IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

Monográfico «Retos y oportunidades del entretenimiento en línea»

ARTÍCULO

Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales.[1] Parte una

Antonio Troncoso Reigada
Profesor Titular de Derecho Constitucional de la Universidad de Cádiz

Fecha de recepción: octubre de 2012
Fecha de aceptación: octubre de 2012
Fecha de publicación: noviembre de 2012

Resumen
El estudio analiza los tratamientos de datos personales que llevan a cabo las empresas que prestan servicios de red social, teniendo en cuenta el nuevo marco jurídico que supone la propuesta de Reglamento general de protección de datos personales de la Unión Europea, que ha presentado en enero de 2012 la Comisión. El estudio analiza a quién le corresponde la responsabilidad del tratamiento y la aplicación de la excepción de las actividades personales o domésticas. Se abordan las dificultades para aplicar la Directiva 95/46/CE a las corporaciones internacionales que tienen su sede fuera de la Unión Europea y la regulación que en este punto hace la propuesta de Reglamento general de protección de datos personales. Igualmente se analiza la información, el consentimiento del interesado para el tratamiento y para las cesiones, el principio de calidad en el servicio de red social, la conservación de la información, las medidas de seguridad y los derechos de las personas, en especial el derecho al olvido en internet a la luz de la propuesta de Reglamento general de protección de datos personales.

1. Este texto recoge mis intervenciones en el VIII Congreso Internet, Derecho y Política, organizado por la Universitat Oberta de Catalunya y dedicado a «Retos y oportunidades del entretenimiento en línea», y en el Curso de Verano de la Universidad Complutense de Madrid-San Lorenzo de El Escorial sobre «Policía 3.0: Redes sociales en la nueva dimensión de la seguridad», organizado por la Dirección General de la Policía del Ministerio del Interior, ambos celebrados en julio de 2012. Una primera reflexión sobre las redes sociales la realicé en la Conferencia Europea de Protección de Datos, celebrada en Edimburgo el 24 de abril de 2009, y en el Seminario «Privacidad del menor en las redes sociales», organizado por la Fundación Solventia y el Colegio de Abogados de Madrid en junio de 2009. Este trabajo se enmarca dentro del proyecto de investigación «Transparencia administrativa y protección de datos personales» -DER2012-39629- del Ministerio de Economía y Competitividad.

Palabras clave
redes sociales, derecho a la protección de datos personales, derecho a la privacidad, Reglamento general de protección de datos

Tema
social networking services, redes sociales

Social networks in light of the General Data Protection Regulation proposal. Part 1

Abstract
This paper examines how personal data is processed by companies offering social network services in the context of the new legal framework entailed in the EU's proposal for the General Data Protection Regulation presented by the European Commission in January 2012. The paper examines who is responsible for data processing and applying the exclusion of personal or domestic activities. An attempt is made to dissect the difficulties in applying Directive 95/46/CE to International Corporations based outside of the EU and how the proposal for the General Data Protection Regulation aims to regulate this matter. The data, the consent of interested parties for data processing and transfers, the principle of quality in social network services, data storage, security measures and the rights of individuals, in particular, the right to be forgotten on the Internet, are analysed in the context of the proposal for the General Data Protection Regulation.

Keywords
social networks, right to protection of personal data, right to privacy, General Data Protection Regulation

Subject
social networking services, social networks

1. El nuevo marco jurídico para los tratamientos de datos personales en los servicios de red social: la propuesta de un Reglamento general de protección de datos personales

La Comisión Europa ha aprobado el 25 de enero de 2012 una propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos.[2] La necesidad de un nuevo marco jurídico europeo es consecuencia de los profundos cambios que han experimentado las tecnologías de la información y la comunicación en los últimos años, que ha supuesto un incremento sin precedentes del intercambio de datos a gran escala, lo que obliga a dar respuesta a los riesgos significativos existentes en la era de internet, algo esencial en la Agenda Digital para Europa y en la Estrategia Europa 2020. El incremento de los tratamientos de datos personales derivado del proceso tecnológico –no sólo las redes sociales sino también el internet de las cosas, la videovigilancia, la

2. COM (2012) 10 final. Cfr. también la comunicación de la Comisión «La protección de la privacidad en un mundo interconectado. Un marco europeo de protección de datos para el siglo XXI», COM (2012) 9 final. Cfr. más ampliamente sobre la cuestión A. Troncoso Reigada, «Hacia un nuevo marco jurídico europeo de protección de datos personales», en *Revista Española de Derecho Europeo,* núm. 43, 2012, págs. 25-160.

biometría, la nanotecnología, la historia clínica electrónica en la nube, la identificación por radiofrecuencia (RFID), etc.– eleva el nivel de riesgo para la privacidad, por lo que este proceso debe ir acompañado de un fortalecimiento de las garantías de las personas. La propuesta de Reglamento sale al paso de este cambio tecnológico, dando a las personas más instrumentos para el control sobre su información personal. A ello hay que añadir la aprobación del Tratado de Lisboa, que refuerza la base jurídica en la Unión Europea para aprobar una normativa en virtud del reconocimiento de un derecho fundamental a la protección de datos personales en el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea. Además, la protección de datos personales es un elemento esencial para la construcción europea y para hacer viable la libre circulación de personas que tiene como presupuesto que los países europeos tengan un modelo de protección de datos personales homogéneo que permita el intercambio de información. Sin embargo, las divergencias en la protección de los datos personales en los Estados miembros son todavía demasiado grandes, consecuencia, por una parte, de una inadecuada transposición de la Directiva 95/46/CE por la propia legislación de los Estados miembros;[3] y por otra, del margen de maniobra que dejaba la propia directiva como derecho derivado institucional y que contenía abundantes cláusulas abiertas (*open-ended principles*). Estas diferencias en la protección de los datos personales entre los Estados miembros han obstaculizado el mercado interior, han dificultado el ejercicio de actividades económicas a escala comunitaria y han falseado la competencia; además, la ausencia de protección equivalente afecta también a la eficacia del derecho fundamental a la protección de datos personales de los ciudadanos europeos. La propuesta de un Reglamento general de protección de datos es, para la Comisión, un marco jurídico coherente y homogéneo de protección de datos que suprime las incongruencias entre los Estados miembros, reduce el margen de elección tanto de los legisladores nacionales como de las autoridades de control y facilita una política más integradora en la Unión Europea en este ámbito. De hecho, las diferencias en el nivel de protección de datos personales entre los Estados miembros afectan especialmente a las empresas multinacionales como las que prestan servicios de redes sociales que operan en el ámbito europeo y que tienen que cumplir diferentes obligaciones en los Estados miembros, lo que impide desarrollar políticas paneuropeas sobre protección de datos y falsea la competencia –no existe tampoco una supervisión coherente y sanciones equivalentes en todo el territorio de la Unión.[4] A ello se unen los problemas que plantea la protección de los datos personales en un mundo globalizado e interconectado donde usuarios y proveedores de servicios se encuentran frecuentemente en países y continentes distintos y donde no existen unos estándares internacionales en este ámbito. La propuesta de Reglamento permite una protección más efectiva de los ciudadanos europeos frente a los tratamientos de datos a escala internacional como los que se dan en el ámbito de las redes sociales, que puede lograrse mejor a nivel de la Unión. La aprobación de este reglamento derogará la actual Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y desplazará la normativa española de protección de datos personales, en especial, a la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos (LOPD), y a su reglamento de desarrollo, aprobado por el Real decreto 1720/2007, de 21 de diciembre (RPDP).

