LA REGULACIÓN DE LA PRIVACIDAD Y SU IMPACTO EN EL ECOSISTEMA DIGITAL (*)

Jorge PÉREZ MARTÍNEZ
Arturo VERGARA PARDILLO
Zoraida FRÍAS BARROSO
Universidad Politécnica de Madrid

Resumen

La evolución tecnológica de los últimos años ha incrementado la capacidad de recogida, uso y almacenamiento de datos personales en un ecosistema digital en el que Internet ha difuminado por completo las barreras territoriales y, por ende, la legislación que regula la privacidad. Ante esta situación, la Comisión Europea ha propuesto un Reglamento general de protección de datos que tiene como reto compaginar los derechos de los ciudadanos con un marco favorable para la industria europea. En este artículo se analiza el posible impacto del futuro Reglamento europeo en los nuevos servicios del ecosistema digital.

Palabras clave: privacidad, ecosistema digital, Internet, Reglamento general de protección de datos.

Abstract

Technological evolution over the past few years has increased the capacity to collect, use and store personal data in a digital ecosystem where the Internet has blurred territorial boundaries, and thus, the legislation that regulates privacy. In this situation, the European Commission has proposed a General Data Protection Regulation which faces the challenge of combining citizen's rights and an advantageous framework for the European industry. This article analyzes the possible impact of the future European Regulation on digital ecosystem new services.

Key words: privacy, digital ecosystem, Internet, General Data Protection Regulation.

JEL classification: L96.

I. INTRODUCCIÓN

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. Un proceso que 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.

A medida que 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 constituirse como factor fundamental, al menos en dos aspectos: para preservar el derecho individual a la intimidad bajo los nuevos parámetros de la realidad, pero 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 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 2015 y 2016.

Este artículo presenta el modelo regulador de protección de datos en Europa (sección II), así como la propuesta de la Comisión (sección III) y la situación

actual del trámite legislativo de la propuesta (sección IV). Posteriormente, se analiza el posible impacto de la propuesta sobre el desarrollo de algunos de los principales servicios y aplicaciones del ecosistema digital como el *cloud computing*, la publicidad *online*, las redes sociales o las aplicaciones móviles (sección V). Por último (sección VI), se presentan las conclusiones.

II. EL MODELO REGULADOR DE PROTECCIÓN DE DATOS EN EUROPA

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). El marco legislativo de protección de datos personales en la Unión Europea se basa en la Directiva 1995/46/EC, conocida como la Directiva de protección de datos.

La Directiva de protección de datos se aplica a cualquier tratamiento automático de datos personales. La Directiva estipula que los Estados miembros deberán asegurar que los datos personales sean recogidos para fines determinados, explícitos y legítimos, siendo adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.

La Directiva establece la figura de responsable del tratamiento de los datos, que queda sujeta a un conjunto de obligaciones entre las que destacan las siguientes: garantizar la calidad del procesado de los datos, proporcionar a los titulares de los datos información sobre la identidad del propio responsable del tratamiento y sobre los fines por los que se procesan los datos, así como obligaciones sobre confidencialidad, notificaciones obligatorias a la Autoridad Nacional de Protección de Datos (ANPD) y el establecimiento de controles previos en los casos que puedan suponer riesgos específicos para los derechos y libertades de los titulares de los datos.

La Directiva establece también los derechos de los que disfrutan los titulares de los datos, designando a los Estados miembros como garantes de su cumplimiento. Entre ellos están los derechos de acceso, rectificación, oposición, el derecho a un recurso judicial y el derecho a recibir una reparación por parte del responsable de datos en casos de perjuicios como consecuencia de un tratamiento ilícito.

Para articular la supervisión y el control de las disposiciones establecidas en la Directiva de 1995 se dispone la creación de autoridades independientes, las Autoridades Nacionales de Protección de Datos, dotadas de poderes de investigación e intervención. Además, se establece un grupo de trabajo de protección de las personas en lo que respecta al tratamiento de datos personales, el denominado Grupo de Trabajo sobre Protección de Datos del Artículo 29 o GT29. El Grupo tiene como cometido el estudio de las cuestiones relativas a la aplicación de la Directiva, la emisión de dictámenes, recomendaciones y asesoría a la Comisión Europea.

La protección de datos en el ámbito de las telecomunicaciones está regulada, además de por la Directiva de protección de datos de 1995, por la Directiva 2002/58/EC sobre la privacidad y las comunicaciones electrónicas, enmendada en 2006 (2006/24/EC) y en 2009 (2009/136/EC).

La Directiva sobre la privacidad y las comunicaciones electrónicas y sus enmiendas posteriores tienen como objetivo 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.

La Directiva establece un conjunto de obligaciones y salvaguardas mayores que en los casos donde solo es de aplicación la Directiva de protección de datos, entre las que destacan mayores requisitos de seguridad y confidencialidad, prestar información en relación a los riesgos existentes, informar a la autoridad nacional competente en caso de una violación de los datos personales, restringir las comunicaciones no deseadas, limitar la capacidad de almacenamiento y tratamiento de los datos de tráfico, así como establecer la obligación de un consentimiento previo para poder utilizar dichos datos con motivos de promoción comercial.

