y consejero asesor de INDRA. En la actualidad es director de la Oficina Internacional de Telefónica. Forma parte de la Fundación IDATE y del Consejo Científico del Real Instituto Elcano.

5.5 Telefónica: la visión de Telefónica sobre la privacidad

Carlos López Blanco
Director de la Oficina Internacional de Telefónica

Telefónica se fundó en 1924 como una subsidiaria de la multinacional americana ITT (International Telephone and Telegraph). Desde entonces, la sociedad no ha parado de evolucionar hasta convertirse en uno de los principales operadores de telecomunicaciones integradas del mundo, que ofrece soluciones para las comunicaciones, la información y el ocio.

Telefónica cuenta con uno de los perfiles más internacionales del sector. Más del 60 % de la actividad de la empresa se lleva a cabo fuera de su mercado nacional. Telefónica opera en veinticinco países de Europa, Latinoamérica y China. En Europa, Telefónica ha conseguido una escala relevante de más de 105 millones de accesos totales, prestando servicios a más de 57,8 millones de clientes.

La anticipación y la transformación ha sido nuestro su principal. Hoy día, y más que nunca, ambos rasgos caracterizan a la empresa.

La sociedad de la información en la actualidad se basa en el tratamiento de la información, que a menudo suele ser de carácter personal. Cada día se genera, procesa, almacena y transfiere una cantidad ingente de datos personales a través de una diversidad de equipos, servicios y plataformas interconectadas en aumento.

En este contexto, en el 2009, la Comisión Europea inició un proceso destinado a analizar el marco legal actual de protección de los datos de carácter personal de la Unión Europea, en concreto a la luz de las nuevas tecnologías y la globalización. Telefónica ha acogido este hecho de buena gana, pues muchos de los aspectos de la Directiva de 1995 en vigor ya no sirven a los fines que se pretendían. Sin embargo, la base de la creación de la Directiva sigue siendo válida.

Tal y como se confirma en los considerandos de la propuesta de Reglamento (y su predecesora, la Directiva), el tratamiento de los datos personales debe servir al hombre, debería respetar los derechos y libertades fundamentales de los individuos, en particular el derecho a la privacidad, y debería contribuir a la evolución económica y social, a la consolidación y convergencia de las economías dentro del mercado interno y al bienestar de los individuos.

Telefónica no podría estar más de acuerdo con esta afirmación. Por tanto, el principal resultado del análisis efectuado debería ser la efectividad en la práctica, la reducción de divergencias dentro del mercado interior y la flexibilidad a la hora de adaptarse a los entornos dinámicos.

El análisis debería producir un marco sobre privacidad tecnológicamente neutro, a prueba de futuro, y centrado en el usuario que fomente la innovación en el uso de la informa-

ción, la tecnología y los modelos empresariales, y que permita a los usuarios ser conscientes y gestionar su privacidad.

Los ciudadanos y los consumidores exigen nuevos servicios basados en una mayor personalización y una movilidad incrementada de los datos de carácter personal, tales como las aplicaciones de administración y sanidad electrónicas, los servicios de información personalizados o la publicidad dirigida que se adecue a sus intereses. Telefónica está en vías de desarrollar varios servicios nuevos en respuesta a las expectativas de los clientes y destinados a mejorar su calidad de vida, además de salvaguardar su intimidad.

Telefónica cree que una «buena» Ley sobre protección de datos a prueba de futuro no debería impedir, sino más bien fomentar el desarrollo de los nuevos servicios y promover el crecimiento económico y el bienestar social.

Fingiendo por un momento que somos los legisladores europeos y que debemos redactar una «buena» Ley sobre protección de datos, la Ley deberá abordar necesariamente las siguientes cuestiones.

1. Para empezar, el primer elemento sería conseguir una armonización total dentro de los Estados miembros con el fin de garantizar que la protección de datos no se emplee erróneamente como excusa para restringir la libre circulación de los datos personales dentro de la UE.

La armonización incita a la creación de soluciones económicamente eficientes por parte de los proveedores de servicios globales y europeos, pero no solo tiene importancia para los agentes económicos, sino también para los ciudadanos: las divergencias dan lugar a una incertidumbre jurídica que afecta a los responsables del tratamiento de los datos y los sujetos registrados por igual, pues podrían no recibir el mismo nivel de protección en los distintos Estados miembros.

Para conseguir esta armonización, el Reglamento parece ser el instrumento legal adecuado. No obstante, no debería permitirse a los Estados miembros que «completaran» el Reglamento, que es aplicable directamente a nivel nacional, añadiendo otra legislación que se ocupe de cuestiones específicas bajo la «excusa» de que no son elementos esenciales de la Ley. Tan solo se conseguirá la armonización si se trata de un Reglamento *de maximis* y los Estados miembros no desarrollan otra normativa adicional.