La propuesta de Reglamento aborda con precisión cuestiones como el ámbito de aplicación territorial y resuelve la problemática de jurisdicción y de ley aplicable que plantean las corporaciones internacionales que ofrecen servicios de tratamiento de datos –redes sociales virtuales, motores de búsqueda, servicios de computación en nube– y que tienen su sede fuera de la Unión Europea. Además introduce nuevas obligaciones del responsable del tratamiento como la evaluación de impacto, el nombramiento de un delegado de protección de datos, la conservación de la documentación o el cumplimiento de requisitos en materia de autorización y consulta previas. Regula con precisión la licitud de los tratamientos –se decanta por el consentimiento explícito–, la transparencia de la información y el derecho al olvido en internet –el deseo de «borrar el rastro en internet»–,

3. Recientemente, la sentencia del Tribunal de Justicia de la Unión Europea, de 24 de noviembre de 2011, ha resuelto una cuestión prejudicial presentada por el Tribunal Supremo de España y ha puesto en evidencia el incumplimiento de nuestro país en la transposición de la Directiva 95/46/CE, que no incluyó como supuesto de legitimación del tratamiento la satisfacción de un interés legítimo del responsable –art. 7.f)–, sino que impuso obligaciones adicionales –en especial, que los datos estuvieran contenidos en fuentes accesibles al público– y no estableció la necesaria ponderación con los derechos del interesado en cada supuesto de hecho. La resolución de la cuestión prejudicial ha llevado al Tribunal Supremo, en su reciente sentencia de 8 de febrero de 2012, a anular el artículo 10.2.b) del RPDP.
4. Basta comparar las diferencias en el ámbito de la supervisión entre la empresa española Tuenti y otras redes sociales.

hace recaer la responsabilidad de garantizarlo en quien haya publicado los datos personales y no en los buscadores, e incorpora límites al derecho a la protección de datos personales para garantizar la libertad de información y de expresión. Por último, fortalece a las autoridades de control, tanto en sus funciones como en la posibilidad de imponer importantes sanciones económicas, de manera que puedan ser eficaces en la supervisión y la aplicación de la protección de datos, al unificar su capacidad coercitiva y establecer mecanismos que faciliten la coherencia en la aplicación de la protección de datos personales en la Unión. Lógicamente, la aprobación de este reglamento general de protección de datos personales representa un nuevo régimen jurídico que debe ser respetado por los tratamientos de datos personales en los servicios de red social.

Las redes sociales, basadas en que los usuarios comparten información a veces muy sensible, suponen un reto a la privacidad personal e implican un cambio de paradigma.[5] De hecho, nuevas realidades como las redes sociales suponen tales amenazas a la privacidad que ha llegado a afirmarse que debemos resignarnos a no tener privacidad –*you already have zero privacy. Get over it*– o si tenemos privacidad es porque alguien tolera que la tengamos.[6] De hecho, el propio concepto de red social conlleva una cierta renuncia de los usuarios a su privacidad.[7] Las personas ponen en común aficiones, gustos y vivencias con la finalidad de facilitar el acceso a esta información por una red de contactos que incluye una mayoría de personas a las cuales no conocen. Las redes sociales son grandes fuentes de información no sólo sobre sus miembros sino sobre las personas que éstos conocen o han contactado alguna vez y suponen tratamientos masivos de datos personales, lo que representa un riesgo para la privacidad de la personas.[8] La información publicada por un usuario en su página personal no sólo permite fácilmente establecer un perfil personal sino que incluye, en muchas ocasiones, datos sobre vida sexual, ideología, religión, que es una información considerada por la normativa como de especial protección. Toda esta información señala pautas de consumo y permite personalizar la publicidad –el principal objetivo de muchas bases de datos privadas–, y a su vez puede comercializarse esta información.[9] Además, los perfiles

5. Cfr. J. L. Piñar Mañas y P. Lucas Murillo de la Cueva, *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009; P. Lucas Murillo de la Cueva, *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990; e *Informática y protección de datos personales*, CEC, Madrid, 1993; M. Carrillo, *El derecho a no ser molestado. Información y vida privada*, Aranzadi, Navarra, 2003; A. Troncoso Reigada (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Cizur Menor, 2010.
6. La afirmación –del año 1999– es del presidente y cofundador de Sun Microsytems, Scott McNealy, y se encuentra en el comienzo del interesante trabajo de J. L. Piñar Mañas «¿Existe privacidad?», en *Protección de datos personales,* Alonso Editores, México, 2010.
7. La privacidad y la intimidad es un requisito necesario, como ha señalado nuestro Tribunal Constitucional, para tener una mínima calidad de vida. Carecer de privacidad –que toda la información personal sea pública– afecta a la propia identidad y a la libertad ya que la actuación tiende a ajustarse a unas pautas previas esperadas. En otro momento hemos diferenciado los círculos de intimidad y privacidad. Cfr. «Transparencia administrativa y protección de datos personales», en A. Troncoso Reigada, *Transparencia administrativa y protección de datos personales,* Civitas-APDCM, Madrid, 2008, págs. 75-86.
8. Esta es una cuestión sobre la que se ha pronunciado la 30.ª Conferencia Internacional de Privacidad, celebrada en Estrasburgo en octubre de 2008, que aprobó la Resolución sobre protección de la privacidad en las redes sociales. Cfr. también el Memorándum de Roma, del Grupo de Trabajo Internacional de Berlín sobre protección de datos en las telecomunicaciones, de marzo de 2008 ‹http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf›. Cfr. especialmente el dictamen 5/2009 del Grupo de Trabajo sobre Protección de Datos del Artículo 29, sobre las redes sociales en línea, de 12 de junio de 2009, ‹http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm›. La Agencia Europea de Seguridad de las Redes y de la Información (ENISA) ha elaborado una lista de riesgos potenciales del uso de las redes sociales: «Security Issues and Recommendations for Online Social Networks», octubre de 2007, disponible en www.enisa.europa.eu. Esta preocupación también se ha trasladado a los medios de comunicación. Cfr. por ejemplo «¿Sabe Facebook demasiado sobre sus usuarios?», *El País.com*, 3-11-2008.
9. Aunque los usuarios de redes sociales utilicen un pseudónimo, existe por parte de las redes sociales un tratamiento de las direcciones IP, que han sido consideradas hasta ahora un dato de carácter personal. De hecho, la dirección IP es utilizada frecuentemente por los prestadores de servicios de estas redes sociales para segmentar la publicidad que se dirige a los distintos tipos de usuarios registrados. Cfr. C. Vela Sánchez-Merlo, «La privacidad de los datos en las redes sociales», *Revista Española de Protección de Datos*, núm. 5, 2008, págs. 246-247. La dirección IP como dato de carácter personal ha sido ya analizado tempranamente en nuestro trabajo «La Administración electrónica», en J. L. Piñar Mañas (dir.), *Administración electrónica y ciudadanos,* Civitas-Thomson Reuters, Madrid, 2011, págs. 67-68. Recientemente, la propuesta de Reglamento general de protección de datos que ha presentado la Comisión precisa el concepto de dato personal como toda información relativa a un interesado y define interesado como toda persona física identificada, directa o indirecta, por medios que puedan ser utilizados razonablemente por el responsable o por cualquier otra persona física o jurídica, añadiendo elementos que no estaban en la Directiva 95/46/CE pero que ya habían sido expresamente admitidos por el Grupo de Trabajo del Artículo 29 como la dirección IP o el identificador en línea. El Tribunal de Justicia de la Unión Europea ha señalado que el derecho a la protección de los datos personales y el