Este marco normativo supuso un hito en la historia de la protección de datos. 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. También permitió dotar de mayor confianza y protección a los servicios de comunicaciones electrónicas, favoreciendo el rápido desarrollo de los servicios de telecomunicaciones y fomentando el desarrollo de Internet.

Sin embargo, la falta de armonización durante la implementación del marco de protección de datos, junto a la necesidad de adaptarlo a los nuevos retos planteados por el avance tecnológico y la globalización, han llevado a iniciar un proceso de revisión de la legislación en materia de protección de datos. La propia comisaria Viviane Reding reconoce que «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».

El proceso de revisión, iniciado en 2007, ha contado con diversas consultas públicas, foros de debate y comunicaciones de la Comisión Europea y del Parlamento Europeo. En enero de 2012, la Comisión Europea propuso un Reglamento general de protección de datos para que sustituya a la Directiva de protección de datos de 1995.

III. EL NUEVO MARCO REGULADOR. LA PROPUESTA DE LA COMISIÓN EUROPEA

El 25 de enero de 2012 la Comisión Europea hizo pública su propuesta para sustituir a la Directiva de protección de datos de 1995. Dicha propuesta inicia el proceso legislativo ordinario que permitirá la configuración del nuevo marco europeo de protección de datos que entrará en vigor entre 2015 y 2016.

El marco planteado por la Comisión se compone de un Reglamento para la protección de los individuos en relación al tratamiento de sus datos personales y al libre movimiento de dichos datos (conocido como Reglamento general de protección de datos), y que reemplazará 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 reemplazará a 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 por 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 Unión Europea, al ser directamente vinculante en los distintos Estados miembros. Una vez que el Reglamento sea aprobado, pasará a formar 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.

El alcance del Reglamento es el conjunto de los ciudadanos de la Unión Europea de manera directa, así como todas las empresas que dirijan sus servicios a estos, sin importar la radicación de la empresa en cuestión.

El Reglamento se refiere también a cuestiones relacionadas con la ampliación de derechos para los ciudadanos de la Unión Europea e incluye los siguientes aspectos:

— El reconocimiento del derecho al olvido mediante la obligación explícita de que los responsables del tratamiento de datos los eliminen cuando se solicita expresamente y cuando no exista un motivo legítimo para retenerlos.

— La configuración de la privacidad por defecto, de forma que los parámetros por defecto sean la no compartición de datos.

— El refuerzo del 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.

— La garantía de acceso fácil a los datos propios y el derecho a la portabilidad de los datos y, en concreto, conceder el derecho a obtener una copia de los datos almacenados por el responsable del tratamiento así como a la libertad de desplazarlos de un proveedor de servicios a otro, sin obstáculos.

En relación con las empresas que lleven a cabo procesos de recopilación, almacenamiento, gestión y procesamiento de datos deberán:

— Reforzar sus medidas de seguridad para evitar posibles violaciones de datos personales.

— Comunicar la existencia de una filtración de datos personales a la ANPD competente y a los individuos afectados sin demora (normalmente veinticuatro horas).

— Minimizar el volumen de datos personales que se recaban y procesan.

— Garantizar un consentimiento explícito, es decir, que se otorgue mediante declaración o mediante acción afirmativa por parte de la persona en cuestión, y que se conceda libremente.

— Obligar a los responsables del tratamiento de los datos a que designen un encargado de protección de datos en empresas con más de 250 empleados y en las que lleven a cabo procesamientos arriesgados.

— Efectuar «evaluaciones de impacto sobre protección de datos» para aquellas empresas que lleven a cabo procedimientos arriesgados.

— Extender el alcance de las normas anteriores a grupos de empresas que puedan compartir datos personales.

En relación con los principios administrativos de seguimiento, control, ejecución y aplicación, el Reglamento introduce las siguientes novedades destinadas a la creación de un verdadero mercado único:

— Una simplificación del entorno regulatorio al anular formalidades burocráticas como los requisitos generales de notificación.

— La creación de un sistema de «ventanilla única» para la protección de datos en la UE que garantizará que los responsables de datos de las sociedades europeas solo tengan que tratar con una única Autoridad Nacional de Protección de Datos (ANPD) correspondiente a la del Estado miembro donde esté situada su sede.

— El establecimiento de mecanismos para la colaboración, coordinación y coherencia entre todas las ANPD europeas, incluyendo la obligación de que una ANPD inicie investigaciones si así lo solicitara otra de ellas y el principio de reconocimiento mutuo de las decisiones adoptadas en cumplimiento de la legislación europea sobre protección de datos, para garantizar así el cumplimiento sistemático de los derechos de protección de todos los ciudadanos europeos.