2. El segundo elemento clave consistiría en conseguir una situación de igualdad de condiciones real para así poder garantizar unos principios tecnológicamente neutrales de aplicación a todos los responsables del tratamiento de los datos.

En el mundo convergente actual, las distorsiones entre los sectores no son justificables y resultan perjudiciales para el ciudadano. Este debería disfrutar del mismo nivel de protección de sus datos de carácter personal, independientemente del sector económico del proveedor de servicios.

En la actualidad, los servicios basados en GPS están sometidos a normas distintas que los servicios basados en ubicaciones geográficas proporcionados por los operadores de telefonía móvil, incluso aunque desde el punto de vista del consumidor ambos servicios sean sustituibles.

Hoy día no es justificable la existencia de legislación específica de un sector, como la Directiva sobre la privacidad y las comunicaciones electrónicas destinada a esa área. El futuro Reglamento no debería regular teniendo en mente tecnologías concretas que podrían quedarse obsoletas rápidamente, sino que debería contar con una naturaleza tecnológicamente neutral que garantice un marco legal a prueba de futuro.

La situación de igualdad de condiciones real podría, además, evitar distorsiones com-

petitivas entre los agentes económicos y situaciones complejas que confundan a los clientes más que protegerlos.

3. El tercer elemento sería el reconocimiento de las distintas normas sobre privacidad en el mundo entero.

Puesto que la Unión Europea no está aislada, incluso aunque se consiguiera contar con la mejor legislación sobre protección de datos más allá de cualquier frontera geográfica, tal hecho no tendría por qué implicar necesariamente que los ciudadanos europeos y su derecho a la intimidad estuvieran totalmente protegidos.

En la era de Internet, las fronteras geográficas desaparecen, y por ello se requiere una mayor colaboración internacional en pos del consenso global en torno a la privacidad.

El criterio de «ofrecer bienes y servicios a los ciudadanos de la UE» constituye un buen paso a la hora de garantizar que todas las empresas cumplan con la normativa europea sobre protección de datos, que no se hallen en desventaja competitiva frente a empresas extracomunitarias y que los ciudadanos europeos puedan disfrutar del mismo nivel de protección independientemente de la situación geográfica del proveedor de servicios.

Se trata de una solución intermedia, pero a largo plazo deberíamos trabajar todos por el acercamiento de los distintos marcos legales del mundo entero.

Una «buena» Ley sobre protección de datos no debería centrarse en la introducción de diversas obligaciones y derechos nuevos si las primeras no son viables y los últimos no son realistas. No se estaría actuando por el bien de los ciudadanos, que seguirían comerciando sin tener en cuenta los obstáculos legales.

Y es más, la consecución de una mayor coordinación de los ordenamientos de los distintos países y regiones podría ayudar a las empresas a tener cada vez más en cuenta el nivel de protección que solicitan los usuarios finales dentro de sus propias estrategias competitivas, con lo que este sería un incentivo evidente para el cumplimiento de estos niveles.

Unos principios comunes en materia de protección de datos que subrayen los distintos ordenamientos jurídicos contribuirían al desarrollo del comercio mundial y facilitarían el intercambio de información entre los agentes económicos de todo el mundo, dando como resultado último un mayor nivel de protección del derecho fundamental a la intimidad.

Volviendo a la realidad, no es un legislador europeo, pero Telefónica seguirá ejerciendo un papel activo y constructivo en este debate. La protección adecuada de los datos de carácter personal es requisito previo a la participación activa de los ciudadanos europeos en una sociedad de la información verdaderamente global. Y Telefónica está empeñada en hacer que esto ocurra.

Anexos

A. Directiva de protección de datos

La Directiva 95/46/CE, conocida como la Directiva de protección de datos, define los fundamentos de la protección de datos personales que los Estados miembros de la UE tienen que trasladar a su legislación nacional. Las disposiciones de la Directiva pueden ser invocadas en los tribunales nacionales contra las normas de protección de datos de los Estados miembros con el fin de derogar la aplicación de normas contrarias a dichas disposiciones.

La Directiva de protección de datos se aplica a cualquier tratamiento automático de datos personales, así como a cualquier otro manejo de datos personales que formen parte de un sistema de almacenamiento. La Directiva estipula que los Estados miembros deberán asegurar que los datos personales sean recogidos para fines determinados, explícitos y legítimos[307], siendo adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente. El tratamiento de dichos datos se deberá realizar de manera leal y lícita, y se deberán conservar en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Asimismo, la Directiva dispone que la entidad o persona responsable del tratamiento de los datos debe garantizar el cumplimiento de los principios relativos a la calidad de los datos, así como proporcionar a las personas información relativa a la identidad del responsable del tratamiento, los fines del tratamiento de que van a ser objeto los datos, así como otros datos de interés[308]. El Artículo 8 establece una protección reforzada para el uso de datos personales sensibles, por ejemplo, aquellos que corresponden a la salud, vida sexual, creencias religiosas o filosóficas.