de las redes sociales pueden ser archivados, lo que facilita la creación de bases de datos de personas con fines ilícitos.[10] Todo ello obliga a repensar y a reforzar la normativa europea de protección de datos personales, como hace la propuesta de Reglamento general de protección de datos personales que ha presentado la Comisión el 25 de enero de 2012, para que contemple y regule estas nuevas realidades que, si bien aportan principalmente oportunidades y ventajas, también conllevan la aparición de nuevos riesgos.

2. El responsable del tratamiento en el servicio de red social, la delimitación de las actividades personales o domésticas y el problema de aplicación de la Directiva 95/46/CE. La regulación de la propuesta de Reglamento general de protección de datos personales de las corporaciones que tienen su sede fuera de la Unión Europea

La normativa de protección de datos personales, a diferencia de la relativa al derecho a la intimidad, reconoce al ciudadano unos principios y derechos de protección de datos, y al mismo tiempo establece un conjunto de obligaciones al responsable del tratamiento, de forma que permite al titular de los datos el control sobre su propia información personal sometida a tratamiento, también dentro de las redes sociales. No obstante, la propia naturaleza de internet –y de estas redes sociales–, que facilita las relaciones con personas de ámbitos geográficos muy alejados, plantea algunos interrogantes a la hora de determinar la aplicación de la Directiva 95/46/CE (art. 4) y de la LOPD (art. 2.1), teniendo en cuenta, además, que algunas redes sociales tienen su sede fuera de la Unión Europea.[11] Pues bien, los titulares de los servicios de redes sociales son responsables del tratamiento de datos personales y, si están establecidos en algún Estado miembro de la Unión Europea o utilizan medios de tratamiento ubicados en ella, deben cumplir la normativa europea –española si están establecidos en nuestro país– sobre protección de datos personales. Así, la Directiva 95/46/CE señala en el art. 4 que serán de aplicación las disposiciones nacionales que traspongan la Directiva a todo tratamiento de datos cuando el responsable no esté establecido en la Unión Europea pero recurra, para el tratamiento de datos personales, a medios situados en el territorio de ese Estado, salvo que tales medios se utilicen únicamente con fines de tránsito. Las redes sociales utilizan medios ubicados dentro de la Unión Europea, no sólo por la utilización de *cookies* o *banners*, sino porque la recogida de datos se produce en parte dentro de la Unión Europea.[12] Los proveedores del servicio de red social son

derecho a la vida privada (arts. 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea) se aplica a toda información sobre una persona física identificada o identificable –sentencia, de 9-11-2010, asunto *Volker und Markus Schecke y Eifert*, apdo. 52. El considerando 26 de la Directiva 95/46/CE y el considerando 23 y el art. 4.1) de la propuesta de Reglamento señalan que para determinar si una persona es identificable deben tenerse en cuenta todos los medios que razonablemente pudiera utilizar el responsable del tratamiento o cualquier otro individuo para identificar a esa persona, en el sentido de lo expresado en el dictamen 4/2007 del Grupo de Trabajo del Artículo 29 sobre el concepto de datos personales, <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_es.pdf>. Así, en relación con los identificadores en línea, el considerando 24 de la propuesta de Reglamento señala que «cuando utilizan servicios en línea, las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como las direcciones de los protocolos de internet o los identificadores de sesión almacenados en *cookies*. Ello puede dejar huellas que, combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas e identificarlas. De ello se deduce que los números de identificación, los datos de localización, los identificadores en línea u otros factores específicos *no necesariamente tienen que ser considerados datos de carácter personal en toda circunstancia*». A nuestro juicio, como hemos señalado en otro momento, las *cookies*, con independencia de la información almacenada en ellas, pueden vincularse con el usuario de un determinado dispositivo conectado a internet y permiten obtener el perfil del usuario. Si bien la dirección IP no siempre es estática sino que puede ser dinámica, además de que no identifica a un usuario sino un equipo –que puede ser de utilización compartida, por ejemplo en puntos de acceso público a internet o en un cibercafé– en muchas ocasiones es una «información concerniente a personas físicas identificadas o identificables».

10. Como señala el dictamen 5/2009 del Grupo de Trabajo del Artículo 29 –ya citado–, las redes sociales «generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden. Los usuarios que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en esta información».
11. Hay redes sociales como Facebook que están adheridas al puerto seguro, lo que significa que han asumido los principios y derechos de protección de datos personales presentes en la Directiva 95/46/CE.
12. Esta es la interpretación que a nuestro juicio debe darse al «Documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en internet por sitios web establecidos fuera de la UE», del

responsables del tratamiento de datos porque han decidido la finalidad, el contenido y el uso del tratamiento –art. 3.d) de la LOPD. Como ha señalado el Grupo de Trabajo del Artículo 29 en el dictamen 5/2009, éstos «proporcionan los medios que permiten tratar los datos de los usuarios, así como todos los servicios "básicos" vinculados a la gestión de los usuarios (por ejemplo, el registro y la supresión de cuentas). Los proveedores de servicios de red social –SRS– determinan también la manera en que los datos de los usuarios pueden utilizarse con fines publicitarios o comerciales, incluida la publicidad proporcionada por terceros. Los proveedores de aplicaciones también pueden ser responsables del tratamiento de datos, si desarrollan aplicaciones que funcionan además de las de los SRS y que los usuarios deciden utilizar».