— La conversión del Grupo de Trabajo del Artículo 29 (1) 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 ANPD, incluyendo al supervisor europeo de Protección de Datos, lo cual fomentará las sinergias y la efectividad.

— El incremento de los recursos administrativos y judiciales correspondientes ante infracciones relativas a los derechos de la protección de datos. En particular, las asociaciones cualificadas podrán emprender medidas legales en nombre del individuo.

— El establecimiento de sanciones administrativas de hasta el 2 por 100 de la facturación mundial de la empresa, que las ANPD están facultadas para imponer.

IV. EL TRÁMITE LEGISLATIVO DE LA PROPUESTA

Tras la presentación de la propuesta de la Comisión, a principios de 2012, se inició el trámite parlamentario con la presentación de informes y opiniones con enmiendas a la propuesta. Durante el otoño de 2012, diferentes comisiones parlamentarias publicaron proyectos de dictámenes sobre el Reglamento general de protección de datos (Comisión de Mercado Interno y Protección del Consumidor, Comisión de Asuntos Jurídicos, Comisión de Empleo y Asuntos Sociales y Comisión de Industria, Investigación y Energía) y sobre la Directiva (Comisión de Asuntos Legales). Uno de los asuntos señalados por los ponentes de todas las comisiones son los actos delegados, proponiéndose en muchos casos la supresión de buena parte de ellos.

La Comisión de Mercado Interno y Protección al Consumidor aplaude en su dictamen el esfuerzo realizado para el fortalecimiento de los derechos de los consumidores, especialmente en relación con el consentimiento. Sin embargo, considera que se necesitan aún detalles y aclaraciones. Estas puntualizaciones abarcan una ampliación del derecho de supresión, el desarrollo de protección específica para los menores de 14 años, la revisión de la definición propuesta de «datos personales», una mayor clarificación de las responsabilidades de las figuras de «responsable de los datos» y «encargado del tratamiento de los datos», y reevaluar el impacto de la regulación en relación con la creación de perfiles.

Por su parte, la Comisión de Empleo y Asuntos Sociales propone aumentar la consideración de la protección de datos de los empleados, al que se dedica poca atención en el nuevo Reglamento. La interpretación del Reglamento para su aplicación a los

trabajadores no es sencilla. Además considera que el Reglamento debería ser el pilar fundamental, pero que pudieran desarrollarse disposiciones adicionales de carácter nacional que ampliaran los derechos efectivos. Manifiesta, asimismo, la importancia de reforzar la plena independencia de los delegados de protección de datos con respecto a las organizaciones, de modo que no puedan verse sometidos a presiones en el ejercicio de sus funciones.

La Comisión de Asuntos Jurídicos apoya mantener una definición amplia de «datos personales» y del principio del consentimiento explícito, así como fortalecer la protección de los niños y el derecho al olvido. Considera, además, que se necesita introducir explícitamente un principio general de responsabilidad del responsable de los datos, así como un sistema de reconocimiento mutuo para las Autoridades Nacionales de Protección de Datos. Esta Comisión apoya la magnitud de las sanciones administrativas, pero muestra reservas acerca de la capacidad de las autoridades de supervisión para imponerlas.

La Comisión de Industria, Investigación y Energía solicita una revisión de los plazos y las condiciones para las responsabilidades y notificaciones de violaciones de datos. Enfatiza además en el papel que juegan las soluciones técnicas, como la «privacidad desde el diseño» y la anonimización de datos, insistiendo en que deben establecerse prioridades para proteger aquellos datos más sensibles. Además, el ponente de la Comisión hace especial hincapié en la importancia de evitar consecuencias no deseadas en la aplicación del nuevo Reglamento, que puedan derivar en perjuicio de otras libertades (la de prensa), o actividades para la justicia (lucha contra el crimen financiero, contra el fraude en el deporte) o para la investigación (*smart grids*, sistemas de transporte inteligente).

En diciembre de 2012, los ponentes del Comité de Justicia, Derechos Fundamentales y Ciudadanía dieron su apoyo total al marco de protección de datos propuesto por la Comisión Europea en sus objetivos de establecer un marco global de protección de datos, acabando con la fragmentación legislativa y reforzando los derechos de los ciudadanos sobre la privacidad *online*.

No obstante, los ponentes plantearon enmiendas a la propuesta en la línea del fortalecimiento de los derechos individuales, entre los que se incluye el derecho al olvido. En el informe del eurodiputado Albrecht, ponente del Comité de Justicia, Derechos Fundamentales y Ciudadanía, en relación con el Reglamento, cabe destacar su insistencia en que este sea de aplicación tanto en el sector público como en el privado, en contra de lo que defienden otros agentes. Además, respecto a los mecanismos y herramientas que provee el Reglamento, se apunta a las siguientes mejoras:

— Que el sistema de «ventanilla única» esté apoyado por la creación de una Agencia de Protección de Datos europea e independiente, que pueda tomar decisiones legalmente vinculantes para las Autoridades Nacionales de Protección de Datos.