Entre las obligaciones adicionales exigibles al responsable del tratamiento de los

307. El Artículo 7 especifica un listado de las razones legítimas para el tratamiento de datos personales, entre los que destacan: a) cuando el interesado dé su consentimiento de forma inequívoca; b) es necesario para la ejecución de un contrato en el que el interesado sea parte; c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; d) es necesario para proteger el interés vital del interesado, y e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público.

308. La Directiva exime de esta obligación de información los casos de tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley.

datos están: a) la obligación de mantener la confidencialidad del tratamiento de los datos (Artículo 16); b) la obligación de implementar las medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción ilegal, la perdida accidental, y contra la alteración, la difusión o el acceso no autorizados, garantizando un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse (Artículo 17); c) la obligación de notificar a la autoridad nacional de control un conjunto de información sobre el tratamiento de los datos previo a su realización (Artículo 18), y d), el establecimiento de controles previos por parte de la autoridad nacional de control al tratamiento de datos que puedan suponer riesgos específicos para los derechos y libertades de los interesados (Artículo 20).

Del lado de los derechos, la Directiva obliga a los Estados miembros a garantizar el cumplimiento de los siguientes derechos de los titulares de los datos: a) derecho de acceso, que incluye el derecho a la confirmación del tratamiento de los datos, así como a recibir información sobre los propósitos del tratamiento (Artículo 12.a); b) derecho de rectificación, borrado o bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva (Artículo 12.b); c) derecho a oponerse a ciertas prácticas de tratamiento o tratamiento de datos (Artículo 14); d) derecho a un recurso judicial en caso de violación de sus derechos (Artículo 22), y e) derecho a recibir una reparación por parte del responsable de datos en casos de perjuicios como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones de la Directiva (Artículo 23).

La Directiva dispone, en su Artículo 28, que los Estados miembros deberán establecer autoridades independientes para el control de las medidas de protección de datos, estando estas dotadas de poderes de investigación e intervención, así como de capacidad procesal en caso de infracciones. Asimismo, el Artículo 29 dispone el establecimiento de un grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales[309], formado por representantes de las autoridades de control, un representante del supervisor europeo de Protección de Datos, y un representante de la Comisión Europea. El Grupo tiene como cometido el estudio de las cuestiones relativas a la aplicación de la Directiva, la emisión de dictámenes y asesoría de la Comisión Europea, así como la formulación de recomendaciones sobre asuntos relacionados con la protección de las personas en lo que respecta al tratamiento de datos personales en la Comunidad.

En el caso de transferencias a terceros países, la Directiva de protección de datos dispone que estas solo se podrán realizar sin necesidad de mayores salvaguardas en los casos en los que dicho país garantice un nivel de protección adecuado[310]. La adecuación de un tercer país a los niveles de garantía exigidos por la UE deberá ser evaluada por la Comisión Europea según el Artículo 25.6 y un proceso de decisión[311]. En di-

309. Denominado Grupo de Trabajo sobre Protección de Datos del Artículo 29 o GT29

310. El apartado 2 del Artículo de la Directiva especifica que «El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración 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».

311. Dicho proceso involucra: a) una propuesta de la Comisión; b) la opinión del Grupo de Trabajo del Artículo 29; c) la opinión del comité establecido según el Artículo 31; d) un plazo de 30 días de escrutinio del Parlamento Europeo para comprobar si la Comisión ha ejercido sus poderes correctamente, y e), la adopción de la decisión.

chos países[312] se podrán producir el intercambio de datos personales sin mayores salvaguardas.

Mientras, las transferencias a países cuyo marco legislativo de protección de datos no se considere adecuado por la UE se podrán producir, si el responsable del tratamiento de los datos dispone las salvaguardas adecuadas para la protección de los mismos. Para ello será necesaria la aceptación de conjunto de cláusulas contractuales diseñadas por la Comisión Europea o de códigos de conducta en el caso de tratarse de una transferencia de datos dentro de una misma empresa multinacional[313]. Finalmente, el Artículo 26 recoge un conjunto de situaciones excepcionales que habilitarían la transferencia de datos personales en casos en los que no se cumplan los requisitos anteriores. En aquellos casos en los que no se cumpla ningún requisito, la transferencia de los datos personales no podrá realizarse.