La propuesta de Reglamento general de protección de datos personales, que ha presentado recientemente la Comisión Europea, contiene una interesante regulación de su ámbito de aplicación territorial, con la finalidad de tratar de resolver la problemática de jurisdicción y de ley aplicable que plantean las corporaciones internacionales que no tienen su sede en la Unión Europea pero que ofrecen en el territorio de la Unión servicios de tratamiento de datos como los servicios de redes sociales virtuales –u otros como los motores de búsqueda o los servicios de computación en nube–, y que había dado lugar recientemente a una cuestión prejudicial planteada por la Audiencia Nacional.[13] Hay que destacar que la propuesta de Reglamento no esgrime para el ámbito de aplicación territorial el criterio –presente en el art. 4.1.c) de la Directiva 95/46/CE– relativo al empleo de medios técnicos en los Estados de la Unión –que el responsable que tiene su sede fuera de la Unión Europea recurra para el tratamiento de datos personales a medios, automatizados o no, situados en los Estados de la Unión– sino que emplea «un factor de conexión más específico» que tiene en cuenta la necesaria «orientación hacia las personas». Para ello, se establece que el Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable no establecido en ella cuando las actividades de tratamiento estén relacionadas con la oferta de bienes o servicios a esos interesados en la Unión y con el control de su conducta (art. 3.2), siguiendo en este punto el dictamen 8/2010, del Grupo de Trabajo del Artículo 29.[14] Esta ampliación del ámbito de aplicación territorial

Grupo de Trabajo del Artículo 29, aprobado el 30 de mayo de 2002, <http://ec.europa.eu/justice_home/fsj/privacy>. El Grupo de Trabajo del Artículo 29, en el dictamen 5/2009, señala que las disposiciones de la Directiva relativas a la protección de datos se aplican en la mayoría de los casos a los proveedores de servicios de redes sociales, aunque su sede se encuentre fuera de la Unión Europea. El Grupo de Trabajo del Artículo 29 remite a su dictamen previo sobre los motores de búsqueda, con el fin de obtener información complementaria sobre las cuestiones del establecimiento y la utilización de equipo como determinantes para la aplicabilidad de la Directiva relativa a la protección de datos y de las normas derivadas del tratamiento de las direcciones IP y la utilización de *cookies*.

13. El auto de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, de 2 de marzo de 2012, planteó una cuestión prejudicial –también en relación con el derecho al olvido en internet–, en el marco de las resoluciones de tutela de derechos que la Agencia Española de Protección de Datos ha dictado frente a Google. Así, se pregunta si debe interpretarse que existe un establecimiento cuando la empresa proveedora del motor de búsqueda crea en un Estado miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese Estado, o cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con esa empresa o cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria [aquí debería producirse una respuesta afirmativa a la luz del art. 3.2 de la propuesta de Reglamento]. También se pregunta si debe interpretarse el art. 4.1.c de la Directiva 95/46/CE en el sentido de que existe un «recurso a medios situados en el territorio de dicho Estado miembro» cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas webs ubicadas en servidores de ese Estado miembro o cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro [ambas respuestas serían afirmativas a la luz de los dictámenes 5/2009 y 8/2010, del Grupo del Artículo 29]. También se pregunta si puede considerarse como un recurso a medios, en los términos del art. 4.1.c de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en internet [existe una responsabilidad del buscador sobre sus propios tratamientos, como hemos señalado en «Transparencia administrativa», *loc. cit.*, págs. 101-112] y si puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas. Por último, en el caso de que el Tribunal de Justicia de la Unión Europea señale que no concurren los criterios de conexión previstos en el art. 4 de la Directiva, se pregunta si debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta Europea de Derechos Fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea.

14. Cfr. dictamen 8/2010 sobre derecho aplicable elaborado por el Grupo de Trabajo de la Unión Europea del Artículo 29, que está accesible en <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_es.pdf>.

se complementa con la obligación de los responsables del tratamiento no establecidos en la Unión de designar un representante en ella, que actúe en lugar del responsable, al que puede dirigirse cualquier autoridad de control en lo que respecta al cumplimiento de sus obligaciones, y que debe estar establecido en uno de los Estados miembros en que residan los interesados cuyos datos personales son objeto de tratamiento en el contexto de una oferta de bienes o servicios o cuyo comportamiento esté siendo controlado (arts. 4.14 y 25).[15]

La propuesta de Reglamento de la Comisión mejora la posición jurídica y las garantías de los ciudadanos europeos, teniendo en cuenta la naturaleza global de internet, basado en plataformas digitales que no se circunscriben a un solo territorio. De esta forma, se trata de poner fin a una práctica frecuente de las corporaciones internacionales, que alegan reiteradamente que no les es de aplicación el derecho europeo, con lo que niegan a sus usuarios europeos algunos derechos que la normativa les garantiza y, además, obligan a los ciudadanos europeos a solicitar la tutela de sus derechos ante tribunales de justicia internacionales, principalmente el estadounidense, lo que genera una indudable indefensión. La propuesta de Reglamento –al igual que anteriormente lo hacia la Directiva y los dictámenes del Grupo de Trabajo del Artículo 29– obliga a los proveedores de servicios en internet como las redes sociales a someterse a la legislación europea de protección de datos personales, de forma que se pueda garantizar de manera efectiva los derechos de los ciudadanos europeos frente a las prácticas de estas empresas, sometiéndolas, además, a las competencias de control de las autoridades administrativas de protección de datos de los Estados de la Unión y de sus órganos jurisdiccionales –y no, por ejemplo, a los de EE.UU.[16]

Los usuarios de redes sociales tienen la consideración de afectados o interesados al ser las personas titulares de los datos que son objeto de tratamiento –art. 3.e) de la LOPD.[17]