— Que se favorezca el uso en las empresas de seudónimos y de datos anónimos y que se refuerce la idea del consentimiento explícito para el procesado de datos, insistiendo en la inteligibilidad de las políticas de privacidad. También se considera el refuerzo del derecho al olvido haciendo a las compañías que hayan transferido datos a terceros sin una base legal legítima que procedan a borrarlos.

— Que se refuerce la aplicación de la normativa europea a empresas cuyos servicios vayan dirigidos a ciudadanos europeos haciendo énfasis en que no se necesita que exista un pago del usuario al proveedor de servicios para que esta normativa sea de aplicación.

— Que se garantice la provisión de recursos humanos y otros recursos por parte de las ANPD para poder hacer cumplir la legislación europea.

— Que se eviten, en la medida de lo posible, los actos delegados, haciendo las provisiones más detalladas en el propio Reglamento, a lo que la Comisión Europea ya ha mostrado su disposición a considerar (2).

— En relación con la Directiva, que se proporcione a las ANPD más capacidad para cooperar en casos transfronterizos.

En el momento de la redacción, la Comisión Europea ha cerrado el plazo de presentación de enmiendas y se encuentra en periodo de discusión de las mismas. Se espera que en el transcurso de la primavera de 2013 la Eurocámara pueda votar un texto, que pasará a discutirse con los Estados miembros para tener finalmente un Reglamento antes de que acabe la legislatura europea, a principios de 2014.

V. IMPACTO DE LA PROPUESTA DE REGLAMENTO DE PROTECCIÓN DE DATOS EN EL ECOSISTEMA DIGITAL

En esta sección se analiza el posible impacto que la propuesta de Reglamento general de protección de datos de la Comisión Europea, descrito en la sección anterior, puede tener sobre algunos de los principales servicios del ecosistema digital. En concreto, se analizan los casos de las tecnologías de *cloud computing*, la publicidad *online*, las redes sociales y las aplicaciones móviles.

1. *Cloud computing*

El *cloud computing* se presenta como una nueva oleada de tecnología 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. Consiste en el almacenamiento de datos (tales como archivos de texto, imágenes y vídeo) y de *software* en ordenadores remotos a los que los usuarios acceden vía Internet a través de los dispositivos de su elección.

El *cloud computing* permite trasladar mayores economías de escala a la prestación de servicios digitales, consiguiendo mayor flexibilidad y menor precio final. La Comisión Europea ha estimado que el uso masivo de estos sistemas por parte de empresas y del sector público permitirá la creación de 2,5 millones de nuevos puestos de trabajo en Europa, así como un incremento anual del PIB en la UE igual a 160.000 millones de euros (en torno a un 1 por 100 del PIB) de aquí a 2020.

Para fomentar el desarrollo del *cloud computing* en Europa, la Comisión Europea publicó el 27 de diciembre de 2012 una estrategia para «liberar el potencial de la computación en la nube en Europa». La Comisión identifica la incertidumbre generada por el marco de protección de datos de 1995 como una de las principales barreras al desarrollo del *cloud* y apuesta por una rápida adopción del nuevo marco de protección de datos propuesto por la Comisión.

Sin embargo, algunos análisis realizados (Queen Mary University, 2012) señalan que la aplicación del Reglamento mantendrá y, en algunos casos, incrementará las incertidumbres y cargas a las que se ven sometidos los proveedores de servicios *cloud*. A continuación se describen las principales cuestiones problemáticas identificadas hasta ahora y se analiza el potencial impacto de la propuesta de Reglamento general de protección de datos.

1.1. *Transferencia internacional de datos personales*

Los servicios de *cloud* se caracterizan, entre otros elementos, por estar distribuidos en diferentes zonas geográficas. La ubicación de los servidores y de los datos no afecta, en principio, a los servicios prestados. Sin embargo, la existencia de marcos de protección de datos distintos en diferentes regiones geográficas genera limitaciones en la prestación de los mismos e incertidumbres entre usuarios, gobiernos y los propios proveedores de *cloud.*

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 Estados Unidos (*Safe Harbour*). A diferencia de los grandes agentes en este segmento como Amazon, Apple, Google o Microsoft, no está tan claro que otros agentes de menor tamaño como Pro Softnet o Dropbox dispongan de servidores fuera de su mercado natural ni que hayan obtenido acuerdos de Puerto Seguro (3). Estas cuestiones pueden limitar el desarrollo de centros de datos en mercados de menor tamaño y suponer una barrera a la innovación.

La propuesta de Reglamento define su ámbito de aplicación según un criterio de oferta de servicios, introduciendo el concepto de establecimiento principal cuya aplicación práctica es incierta (Queen Mary University, 2012). De esta forma, es improbable que la redacción actual de la propuesta del Reglamento consiga resolver las incertidumbres sobre la aplicabilidad o no de la regulación de protección de datos para aquellos casos en los que usuarios externos a la UE utilicen un proveedor de servicios *cloud* o un centro de datos dentro de la UE.