B. Directiva sobre la privacidad y las comunicaciones electrónicas

La protección de datos en el sector de las telecomunicaciones ha estado regulada desde 1997, además de por la Directiva de protección de datos, por una Directiva específica (Directiva 1997/66/EC de Privacidad de las Telecomunicaciones) que trasladaba los principios de la primera a reglas específicas para el sector de las telecomunicaciones. Dicha Directiva fue reemplazada en el 2002 por la Directiva 2002/58/EC sobre la privacidad y las comunicaciones electrónicas, y enmendada en el 2006 (2006/24/EC) y en el 2009 (2009/136/EC).

La Directiva sobre la privacidad y las comunicaciones electrónicas y sus enmiendas posteriores tienen como objetivos la protección de los datos personales y la privacidad de los usuarios en el contexto de los avances de las tecnologías digitales, Internet, y los servicios de comunicaciones electrónicas fijos y móviles realizados a través de redes públicas de comunicaciones. Las disposiciones de la Directiva se aplican al tratamiento de los datos personales así como a los datos de tráfico y de localización.

En este sentido, la Directiva establece sobre los operadores de telecomunicaciones un conjunto mayor de requisitos de los que se requieren a otros agentes bajo la Directiva de protección de datos. Si bien esto permitió en el pasado una mayor protección de las comunicaciones, la evolución de las tecnologías y la convergencia entre agentes y servicios que se ha desarrollado en Internet, supone hoy en día una diferenciación entre las protecciones realizadas mediante sistemas de telecomunicación clásicos y las efectuadas a través de otros medios como puede ser Internet.

La Directiva establece que los proveedores de servicios de comunicaciones electrónicas deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad[314] y la

312. Las decisiones de la Comisión Europea sobre la idoneidad de la protección de datos personales en terceros países actualmente comprenden a Andorra, Argentina, Australia, Canadá, el Bailiazgo Guernsey, Israel, el Bailiazgo de Jersey, la isla de Man, las islas Feroe, Suiza. En el caso de EE. UU., las empresas pueden suscribirse al Acuerdo de Puerto Seguro (Safe Harbour) para alcanzar los requisitos exigidos por la UE. Se pueden consultar las decisiones sobre la adecuación de la protección de datos en terceros países en: http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

313. Una guía sobre las condiciones para las transferencias de datos personales a terceros países puede encontrarse en: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

314. El Artículo 4 recoge que, «Sin perjuicio de lo dispuesto en la Directiva 95/46/CE, las medidas a que se refiere el apartado 1, como mínimo: garantizarán que solo el personal autorizado tenga acceso a los datos personales para fines autorizados por la ley; protegerán los datos personales almacenados o transmitidos de la destrucción accidental o ilícita, la pérdida o alteración accidentales o el almacenamiento, tratamiento, acceso o revelación no autorizados o ilícitos; y garantizarán la aplicación efectiva de una política de seguridad con respecto al tratamiento de datos personales».

confidencialidad[315] de los servicios y datos personales[316], teniendo las autoridades nacionales competentes la capacidad de examinar las medidas adoptadas.

Entre las obligaciones de los proveedores se encuentra la de prestar información suficiente a los usuarios en relación con los riesgos de seguridad existentes, así como de informar a la autoridad nacional competente en caso de una violación de los datos personales. Si dicha violación pudiese afectar negativamente a la intimidad o datos personales de un usuario, y no se probase la aplicación de medidas de protección tecnológica convenientes, el operador tendrá la obligación de informar asimismo al usuario afectado. Además, la Directiva restringe las comunicaciones no deseadas, como las llamadas automáticas, el envío de mensajes publicitarios, etc. al consentimiento de los usuarios.

La Directiva cubre las situaciones de almacenamiento y tratamiento de datos de tráfico por parte del proveedor del servicio, limitando estas actividades a las necesarias para la prestación del servicio, siendo necesaria la eliminación de aquellos una vez concluido. Estos datos podrán ser utilizados para la promoción comercial de servicios electrónicos, siempre y cuando el usuario haya dado su consentimiento previo, contando en todo momento con la posibilidad de retirar su consentimiento para el tratamiento de estos. Mientras, los datos necesarios para la facturación podrán ser procesados hasta la expiración del plazo durante el cual pueda impugnarse legalmente la factura o exigirse el pago. Por su parte, los datos relacionados con la localización solo podrán procesarse si se hacen anónimos, o previo consentimiento de los usuarios.

Finalmente, la Directiva contempla la limitación de los derechos y obligaciones en tanto sea una medida necesaria, proporcionada y apropiada, en una sociedad democrática, para proteger la seguridad nacional, permitiendo la conservación de datos de comunicaciones por motivos de seguridad.