15. No es aplicable la obligación de designar representante cuando el responsable esté establecido en un país con nivel adecuado de protección, cuando sea una empresa con menos de doscientos cincuenta trabajadores o un organismo público, o cuando el responsable ofrezca sólo ocasionalmente bienes o servicios a interesados residentes de la Unión. El carácter ocasional se desprende de analizar las actividades generales del responsable para determinar si la oferta de bienes y servicios a los interesados es accesoria a las actividades principales (considerando 64). En todo caso, hay que recordar que la Directiva 95/46/CE ya preveía que cuando el responsable no estuviera establecido en el territorio de la Unión Europea y utilice en el tratamiento medios situados en un país de la Unión Europea, deberá designar un representante en ese país (art. 4.2), lo que no siempre se cumplía.
16. Recientemente Google ha presentado una nueva política de privacidad, en la que prevé crear un perfil de datos del usuario utilizando todas las aplicaciones derivadas del buscador como redes sociales o programas de localización geográfica. La comisaria europea de Justicia, Viviane Reding, ha pedido a Google que deje en suspenso las nuevas normas de privacidad anunciadas porque no cumplen la legislación europea de protección de datos, y ha recordado, en línea con la propuesta de Reglamento, que las compañías internacionales que ofrecen sus servicios a los consumidores de la UE deben respetar las normas europeas de protección de datos. También las autoridades de control de privacidad de Asia-Pacífico –en concreto su Grupo de Trabajo Tecnológico TWG– han remitido un escrito a Google en el que manifiestan su preocupación por sus cambios en la política de privacidad y, en concreto, si se podrá combinar información suministrada por usuarios registrados en un servicio (como Gmail, YouTube o el motor de búsqueda de Google) con información de otros servicios, y también ha señalado la falta de plazos para la eliminación de la información cuando ha sido solicitada por el interesado.
17. La protección de los datos personales de los usuarios fallecidos –un problema que surge habitualmente en el ámbito de las redes sociales– ha sido analizado extensamente en otro momento. El art. 2.a) de la Directiva definía dato de carácter personal como toda información sobre una persona física identificada o identificable, sin aclarar si protegía o no la información relativa a fallecidos, algo que tampoco resuelve la propuesta de Reglamento de la Comisión Europea. Hasta ahora, la mayoría de las leyes se aplican únicamente a las personas naturales o físicas, y se excluye expresamente a los fallecidos (*natural living persons or living individuals*). En España el Reglamento de protección de datos personales establece que no será de aplicación a los datos referidos a personas fallecidas, sin perjuicio de que las personas vinculadas a aquellas puedan dirigirse a los responsables de los ficheros que contengan datos de aquellas personas con la finalidad de notificar el óbito, aportando acreditación suficiente de la persona fallecida y solicitar, en su caso, la cancelación de los datos (art. 2.4). En la misma dirección, la Ley 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen prevé las personas que pueden ejercer las acciones de protección del derecho a la intimidad de la persona fallecida y solicitar la cancelación de su perfil personal –la persona designada en testamento a tal efecto, los familiares directos o el Ministerio Fiscal (arts. 4 y 5).

    Ha existido una evolución en la posición de las redes sociales sobre el mantenimiento de la publicación del perfil personal de una persona tras su muerte. Algunas redes sociales, desde un planteamiento patrimonialista de la propiedad intelectual de lo publicado en su plataforma, continuaban con la publicación del perfil personal de los fallecidos, lo mismo que ocurriría con los blogs escritos para ser difundidos y leídos por internet y que siguen publicados en la red. Inicialmente Facebook se negaba a cerrar los perfiles en internet de las personas fallecidas –esto ocurrió con el perfil del periodista William Bemister, a pesar de las reclamaciones de su hermana. Esta es una cuestión que en nuestro país se planteó con la continuidad de la publicación de los datos y conversaciones privadas de Marta del Castillo

Los usuarios de redes sociales incluyen en sus páginas personales datos de otras personas. En la mayoría de los casos son tratamientos que se encuentran excluidos del régimen de protección de datos personales al ser considerados «ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas» –art. 2.2.a) de la LOPD, una excepción también prevista en el art. 3.2 de la Directiva 95/46/CE– que va destinada a los datos personales que afecten a la esfera familiar y de amistad y que cubre aquellos tratamientos que no pretendan otra finalidad que las relaciones propias de estos ámbitos.[18] La propuesta de Reglamento general de protección de datos también excluye de su ámbito de aplicación material los tratamientos de datos personales que lleve a cabo una persona física en el ejercicio de sus actividades exclusivamente personales o domésticas, y precisa con acierto «siempre que no tengan un interés lucrativo» –art. 2.2.d).[19] Esta cuestión tiene particular interés en el ámbito de las redes sociales, donde, si bien la mayoría de los tratamientos que llevan a cabo los usuarios afecta a la esfera familiar y de amistad –y se encuentran excluidos, por tanto, del ámbito material de aplicación de la normativa–, hay otros tratamientos desarrollados por los usuarios en los servicios de redes sociales que no pueden ser considerados de carácter «personal o doméstico» y que, por tanto, no se encuentran excluidos de la normativa de protección de datos.[20] Esto ocurriría, por ejemplo, cuando los usuarios utilizan el servicio de red social como una plataforma de colaboración con una empresa para una finalidad comercial[21] o como un medio para desarrollar una finalidad de carácter político o social, que no son finalidades personales o domésticas.[22] Igualmente, un número muy elevado de contactos por parte de un usuario implica

obtenidas de la red social Tuenti. En ese caso, Tuenti cerró, a petición de la Fiscalía, su perfil y el de alguno de los adolescentes relacionados con el suceso. En la actualidad las redes sociales cuentan con un protocolo relativo a los datos de personas fallecidas. Facebook establece en su política de privacidad el mantenimiento de las páginas del perfil de los fallecidos «de forma especial y conmemorativa durante un periodo de tiempo determinado, eliminando cierta información sensible» y permite el acceso a la página sólo a los amigos que ya estaban confirmados por el usuario en el momento de su muerte. Al mismo tiempo, Facebook ofrece también a los familiares cercanos la solicitud para cerrar completamente la cuenta del fallecido. Igualmente, Tuenti ofrece a los familiares y personas vinculadas a éste la posibilidad de notificar el fallecimiento de un usuario y solicitar la cancelación del perfil, con los requisitos de acreditación del fallecimiento y de la relación directa. El cierre de la cuenta supone el borrado automático de todos los datos, imágenes y cualquier tipo de información que apareciera del usuario. Por último, hay que señalar que existen redes sociales para fallecidos como Lifestrand, una especie de cementerio virtual con el fin de expresar las condolencias a los familiares, rendirles un homenaje y compartir recuerdos –fotos y vídeos–, que tratan de eternizar su recuerdo a través de internet. Incluso hay empresas que han desarrollado una aplicación para que tras el fallecimiento se publique un mensaje que se grabó con anterioridad.