Además, el Reglamento impone como requisito adicional a los ya existentes la necesidad de aprobación de las transferencias por parte de los organismos reguladores correspondientes, creando mayores cargas para aquellas empresas europeas que utilicen servicios *cloud.*

1.2. *Clarificación de los roles de responsable del tratamiento y encargado del tratamiento*

El Foro Económico Mundial (World Economic Forum, 2011)

señala la necesidad de clarificar el reparto de responsabilidad entre el prestador de los servicios de *cloud*, habitualmente un agente intermediario para el que los datos almacenados o procesados en sus servidores son transparentes, y el responsable del tratamiento, que es quien utiliza el servicio *cloud* para realizar el tratamiento de los datos personales.

El marco europeo solo distingue dos tipos de agentes involucrados en el tratamiento de los datos personales: el «responsable del tratamiento» (4), que es quien determina los fines y los medios del tratamiento de datos personales; y el «encargado del tratamiento» (5), quien trata datos personales por cuenta del responsable del tratamiento. La cuestión en este caso es 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.

En Queen Mary University (2012) y en Renda y Guido (2012) se argumenta que el modelo de responsabilidades de la propuesta de Reglamento de la Comisión no encaja bien con la naturaleza de los proveedores de servicios *cloud*, quienes deberían ser considerados meros «auxiliares».

1.3. *Problemas 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 los mismos. En este sentido, los temas de seguridad señalados por el Foro Económico Mundial se centran en mejorar la seguridad, integridad y disponibilidad de los datos, así como la garantía de que los datos se eliminan una vez que no son necesarios o cuando lo solicitan los responsables del tratamiento.

El futuro Reglamento puede jugar un papel muy importante en este sentido, gracias a los requisitos de notificación de las violaciones de datos y las sanciones económicas, que contribuirán a la mejora de la seguridad y la confianza en estos nuevos servicios.

2. 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. La evolución tecnológica y el propio desarrollo de Internet han permitido pasar de los primeros *banners* genéricos a una oferta de publicidad personalizada, basada en la observación del comportamiento del individuo a través de sus acciones. Las principales ventajas de este tipo de publicidad radican en que los individuos reciben una publicidad más útil y que los anunciantes realizan una mejor selección de su audiencia, permitiendo a los sitios web incrementar su valor e ingresos.

Los principales agentes involucrados en la provisión de publicidad son los proveedores de redes publicitarias (conocidos como *ad networks*), quienes 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 puede encontrar a Google AdSense o Yahoo! Advertising Solutions.

La inversión en publicidad mediante *banners* y en sitios web en Estados Unidos superó los 11.000 millones de dólares en 2011 (Internet Advertising Bureau, 2012), lo que supuso un 34,8 por 100 de toda la inversión en publicidad en Internet y un aumento del 15 por 100 sobre 2010. De estas cifras de inversión *online* en Estados Unidos, Google captura más del 40 por 100, mientras que Yahoo o Microsoft se limitaban a una cuota del mercado estadounidense del 11 y del 6 por 100 respectivamente (6).

Los problemas asociados a la privacidad *online* surgen de la utilización de tecnologías de monitorización del comportamiento para la elaboración de perfiles de usuario que permitan personalizar la publicidad. Estas tecnologías se basan habitualmente en el uso de cookies, que son instaladas por los *ad networks* en el navegador o equipo de usuario.

Los perfiles de usuarios se generan mediante la combinación de perfiles explícitos, creados a partir de 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 minería de datos (*data mining*) sobre la información del comportamiento almacenado. Asimismo, en la creación de los perfiles de usuario se utiliza información adicional como puede ser la localización —por ejemplo 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 como son la gestión del consentimiento, la creación de perfiles y la distribución de responsabilidades. Estas cuestiones se abordan a continuación, analizando para cada una de ellas el posible impacto que puede tener la entrada en vigor del nuevo Reglamento.

2.1. *Gestión del consentimiento*

La mayoría de los usuarios no son conscientes de que su comportamiento al navegar en Internet puede ser monitorizado por las redes publicitarias. Por ello, la revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas de 2009 estableció el requisito de obtener el consentimiento informado del usuario para poder almacenar información o para acceder a información previamente almacenada en el terminal del usuario.

Estos requisitos, que implican un mecanismo de consentimiento positivo u *opt-in*, suponen 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 (7) y permiten mecanismos de *opt-out* en los que los usuarios se pueden dar de baja de los servicios voluntariamente.

Este cambio de enfoque ha recibido el rechazo frontal de la industria de la publicidad y los medios (8), 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. En términos del impacto sobre el negocio, la introducción de la obligación de consentimiento previo disminuiría la efectividad de la publicidad *online* sobre el cambio de intención de compra en un 65 por 100, lo que podría generar una tendencia negativa en la inversión publicitaria en Internet (9).