C. Resumen de la propuesta de Reglamento general de protección de datos

El Reglamento propuesto por la Comisión sustituirá, una vez concluido el proceso legislativo ordinario, a la Directiva de protección de datos y a las transposiciones de esta en los distintos Estados miembros, situándose como el principal mecanismo para afrontar los retos en materia de privacidad derivados del avance de las tecnologías y del proceso de globalización. Para hacer frente a estos retos, la propuesta de Reglamento elaborada por la Comisión incorpora un conjunto de modificaciones respecto a la Directiva actual en materia de principios de protección de datos, derechos de los interesados, obligaciones de los responsables y los encargados del tratamiento de datos, transferencias de datos a terceros países, y sobre el funcionamiento de las autoridades nacionales de protección de datos. No obstante, la evolución del procedimiento legislativo entre el Parlamento y el Consejo podrá variar algunos de los elementos propuestos por la Comisión.

Principios de protección de datos

En relación con los principios de protección de datos, el Reglamento incluye como requisito previo al tratamiento que los interesados den su consentimiento «específico, informado y explícito» (Artículo 4). La obtención del con-

315. El Artículo 5 establece que los Estados miembros deberán garantizar la confidencialidad de las comunicaciones y los datos de tráfico asociados, prohibiendo la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de los mismos, sin el consentimiento de los usuarios interesados.

316. La información almacenada en los terminales de usuario también se encuentra amparada por esta protección.

sentimiento explícito, ya sea mediante una «declaración» o un «acto positivo unívoco» de los interesados, se sitúa como uno de los principales retos para los responsables del tratamiento, que tendrán que lograr que este sea solicitado de forma amigable dentro del proceso de prestación del servicio, cumpliendo asimismo con los requisitos del nuevo Reglamento[317].

Otra de las novedades de la propuesta se refiere al tratamiento de los datos de los niños en servicios de sociedad de la información. A ese respecto, el Artículo 8 especifica que será obligatorio para el tratamiento de los datos personales de niños menores de trece años el consentimiento o autorización de los padres o tutores legales.

La propuesta también aclara, en su Artículo 3, el ámbito de aplicación de la normativa de protección de datos, elemento no resuelto en la actual Directiva. El Reglamento propuesto se aplicará, además de a los responsables y encargados del tratamiento establecidos en la UE, a aquellos negocios no establecidos en Europa que ofrezcan servicios o que monitoricen el comportamiento de individuos en la UE. Estos últimos deberán designar un único representante en la UE establecido en uno de los Estados miembros donde presten sus servicios (Artículo 25). Asimismo, el Reglamento amplía las categorías de datos especiales sometidas a un mayor control para incluir los datos genéticos (Artículo 9).

Derechos de los interesados

La mejora del control que los interesados tienen de sus propios datos personales, tanto en el entorno físico como *online*, es uno de los aspectos que se refuerzan en la propuesta de la Comisión. De esta forma, a los derechos de acceso, rectificación y objeción, se añaden el derecho al olvido, como parte del derecho de supresión (Artículo 17), y el derecho a la portabilidad de los datos (Artículo 18).

El derecho al olvido incluye como obligación adicional a la eliminación de los datos personales y al cese de su publicación (derecho de supresión[318]), que en aquellos casos en los que los datos fueron hechos públicos bajo responsabilidad de sus controladores, estos tomen todos los pasos razonables para informar a terceras partes que estén procesando dichos datos de que el interesado solicita la eliminación de los enlaces, copia o réplica de ellos[319]. El borrado y la posterior aplicación del derecho al olvido se deberá realizar sin retraso, salvo que existan motivos para ello[320].

Por su parte, el derecho de portabilidad garantiza que el interesado pueda recibir una copia de sus datos a través de un medio elec-

317. Que el consentimiento deba ser explícito hará necesario que se especifique el tipo de datos que se van a recoger y procesar, así como el uso de estos. Asimismo, el Artículo 7 especifica que en aquellos casos en los que el consentimiento se proporcione a través de una declaración escrita, se deberá separar el consentimiento para el tratamiento de datos personales de cualquier otro consentimiento recabado, poniendo en duda las prácticas habituales del consentimiento «ómnibus», en las que se recoge en la misma declaración el consentimiento para el tratamiento de datos y para los términos y condiciones de uso o de venta. Además, el Reglamento especifica que será el controlador de los datos quien tenga que aportar la carga de la prueba de dichos consentimientos.

318. Este derecho se activará cuando: los datos no sean necesarios para los objetivos que fueron recogidos; el interesado retire su consentimiento; el interesado ejercite el derecho de objeción, o cuando el tratamiento de los datos no cumpla con el Reglamento por otros motivos.