18. La Audiencia Nacional, en su sentencia de 15 de junio de 2006, ha establecido que se consideran ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas los datos que «afecten a la esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad del tratamiento no sea otra que surtir efectos en estos ámbitos».
19. El considerando 15 de la propuesta pone como ejemplo de tratamientos personales o domésticos la correspondencia y la llevanza de un repertorio de direcciones, sin ningún interés lucrativo y, por tanto, sin conexión alguna con una actividad profesional o comercial. Sin embargo precisa que esta exención no debe aplicarse a los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domésticas.
20. El dictamen 5/2009 del Grupo de Trabajo del Artículo 29 precisa en qué circunstancias las actividades de un usuario de servicios de redes sociales no están cubiertas por la «exención doméstica». Una preocupación de este grupo de trabajo es la difusión y utilización de la información disponible en los servicios de redes sociales con fines secundarios, no buscados. Así, el dictamen 5/2009 señala que una tendencia creciente que se evidencia en los servicios de redes sociales es el paso de la web 2.0 para el ocio a la web 2.0 para la productividad y los servicios.
21. Así, muchas redes sociales especializadas son básicamente redes de profesionales, como LinkedInn, que quiere favorecer las relaciones entre profesionales, o Ryze.com, que hace conexiones de empresas para resolver sus necesidades. Hay que tener en cuenta que la normativa española no protege los datos de personas jurídicas ni los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquellas –cuando constan únicamente nombre y apellidos, funciones o puestos desempeñados, dirección postal o electrónica, teléfono y número de fax profesionales–, ni los ficheros con datos relativos a empresarios individuales, cuando se haga referencia a ellos en su calidad de comerciantes, industriales o navieros (art. 2 del RPDP). Así, la información de relaciones profesionales no forma parte nuclear de la privacidad de las personas. En ese sentido, las redes generalistas tienen un mayor nivel de riesgo ya que no sólo ofrecen información profesional sino también vivencias o aficiones. No obstante, no están excluidos de la LOPD los tratamientos de datos personales de potenciales clientes. MySpace, si bien es una red generalista, dispone de un grupo formado por artistas que la aprovechan para dar a conocer sus trabajos ante el público en general.
22. El hecho de que no se aplique al usuario la excepción de los tratamientos con fines personales o domésticos no significa que no sean de aplicación otras excepciones a los principios y derechos de protección de datos, como son las destinadas a aquellos tratamientos que suponen el ejercicio de otros derechos fundamentales, como la libertad de información y de expresión, que en todo caso se encuentran limitados por

que no conoce a muchos de ellos –consecuencia de una aceptación indiscriminada de peticiones de amistad sin que exista una relación personal–,[23] por lo que no puede hablarse de datos que afecten a la esfera familiar y de amistad o de tratamientos personales o domésticos. Tampoco puede hablarse de un tratamiento «personal o doméstico» cuando el perfil y los contactos personales se encuentran abiertos para todos los usuarios de la red social o cuando la información personal puede ser indexada a través de motores de búsqueda fuera de la propia red. En estos supuestos, el usuario debe ser considerado responsable de tratamiento, y debe aplicársele el mismo régimen que en la publicación de datos personales en otras plataformas tecnológicas de manera abierta en internet. Así, el Tribunal de Justicia de la Unión Europea ha señalado en la sentencia *Lindqvist* que los tratamientos de datos personales que consistan en la publicación de datos de manera que éstos sean accesibles para una pluralidad de personas, aunque sean personales o domésticos y no tengan un interés lucrativo, estarían dentro del ámbito material de aplicación de la normativa de protección de datos.[24] De hecho, la interpretación limitada del concepto de tratamiento personal o doméstico es una consecuencia del principio *pro libertate*, que obliga a una interpretación restrictiva de los límites a un derecho fundamental, especialmente cuando afecta al contenido esencial del derecho y a los intereses jurídicos que le dan vida. Así, excluir estos tratamientos del derecho fundamental a la protección de datos personales afectaría a los intereses jurídicos que dan vida a este derecho –especialmente de terceras personas–, y los dejarían sin protección (STC 11/1981). Este planteamiento es una exigencia del respeto a los derechos de las personas en las redes sociales. Así, no tendría sentido que no pueda aplicarse la normativa de protección de datos personales –y, por tanto, no esté vigente el derecho fundamental a la protección de la información personal– a tratamientos que suponen una cesión indiscriminada de datos –incluso sensibles– de terceras personas a un número muy amplio de usuarios de una red social, a todos los usuarios de esta sin restricciones de acceso o al público en general –a través de motores de búsqueda. Esta publicación de datos personales debe suponer que el usuario de la red social asume la responsabilidad del tratamiento –en relación con las personas cuyos datos y fotografías aparecen publicadas en su perfil–, lo que le obliga, en especial, al cumplimiento de los principios de información y consentimiento y al respeto a los derechos de los afectados que establece la LOPD, así como a la notificación del tratamiento a la Agencia Española –obligación ésta que desaparece en la propuesta de Reglamento y es sustituida por la documentación de los tratamientos. De hecho, el usuario, como más adelante señalaremos, es responsable no sólo ante la Agencia de Protección de Datos sino también tanto en el orden jurisdiccional civil como en el penal por las vulneraciones de los derechos de las personas que se deriven de la información incorporada por éste a la red social.

el derecho a la intimidad, como ha establecido el art. 9 de la Directiva 95/46/CE y los arts. 21.1.f) y 80 de la propuesta de Reglamento general de protección de datos personales –que regula los tratamientos efectuados exclusivamente con fines periodísticos y de expresión literaria o artística. Cfr. sobre esta cuestión nuestra «Introducción y presentación» a *An Approach to Data Protection in Europe,* Thomson-Civitas, APDCM, 2007, págs. 26-33, y, más recientemente, «Hacia un nuevo marco jurídico europeo de protección de datos personales», *loc. cit*.

23. Muchas decisiones en la era de internet –como abrir el nivel de acceso al perfil personal, aceptar una solicitud de amistad, publicar una fotografía en una red social, insertar un comentario en Twitter o contestar un correo electrónico– se toman, a nuestro juicio, en lo que Kahneman ha definido el sistema 1 –el pensamiento más intuitivo y rápido, que requiere un menor esfuerzo mental–, un comportamiento que generalmente incrementa la posibilidad de error y crea problemas a los usuarios. D. Kahneman, premio Nobel en Ciencias Económicas por sus trabajos sobre psicología económica, ha publicado *Thinking, Fast and Slow* –Farrar, Straus and Giroux, Nueva York, 2011, esp. págs. 19-107 y 408-419–, un estudio que cuestiona el modelo racional del juicio y la toma de decisiones. Kahneman ha explicado que existen dos sistemas que conducen a la manera en que pensamos. El sistema 1, que es rápido, intuitivo y emocional, y concluye rápidamente sin esperar a la conciencia racional; y el sistema 2, que es más lento, deliberativo y lógico.

24. Cfr. la sentencia del Tribunal de Justicia de la Unión Europea, de 6 de noviembre de 2003, asunto *Lindqvist*, sobre la catequista sueca que publicó datos personales en internet. Cfr. E. Pérez Luño, *La tercera generación de derechos humanos,* Thomson-Aranzadi, Cizur Menor, 2006, págs. 110-114; M. C. Guerrero Picó, *El impacto de internet en el derecho fundamental a la protección de datos de carácter personal*, Civitas, Cizur Menor, 2006, págs. 356-361. También nosotros hemos señalado que la realización de fotografías de grupos de menores en centros educativos por parte de los padres puede considerarse un tratamiento personal o doméstico pero su publicación en internet en abierto supone un tratamiento que sale de la esfera personal y se constituye en una cesión indiscriminada de datos personales. 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, señala que la protección de estos derechos «quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia». Cfr. nuestra «Introducción y presentación» a *Protección de datos personales para centros educativos públicos,* Civitas-APDCM, Madrid, 2008, pág. 55.