2.2. *Datos personales y creación de perfiles*

El Grupo de Trabajo del Artículo 29 considera que, en aquellos casos en los que la información capturada permite la identificación del individuo (10), 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 a la Directiva de Protección de Datos (Article 29 Data Protection Working Party, 2010).

En este sentido, es probable que la propuesta de Reglamento afecte a la publicidad *online*, limitando la elaboración de perfiles al consentimiento positivo por parte del interesado. Además, la propuesta recoge también el derecho de oposición para el tratamiento de datos para fines de mercadotecnia directa, lo que podría tener un impacto significativo en los ingresos de los proveedores de servicios financiados con publicidad.

2.3. *Clarificación de los roles de responsable del tratamiento y encargado del tratamiento*

La aplicación del Reglamento puede tener impacto, además de sobre las redes de publicidad, sobre los propios anunciantes y sobre aquellos sitios web que publiquen los anuncios. El GT29 considera que son estos últimos agentes quienes inician el tratamiento de los datos personales y que, por tanto, tienen cierta responsabilidad en el tratamiento de los mismos.

En aquellos casos en los que el sitio web no se limite a la redirección a la red de publicidad sino que activamente recoja ciertos datos y los envíe, el sitio web podrá ser considerado como responsable conjunto del tratamiento y verse sometido a las obligaciones pertinentes. Por su parte, los anunciantes pueden ser considerados como responsables del tratamiento de los datos personales si también capturan información de la clasificación del usuario y la combinan con el comportamiento del mismo durante la visita o con los datos de registro.

La industria europea de publicidad cree (11) que la aplicación de la propuesta de Reglamento de la Comisión Europea tendrá como consecuencia el incremento de las cargas administrativas y los costes asociados al considerarse como datos personales la información utilizada para la monitorización del comportamiento. Han manifestado que, además, 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 sean considerados como responsables del tratamiento cuando en muchos casos el objetivo no es la identificación de los afectados. En ese sentido, este sector ha solicitado la consideración de una nueva categoría de datos que refleje esta situación y equilibre las obligaciones con los riesgos existentes.

3. 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 4.300 millones de usuarios (12) 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, fotografías, vídeos, comentarios o recomendaciones. El número de usuarios, el tipo y la cantidad de información disponible sobre los mismos, 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.

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 a través de acuerdos con redes de distribución de publicidad. De hecho, la inversión en publicidad en las redes sociales alcanzó los 6.000 millones de dólares en 2011, entre las que destaca principalmente Facebook (13) con más de un 67 por 100.

Los problemas 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 los mismos sobre los riesgos asociados y a la dificultad de algunos usuarios para configurar adecuadamente estas herramientas.

Los principales temas de privacidad en relación con las redes sociales 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* (ENISA, 2007; 2010; 2012). 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 (Article 29 Data Protection Working Party, 2009). 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* (International Working Group on Data Protection in Telecommunications —IWGDPT—, 2008).

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 para la revisión del marco regulador europeo incorpora cambios relevantes que plantean diversos problemas. Muchos son similares a los presentados en el caso de la publicidad *online*, por lo que a continuación se describen los que resultan más específicos por la naturaleza de las redes sociales.

Uno de los problemas que mayor alcance puede tener es 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.

3.1. *Recogida de datos personales*

Uno de los principales problemas de privacidad en las redes sociales es el tipo y cantidad de información recogida por estas. En ese sentido, existe un desacople 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 con relación a los fines para los que se recaben y para los que se traten posteriormente» (14), con la naturaleza de las mismas, 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.

La propuesta de Reglamento de la Comisión Europea introduce un requisito explícito que obliga a las redes sociales (como responsables del tratamiento de los datos) a minimizar el volumen de datos personales de los usuarios que se recaban y procesan, lo cual puede estar en muchos casos en clara contraposición a la propia naturaleza de la red social.

3.2. *Derecho al olvido*

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 periodo no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente» (15). Este principio es de aplicación tanto a la información creada por el usuario —que puede querer conservar indefinidamente (16)—, como a la basada en su comportamiento.

Asimismo, algunas de las redes sociales de mayor éxito —como Facebook o Google+— se encuentran establecidas en Estados Unidos, por lo 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 periodo de tiempo, lo que ha generado problemas 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.

Empresas como Facebook (17) han defendido públicamente el derecho de los usuarios a eliminar su cuenta y sus contenidos. Sin embargo, insisten en que el alcance de esta supresión que la propia red social es capaz de garantizar queda confinado a la misma, no pudiendo ejercerse sobre aquellos contenidos que hayan sido extraídos y publicados en lugares externos. Sin embargo, el nuevo Reglamento incluye la obligación del responsable del tratamiento de los datos de informar a terceros sobre la solicitud de supresión tomando todas las medidas «razonables», lo que puede resultar tremendamente ambiguo en una red social. Además, Facebook ha advertido (Allan, 2012) que en una red social, donde suele haber contenido que pertenece a varios usuarios, la implementación del derecho al olvido puede entrar en conflicto con otros derechos, como el de la libertad de expresión, excepción que está contemplada en la propuesta de la Comisión.