319. La versión filtrada a finales del 2011 incluía una codificación más exigente del derecho al olvido. En ella, los controladores de los datos eran obligados a eliminar cualquier enlace en Internet, copia o réplica de los datos en lugar de tener que tomar los pasos razonables para notificar la petición de borrado del interesado. Tras la filtración, múltiples agentes avisaron de la imposibilidad de cumplir con dicho requisito, elemento que ha llevado a la racionalización del derecho al olvido por parte de la Comisión.

320. La versión filtrada a finales del 2011 incluía una codificación más exigente del derecho al olvido. En ella, los controladores de los datos eran obligados a eliminar cualquier enlace en Internet, copia o réplica de los datos en lugar de tener que tomar los pasos razonables para notificar la petición de borrado del interesado. Tras la filtración, múltiples agentes avisaron de la imposibilidad de cumplir con dicho requisito, elemento que ha llevado a la racionalización del derecho al olvido por parte de la Comisión.

trónico, o de transferir sus datos personales a otros sistemas de tratamiento automático.

Asimismo, la propuesta de la Comisión introduce obligaciones de transparencia en las políticas y condiciones del tratamiento, obligando al uso de lenguaje claro, sencillo y orientado a los interesados (Artículo 11). Este principio de transparencia se basa en el consenso internacional alcanzado en la resolución de Madrid (véase el apartado Transparencia y consentimiento de los usuarios).

Obligaciones de los responsables y los encargados del tratamiento de datos

En primer lugar, el Artículo 22 de la propuesta de la Comisión obliga al responsable del tratamiento a asumir el principio de responsabilidad (véase en detalle en el apartado Principio de responsabilidad), según el cual este tendrá que adoptar las políticas y las medidas necesarias para garantizar, así como demostrar, que el tratamiento de los datos cumple correctamente con el Reglamento. Asimismo, se introducen como requisitos los principios de privacidad desde el diseño y de privacidad por defecto[321] (Artículo 23).

En segundo lugar, la Comisión propone incrementar las obligaciones para los responsables del tratamiento en los casos de violaciones de los datos personales. En estos casos los responsables del tratamiento deberán notificar el suceso a la Autoridad de Protección de Datos (APD) en menos de 24 horas, y proporcionar una justificación razonable en caso de exceder el plazo temporal (Artículo 31). Asimismo, cuando la violación de los datos personales pueda afectar negativamente a su protección de los datos personales o a la privacidad de algunos interesados, el responsable del tratamiento, tras la notificación a la APD, deberá comunicar la situación a aquellos. Esta comunicación podrá omitirse si el responsable del tratamiento demuestra a la APD que se han implementado las medidas técnicas necesarias para que dichos datos sean ininteligibles (Artículo 32). Estas obligaciones, hasta ahora solo requeridas para los operadores de telecomunicación sometidos a la Directiva sobre la privacidad y las comunicaciones electrónicas, se amplían mediante la propuesta de Reglamento al resto de agentes.

En tercer lugar, la propuesta de Reglamento elimina la obligación, impuesta sobre los responsables del tratamiento, de notificar a las APD antes de llevar a cabo un tratamiento automático. Sin embargo, la propuesta incluye la obligación para los responsables y encargados del tratamiento de realizar análisis de impacto sobre aquellos procesos que puedan entrañar riesgos específicos para los derechos y libertades de los interesados (Artículo 33). En aquellos casos en que el análisis de impacto determine la existencia de un riesgo, o las APD lo consideren necesario por este motivo, los responsables y los encargados del tratamiento deberán notificar y solicitar la autorización previa de las APD para proceder al tratamiento de los datos personales (Artículo 34). Por tanto, la propuesta de la Comisión elimina un conjunto de trabas administrativas, pero al mismo tiempo incluye otras adicionales, que en este caso se amplían también a los encargados del tratamiento de datos.

Finalmente, el Artículo 35 impone la obligación a los responsables y los encargados del tratamiento de designar un delegado de protección de datos[322] en aquellos casos en los que el tratamiento sea realizado por entidades públicas, por compañías de más de 250 empleados o en empresas cuyas actividades

321. Esto significa que las salvaguardas para la protección de datos deberán incorporarse en los productos y servicios desde las primeras fases de diseño y desarrollo, así como que las configuraciones respetuosas con la privacidad deberán ser la norma y la configuración por defecto en los servicios, especialmente en las redes sociales.

322. Data protection officer

principales requieran la monitorización habitual y sistemática de interesados.

Transferencias de datos a terceros países

La propuesta de la Comisión mantiene la condición principal, ya existente en la actual Directiva, de verificar la existencia de un adecuado nivel de protección en terceros países, para permitir la transferencia de datos personales fuera de la UE (Artículo 41). Asimismo, se mantiene la posibilidad de realizar dichas transferencias, en aquellos casos en los que no se hubiese verificado la adecuación, si se dan un conjunto de salvaguardias apropiadas. La principal novedad al respecto incluida en la propuesta de Reglamento es que se añaden al listado de salvaguardias adecuadas el uso de reglas vinculantes corporativas y el cumplimiento con cláusulas estándar adoptadas por la Comisión o por una APD (Artículo 42).