3. La información y el consentimiento del interesado para el tratamiento y para las cesiones a la luz de la propuesta de Reglamento general de protección de datos personales, el establecimiento de niveles de acceso y la inclusión de datos de otras personas en el propio perfil

El artículo 6 de la propuesta de Reglamento mantiene las condiciones de licitud de los tratamientos presentes en el artículo 7 de la Directiva y los especifica más en profundidad.[25] En especial, la propuesta fija las condiciones para que el consentimiento sea válido como fundamento jurídico del tratamiento lícito. El cambio más relevante se encuentra en el capítulo I –disposiciones generales–, y más concretamente en las definiciones donde desaparece la legitimidad del consentimiento tácito. El consentimiento es para la propuesta de Reglamento toda manifestación de voluntad no sólo libre, específica, informada sino también *explícita*, «mediante la que el interesado acepta, ya sea mediante una declaración, ya sea mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen». Se trata, como señala la exposición de motivos, de «dotarse de una definición única y coherente que garantice que el interesado es consciente de que da su consentimiento y a qué lo da».[26] Por tanto, el consentimiento explícito para el tratamiento de datos personales será plenamente de aplicación a los servicios de redes sociales. Posiblemente, la mejora de las tecnologías de la comunicación ha facilitado la posibilidad de exigir el consentimiento explícito, algo que en el pasado podía ralentizar la relación jurídica en internet. Se establecen ahora algunos rasgos nuevos en relación con el consentimiento, que ya estaban señalados por la doctrina y la jurisprudencia: que la carga de la prueba del consentimiento la tiene el responsable del tratamiento, que el consentimiento para el tratamiento debe ser distinguido de cualquier otra dación de consentimiento para otro asunto y que el consentimiento no es una base jurídica válida cuando existe un desequilibrio entre el interesado y el responsable del tratamiento. Como señala la exposición de motivos de la propuesta de Reglamento, a juicio de la Comisión, era necesaria una interpretación clara y uniforme del consentimiento válido en toda la Unión Europea que dé seguridad jurídica a los agentes económicos.

Por tanto, la recogida de datos personales por el proveedor del servicio de red social así como las posibles cesiones tienen que hacerse mediante el consentimiento libre, inequívoco, específico e informado del interesado –art. 3.h) de la LOPD–, así como explícito. Debe ser el usuario el que dé su consentimiento y establezca el nivel de acceso a su perfil personal –a sus amigos, a los amigos de sus amigos, a toda la red social o fuera de ella permitiendo la indexación por motores de búsqueda. Este consentimiento se ejerce habitualmente aceptando la política de privacidad establecida por defecto, una cuestión que después analizaremos.[27] El interesado, de esta forma, consiente el tratamiento de sus datos personales por el servicio de red social. Sin embargo, el interesado no consiente los tratamientos de sus datos que se llevan a cabo en las páginas personales de otros usuarios. El consentimiento es un derecho del usuario y una obligación del responsable de la red social como responsable del tratamiento; por tanto, no es una obligación legal del usuario, salvo que también sea responsable del tratamiento en los términos antes señalados[28] o salvo que la información revelada por el usuario afecte al derecho a la intimidad, honor y propia imagen de otras personas y supere los usos admitidos socialmente (art. 2.1 de la Ley orgánica 1/1982,

25. Así, los tratamientos de datos personales se consideran legítimos si existe consentimiento, relación contractual, obligación jurídica del derecho de la Unión o de la legislación del Estado, cumplimiento de una misión de interés público o inherente al ejercicio de poder público y satisfacción del interés legítimo del responsable.
26. De esta forma, la propuesta de Reglamento es más garantista que la Carta de Derechos Fundamentales de la Unión Europea que señala que el consentimiento ha de prestarse de forma inequívoca (art. 8). Esto estaba en línea con la Directiva que consideraba únicamente como rasgos esenciales del consentimiento que fuera libre, específico e informado –art. 2.h)–, e inequívoco –art. 7.a). En cambio, el consentimiento expreso o explícito se requería únicamente para el tratamiento de categorías especiales de datos –art. 8.2.a) de la Directiva y art. 7 de la LOPD.
27. Existen distintas medidas que pueden implantar los servicios de redes sociales para limitar las injerencias en la privacidad de las personas. Así, la 30.ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de Estrasburgo del año 2008 estableció que los servicios de red social deben tomar medidas eficaces para impedir el «spidering» y/o las descargas en masa de datos de perfil por parte de terceros.
28. La publicación excesiva de información de terceros –fotos– sin consentimiento de estos ha sido sancionada por la Agencia Española (procedimiento sancionador 000117/2008).

de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen). Hay que recordar de nuevo la distinción existente entre el proveedor del servicio de red social, que es el responsable del tratamiento, y el usuario ya que las cesiones que haga este último en un ámbito restringido pudieran entenderse como un tratamiento para fines personales, familiares o domésticos, que están excluidos de la Directiva 95/46/CE y de la LOPD.[29] Un modelo ideal sería que los usuarios no cedieran datos de otras personas –por ejemplo, imágenes de grupo– sin su consentimiento. A este criterio tienen que ir encaminados todos los códigos de buenas prácticas y la concienciación de los usuarios. Sin embargo, muchas redes sociales permiten el tratamiento de datos de otras personas –por ejemplo, la fotografía o su etiquetado– sin este consentimiento. Hay que ser conscientes de que no siempre es fácil solicitar y obtener el consentimiento de todas las personas que aparecen en una fotografía. La publicación por parte de los usuarios de redes sociales de datos personales de terceros sin su consentimiento –por ejemplo, fotografías–, aunque sea entre amigos y para un círculo restringido, es una cuestión compleja desde el punto de vista del derecho a la intimidad y a la imagen. Parece razonable que la publicación para un número limitado de amigos y, por tanto, con el máximo grado de privacidad –y no para amigos de amigos, toda la red social y todo internet– pueda considerarse un uso admitido socialmente, que en este caso formaría parte de un tratamiento familiar o doméstico, lo que significa que no se considera una intromisión ilegítima que deba ser perseguida –por otra parte, no sería posible hacerlo– y siempre que la información publicada no afecte a la intimidad de una persona. No obstante, la existencia de una oposición del interesado debería bastar para la supresión de esta información de esta comunidad restringida y es importante, por ello, que las redes sociales tengan canales de denuncia que lo permitan.[30]

Como hemos señalado anteriormente, el usuario de los servicios de red social que no lleva a cabo tratamientos personales o domésticos –bien porque desarrolla una actividad comercial, empresarial o profesional a través de la red social, bien porque mantiene un número muy elevado de contactos, bien porque establece su perfil personal con datos de otras personas abierto a todos los usuarios de la red social o indexable a través de buscadores fuera de la red social– es el responsable del tratamiento de los datos de otras personas publicados en su perfil y está obligado por ello a cumplir los principios y derechos de protección de datos, en especial, el principio de consentimiento. Hemos analizado en otro momento las excepciones a algunos principios de protección de datos, especialmente el consentimiento, en los tratamientos de los datos personales efectuados exclusivamente con fines periodísticos o de expresión literaria o artística, algo frecuente en el ámbito de las redes sociales, y la necesidad de conciliar el derecho a la protección de los datos personales con la libertad de expresión, una previsión