3.3. *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.

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, hecho cada vez más común (18). 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 suponen un problema añadido.

En este sentido, los supervisores de protección de datos presionan para que la configuración de privacidad por defecto sea más restrictiva, pues es previsible que un número significativo de usuarios no la modifique. La propuesta de Reglamento establece en su artículo 23 que «[…] por defecto, los datos personales no sean accesibles a un número indeterminado de personas». Por su parte, Facebook (Allan, 2012) asegura que los ajustes por defecto en la actualidad están establecidos para que los usuarios puedan encontrar a sus amigos fácilmente y protejan al mismo tiempo los datos más sensibles. Sin embargo, actualmente los parámetros por defecto permiten la búsqueda de usuarios a través de su correo electrónico o teléfono, y la muestra del perfil en los motores de búsqueda, por citar algunos.

3.4. *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 entre las que se incluyen juegos, aplicaciones de gestión de chats, de integración de preferencias (por ejemplo Spotify), etcétera.

Los principales problemas en este sentido 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 por parte de terceros y, fundamentalmente, de la falta de mecanismos de consentimiento que permitan diferenciar los permisos prestados, siendo la cesión de datos el único

modo de poder utilizar una determinada aplicación.

El GT29 (Article 29 Data Protection Working Party, 2009) considera que en los casos en los que sea la red social quien medie para prestar el acceso a los datos, deberá asegurar que las aplicaciones cumplen con las Directivas europeas. Mientras, en el caso en el 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.

En cualquier caso, el impacto del Reglamento en el funcionamiento actual de las aplicaciones integradas en las redes sociales abarca muchas de las cuestiones problemáticas tratadas anteriormente como el derecho al olvido, la gestión del consentimiento, el derecho de oposición y la minimización de los datos recogidos y procesados.

3.5. *Usuarios de las redes sociales como responsables del tratamiento de datos personales*

La distribución de responsabilidades en las redes sociales es más compleja que en otros casos porque los propios usuarios pueden ser considerados responsables del tratamiento de los datos al publicar datos propios o de terceros usuarios (Article 29 Data Protection Working Party, 2009), lo que puede resultar problemático en la aplicación de la normativa.

Las casuísticas principales responden a situaciones que exceden la exención de «actividades domésticas» implementada por la Directiva de protección de datos y contemplada en el Reglamento, como son: 1) el uso de las redes sociales para actividades empresariales, colaborativas, comerciales, políticas, etc.; 2) 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 (19); y 3) cuando se produce el tratamiento o publicación de datos de terceras partes.

4. Aplicaciones móviles

Las aplicaciones móviles se encuentran en un mercado naciente y dinámico con una alta capacidad 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 (FTC, 2012).

El rápido crecimiento del mercado proporciona oportunidades y beneficios muy significativos para los usuarios, pero también puede generar problemas en relación a 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 las 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 generado algunos conflictos en relación a la privacidad de los datos personales (20) y de los derechos de los usuarios (21), y previsiblemente irán en aumento.

La problemática que afecta a las aplicaciones móviles es similar a la de la publicidad *online* (de hecho, la publicidad supone la principal fuente de ingresos de este mercado). Sin embargo, esta problemática se ve magnificada debido a la inmensa cantidad de datos a la que se puede tener acceso, dadas las capacidades de los nuevos teléfonos inteligentes.

Por lo tanto, afecta a la transparencia y control del usuario, la gestión del consentimiento, el derecho de oposición y la minimización de los datos recogidos. Sí merece especial mención el caso de la distribución de responsabilidades entre los distintos agentes que participan en este mercado.

4.1. *Distribución de responsabilidades*

En un ecosistema tan complejo como el de las aplicaciones móviles, resulta muy relevante la distribución de las responsabilidades en relación a la privacidad de los datos personales entre los desarrolladores de las mismas, 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 al dinamismo de este mercado.

Al igual que en el caso del *cloud computing*, la división de responsabilidades que figura en la propuesta de Reglamento de la Comisión Europea no es fácil de identificar en el negocio de las aplicaciones móviles. El responsable del tratamiento de los datos debería ser, a priori, el gestor de la aplicación, es decir, quien la publica en las tiendas de aplicaciones. Sin embargo, la plataforma intermediaria, propietaria de dicha tienda y vinculada al sistema operativo del teléfono, podría ser también considerada, en ciertas circunstancias, responsable del tratamiento.

VI. CONCLUSIONES

La propuesta de Reglamento general de protección de datos de la Comisión Europea se enfrenta a la difícil labor de equilibrar los derechos de los ciudadanos en materia de protección de datos —y su cumplimiento efectivo—, con la necesidad de impulsar el desarrollo de los nuevos servicios en el ecosistema digital. A continuación se enumeran las principales conclusiones de este trabajo.