El uso de reglas vinculantes corporativas permitirá a los grupos empresariales la transferencia de datos personales a entidades situadas fuera de la UE con una mayor sencillez y flexibilidad, disminuyendo las cargas administrativas. Dichos mecanismos deberán ser previamente aprobados por una APD (Artículo 43).

Autoridades de Protección de Datos

Para mejorar la aplicación consistente del nuevo marco, la propuesta de Reglamento establece que en aquellos casos de empresas que operen en múltiples Estados miembros, la APD del país donde esta empresa tenga su sede será la única con la que tenga que tratar para todos los asuntos de protección de datos. Mediante este sistema de «ventanilla única» se evita la existencia de resoluciones incoherentes entre diferentes APD y se reducen los plazos y los costes administrativos.

Para garantizar la coherencia de este sistema, la Comisión propone introducir obligaciones de cooperación entre diferentes Autoridades, asistencia mutua, operaciones conjuntas y de reconocimiento mutuo de las decisiones. Asimismo, la propuesta establece un mecanismo de consistencia para garantizar que, en las situaciones en las que las decisiones tengan un impacto amplio a nivel europeo, las opiniones del resto de autoridades nacionales serán debidamente tenidas en cuenta[323]. Este mecanismo de consistencia contará con la participación de la Comisión Europea, del resto de APD, y del actual Grupo de Trabajo del Artículo 29, que pasará a llamarse Consejo Europeo de Protección de Datos y que estará formado por los directores de las distintas APD nacionales de los distintos Estados miembros, y por el director del Supervisor Europeo de Protección de Datos.

Asimismo, la Comisión Europea propone en el Reglamento incrementar la independencia de las APD y los poderes de estas, pudiendo llevar a cabo investigaciones así como imponer sanciones que podrán alcanzar hasta el 2 % de los ingresos globales de una compañía en casos de violaciones serias del Reglamento, que incluyen, entre otras, no notificar en plazo la existencia de una brecha de seguridad en los datos personales.

323. Para mejorar la consistencia de las medidas adoptadas, la nueva Regulación establece un proceso según el cual las APD nacionales deberán comunicar la propuesta realizada tanto al Consejo Europeo de Protección de Datos como a la Comisión Europea. Tras dicha comunicación, tanto el Consejo como la Comisión Europea podrán emitir opiniones que deberán ser tenidas en cuenta, en un plazo de cuatro y diez semanas respectivamente, tiempo en el que la APD no podrá adoptar dicha medida. En caso de que la Comisión tenga serias dudas sobre la consistencia de la medida propuesta, y tras el proceso anteriormente mencionado, podrá adoptar una decisión razonada para suspender la aplicación de la medida propuesta. Este mecanismo se aplicará a aquellas medidas que: a) afecten a interesados en otros Estados miembros distintos al de la APD que la propone; b) que puedan afectar a la libre circulación de datos personales en la UE; c) que tengan como objetivo definir prácticas de tratamiento de datos sujetas al requisito de consulta previa; d) que determinen o autoricen clausulas estándar de protección de datos para transferencias a terceros países, o e), que aprueben reglas vinculantes corporativas. Asimismo, la Regulación permite a las APD solicitar al Consejo la aprobación de medidas urgentes sin realizar el proceso anterior, para ello el Consejo deberá emitir una opinión favorable en un plazo máximo de dos semanas.

D. Derecho al olvido y a la supresión

COMISIÓN EUROPEA
Bruselas, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos)

(Texto pertinente a efectos del EEE)
{SEC(2012) 72 final}
{SEC(2012) 73 final}
Artículo 17

Derecho al olvido y a la supresión

1. El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes:
a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados;
b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el Artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación autorizado y no existe otro fundamento jurídico para el tratamiento de los datos;
c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el Artículo 19;
d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos.
2. Cuando el responsable del tratamiento contemplado en el apartado 1 haya hecho públicos los datos personales, adoptará todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a terceros que estén tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de estos. Cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación.
3. El responsable del tratamiento procederá a la supresión sin demora, salvo en la medida en que la conservación de los datos personales sea necesaria:
a) para el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el Artículo 80;
b) por motivos de interés público en el ámbito de la salud pública de conformidad con lo dispuesto en el Artículo 81;
c) con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el Artículo 83;
d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o por la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida;

e) en los casos contemplados en el apartado 4.

4. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales cuando:

a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los datos;

b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios;

c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso;

d) el interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado de conformidad con lo dispuesto en el Artículo 18, apartado 2.

5. Con excepción de su conservación, los datos personales contemplados en el apartado 4 solo podrán ser objeto de tratamiento a efectos probatorios, o con el consentimiento del interesado, o con miras a la protección de los derechos de otra persona física o jurídica o en pos de un objetivo de interés público.

6. Cuando el tratamiento de datos personales esté limitado de conformidad con lo dispuesto en el apartado 4, el responsable del tratamiento informará al interesado antes de levantar la limitación al tratamiento.

7. El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales o para el examen periódico de la necesidad de conservar los datos.

8. Cuando se hayan suprimido datos, el responsable del tratamiento no someterá dichos datos personales a ninguna otra forma de tratamiento.

9. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el Artículo 86, a fin de especificar:

a) los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos;

b) las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público a que se refiere el apartado 2;

c) los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4.

Acrónimos

APD	Autoridad de Protección de Datos
APEC	Asia-Pacific Economic Cooperation
API	Interfaz de programación de aplicaciones
CAGR	Tasa de crecimiento anual compuesto
CE	Constitución Española
CERT	Computer Emergency Response Team
EASA	European Advertising Standards Alliance
EDPD	European Data Protection Day
ENISA	The European Network and Information Security Agency
FCC	Federal Communications Commission
FTC	Federal Trade Commission
GT29	Grupo de Trabajo del Artículo 29
IaaS	Infrastructure as a Service
ICDPPC	International Conference of Data Protection and Privacy Commissioners
IP	Internet Protocol
LDAP	Protocolo Ligero de Acceso a Directorios
LOIC	Low Orbit Ion Cannon
MMS	Multimedia Messaging System
OCDE	Organización para la Coooperación y el Desarrollo Económico
PaaS	Platform as a Service
PYME	Pequeña Y Mediana Empresa
RAE	Real Academia de la Lengua Española
RFID	Radio Frequency IDentification
SaaS	Sowtware as a Service
SLA	Service Level Agreement
SMS	Short Message Service
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
VoIP	Voz sobre IP

Bibliografía seleccionada

Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising* (2010)

Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability* (2010)

Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking* (2009)

Tucker, C. «Internet Privacy: The Impact and Burden of EU Regulation» (2011), *Testimony to the Committee on Energy and Commerce: Subcommitte on Comerce, Manufacturing and Trade, U.S. House of Representatives*

Solove, D. J., «A Taxonomy of Privacy» (2006), 154 *U. Penn. L. Rev* 477

Solove D. J., «Conceptualizing Privacy» (2002), 90 *California Law Review* 1087

Solove, D. *Understanding Privacy* (2008), Harvard University Press.

ENISA, *Online as soon as it happens (*2010)

ENISA, *Security Issues and Recommendations for Online Social Networks* (2007)

ENISA, *Study on data collection and storage in the EU* (2012)

Etro, F., «The Economic Consequences of the Diffusion of Cloud Computing» in *The Global Information Technology Report 2009-2010* (2010), World Economic Forum

European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final

European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012) 11 final

European Commission. *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments* (2010), Final Report

European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995)*, Official Journal L 281 , 23/11/1995 P. 0031 - 0050

European Union, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* (2002), Official Journal L 201 , 31/07/2002 P. 0037 - 0047

European Union, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC* (2006), Official Journal L 105, 13/04/2006 P.0054 - 0063

European Union, *Directive 2009/136/EC OF the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws* (2009), Official Journal L 337, 18/12/2009 P.0011 - 0036

FTC, *Protecting Consumer Privacy in an Era of Rapid Change* (2010)

Goldfarb A., Catherine E. Tucker, «Privacy regulation and online advertising», *Management Science*, 57(1), (2011), pp. 57-71

GSMA, *Privacy Design Guidelines for Mobile Application Development* (2011), Global System for Mobile Communications Association

International Standards on the Protection of Personal Data and Privacy, *The Madrid Resolution* (2010)

International Working Group on Data Protection in Telecommunications, *Report and guidance on Social Network Services «Rome Memorandum» (*2008)

Kuan Hon et Al, *Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law. The Cloud of Unknowing, Part 3* (2011), Legal Studies Research Paper No 84/2011. Queen Mary University of London, School of Law

OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980)

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

Schwartz, P. M., «Privacy and democracy in cyberspace» (1999), *Vanderbilt Law Review, 52*, 1609-1701

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

The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (2012)

Mayer-Schönberger, V. *Delete: the Virtue of Forgetting in the Digital Age* (2009), Princeton University Press

World Economic Forum, *Advancing Cloud Computing: What to do now? Priorities for Industry and Governments* (2011), World Economic Forum in partnership with Accenture