1. *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 momento oportuno para establecer una convergencia reguladora, sin necesidad ni riesgo de situar una concepción o tradición histórica por encima de las demás.

2. *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 precedentes —poco favorables— ya consolidados en el mundo Internet.

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

4. *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.

5. *Mejorar transparencia y 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.

6. *Consentimiento transparente*. La falta de conciencia e incluso 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.

NOTAS

(*) La investigación realizada en este artículo ha sido financiada por Fundación Telefónica. Se puede encontrar una versión más amplia del mismo en el libro *El debate sobre la privacidad y seguridad en la Red: Regulación y mercados*, Cuaderno 36, Editorial Ariel, 2012.

(1) Véase www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php.

(2) Véase http://europa.eu/rapid/press-release_SPEECH-12-764_en.htm.

(3) En el caso de Dropbox, este alcanzó el cumplimiento del acuerdo SafeHarbour con la UE en febrero de 2012 (http://blog.dropbox.com/?p=972). Hasta ese momento no cumplía con los requisitos para realizar transferencia de datos personales entre Europa y EE.UU., forzando 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 art. 3 de la Directiva de Protección de Datos).

(4) Conocido también como el controlador de los datos derivado de la traducción del término en inglés *data controller*.

(5) Conocido también como el procesador de los datos derivado de la traducción del término en inglés *data processor*.

(6) Véase http://www.emarketer.com/blog/index.php/tag/online-ad-revenues/.

(7) 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 de Privacidad de las Comunicaciones Electrónicas. Para que el consentimiento pueda darse a través de la configuración del navegador, el GT29 considera que deben darse las siguientes condiciones: 1) 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 2) 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 la problemática de privacidad relacionada con la publicidad *online*.

(8) En 2009 se presentó una posición conjunta al Parlamento durante el proceso de revisión del Marco Regulador Europeo (véase 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 (véase 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).

(9) Según FORRESTER, la inversión en publicidad en Europa Occidental es una cuarta parte inferior a la de Estados Unidos. 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.

(10) 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.

(11) 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.

(12) Véase http://vincos.it/social-media-statistics/.

(13) Véase http://www.socialmediaportal.com/News/2011/01/Social-media-ad-spend-to-hit-6-billion-worldwide-in-2011.aspx.

(14) Artículo 6(1)(c) de la Directiva de protección de datos.

(15) Artículo 6(1)(e) de la Directiva de protección de datos.

(16) 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 los usuarios y para el funcionamiento y reputación de la propia red social.

(17) Para más información véase https://www.facebook.com/help/359046244166395/.

(18) Véase http://www.bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/.

(19) 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.

(20) 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. Véase http://www.huffingtonpost.com/2011/05/10/senate-panel-apple-google-location-data-privacy_n_860155.html.

(21) Por ejemplo, el caso de Instagram, cuya nueva política de privacidad y términos y condiciones se anunciaron a final de 2012 resultando en una pérdida espectacular de usuarios de la aplicación por considerarlas abusivas.

BIBLIOGRAFÍA

ALLAN, R. (2012), «La posición de Facebook sobre la privacidad y la seguridad», en *The debate on privacy and security over the network. Regulation and markets*, Fundación Telefónica, pp. 143-147.

ARTICLE 29 DATA PROTECTION WORKING PARTY (2009), *Opinion 5/2009 on online social networking, WP163.*

— (2010), *Opinion 2/2010 on online behavioural advertising.*

ENISA (2007), *Security issues and recommendations for online social networks.*

— (2010), *Online as soon as it happens.*

— (2012), *Study on data collection and storage in the EU.*

EUROPEAN COMMISSION (2010), *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committe and the Commitee of the Regions. A comprehensive approach on personal data protection in the European Union.* COM(2010)609 final.

— (2011a), *ePrivacy Directive: circumstances, procedures and formats for personal data breach notifications.* http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/data_breach/index_en.htm.

— (2011b), *Cloud computing: public consultation report.*

EUROPEAN PARLIAMENT (2011), *European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union.* 2011/2025(INI).

GOLDFARB, A., y TUCKER, C. (2011), «Privacy regulation and online advertising», *Management Science*, 57-71.

GSMA (2011), *Privacy design guidelines for mobile application development.*

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (IWGDPT) (2008), *Report and guidance on social network services («Rome Memorandum»).*

INTERNET ADVERTISING BUREAU (2012), *Internet Advertising Revenue Report, 2011 full year report.*

MMA (2011), *Mobile application privacy policiy framework.*

QUEEN MARY UNIVERSITY (2012), *Cloud Legal Project. Centre for Commercial Law Studies.*

RENDA, A., y GUIDO, L. (2012), *The economics of cloud computing.* CEPS Digital Forum.

WORLD ECONOMIC FORUM (2011), *Advancing Cloud Computing: What to do now? Priorities for Industry and Governments.* World Economic Forum in partnership with Accenture.