29. Los usuarios de redes sociales tratan en muchas ocasiones datos de personas que no son miembros de la red social y que no han dado su consentimiento. Lo esencial es que el propio servicio de red social como responsable del tratamiento no lleve a cabo un tratamiento de estos datos personales –por ejemplo, no cree perfiles de no miembros prerrellenados ni invite a no miembros a adherirse a la red. Este es el sentido que hay que darle a este apartado del dictamen 5/2009 del Grupo de Trabajo del Artículo 29: «Muchos servicios de redes sociales permiten a los usuarios proporcionar datos sobre otras personas, como añadir un nombre a una imagen, evaluar a una persona, o poner una lista de "gente que he conocido/quiero conocer" en acontecimientos. Esta información puede identificar también a no miembros. Sin embargo, el tratamiento de este tipo de datos relativos a no miembros por el SRS sólo puede realizarse si se cumple uno de los criterios contemplados en el artículo 7 de la Directiva relativa a la protección de datos. Además, la creación de perfiles de no miembros prerrellenados mediante la agregación de datos proporcionados independientemente por usuarios de SRS, incluidos los datos afines deducidos de las listas de contactos en línea, no tiene ninguna base jurídica. Incluso aunque el SRS tuviese los medios para ponerse en contacto con el no usuario e informarle de la existencia de datos personales relativos a él, una posible invitación por correo electrónico para adherirse al servicio de red social con el fin de acceder a estos datos personales violaría la prohibición prevista en el artículo 13, apartado 4, de la Directiva sobre la privacidad y las comunicaciones electrónicas, relativa al envío de mensajes electrónicos no solicitados con fines de comercialización directa».

30. El dictamen 5/2009 plantea la implementación de herramientas que mejoren el consentimiento entre los usuarios miembros de la red social. Se habla así de la «introducción de herramientas de gestión de etiquetas de la información en los sitios de redes sociales, en particular, creando espacios en un perfil personal para indicar la presencia de un nombre de usuario en imágenes o vídeos con etiqueta que estén a la espera del consentimiento del usuario en cuestión, o fijando plazos de expiración para las etiquetas que no hayan recibido el consentimiento de la persona señalada». Así, por ejemplo, Tuenti ofrece a sus usuarios en las «condiciones de uso» mecanismos técnicos para el borrado de una foto, para quitar una «etiqueta» que marca una fotografía que identifica a un usuario y para su denuncia. Además, informa de que los usuarios no están autorizados a subir fotografías sin haber obtenido el oportuno consentimiento de las personas que en ellas pudieran aparecer.

que se encuentra en los arts. 80 y 21.1.f) de la propuesta de Reglamento y en el art. 9 de la Directiva.[31] Además, el art. 7.f) de la Directiva 95/46/CE –que se mantiene en el art. 6.1.f) de la propuesta de Reglamento– permite el tratamiento de datos personales sin consentimiento del interesado cuando concurran dos requisitos acumulativos: que sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y que no prevalezcan los derechos y libertades fundamentales del interesado, lo que exige una ponderación que dependerá de las circunstancias concretas en cada caso. Este precepto tiene efecto directo, como ha recordado recientemente el Tribunal de Justicia de la Unión Europea, en la sentencia de 24 de noviembre de 2011.[32] El tratamiento de datos de otras personas sin consentimiento previsto en el art. 7.f) de la Directiva podría encontrar su justificación en la satisfacción de un interés legítimo si el número de contactos es reducido o el acceso al perfil personal está restringido –estaríamos hablando, además, en este caso, de un usuario que lleva a cabo un tratamiento personal o doméstico y no de un responsable de tratamiento. Sin embargo, cuando el usuario se convierte en responsable del tratamiento por tener un muy elevado número de contactos personales o un perfil abierto, el tratamiento de datos de otras personas sin su consentimiento en su perfil personal difícilmente podría justificarse en la satisfacción de un interés legítimo de éste y no superaría el *balance test* que obliga a llevar a cabo una ponderación, valorando la posible prevalencia de los derechos y libertades de los interesados. A nuestro juicio, la cláusula del equilibro de intereses que prevé el art. 6.1.f) de la propuesta de Reglamento –y el art. 7.f) de la Directiva– puede justificar la ausencia del consentimiento del interesado para los tratamientos de datos personales o la cesión de datos a un concreto cesionario en la actividad económica o de prospección comercial –especialmente cuando estos datos consten en fuentes accesibles al público, como señalaba la legislación española, porque implica una menor gravedad de la injerencia, sin perjuicio de no poder excluir los tratamientos sin consentimiento de otros datos que no figuren en fuentes accesibles al público. Sin embargo, la inclusión de datos de otras personas en un perfil personal con un número muy elevado de contactos o abierto a todos los usuarios de red social sin restricciones de acceso o al público en general a través de motores de búsqueda implica una publicación de datos personales que en muchas ocasiones no permite identificar al cesionario y, por tanto, supone una cesión indiscriminada de datos –incluso sensibles– donde el interesado pierde el control de su información personal.

Los proveedores de redes sociales no pueden tratar datos de ideología, religión o creencias de los usuarios sin el consentimiento expreso y escrito de éstos y con expresa advertencia del derecho a no prestarlo (arts. 7.1 y 2 de la LOPD). Los datos de raza, salud o vida sexual de los usuarios no pueden ser objeto de tratamiento por el servicio de red social sin el consentimiento expreso del usuario (art. 7.3 de la LOPD). Además, los formularios de inscripción en la red social deben señalar expresamente que esta información es voluntaria. La LOPD prohíbe expresamente los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico o vida sexual (art. 7.4), lo que debe ser tenido en cuenta por las empresas proveedoras de estos servicios a la hora de configurar la organización de grupos. Estamos hablando, de nuevo, de las obligaciones del responsable del tratamiento y, por tanto, de los derechos del usuario. Lógicamente, estos criterios son de aplicación al usuario que es al mismo tiempo responsable del tratamiento –en los supuestos antes señalados–, de forma que éste, por ejemplo, no puede publicar datos sensibles de otras personas en abierto en internet sin los mismos requisitos de consentimiento antes señalados. Si bien la legislación de protección de datos personales no se aplica a los tratamientos personales, familiares o doméstico, la obligación que tiene toda persona –no sólo el responsable del tratamiento– de respetar el derecho a la intimidad de los demás y las eventuales responsabilidades penales o civiles al margen del derecho fundamental a la protección de datos personales que pueden derivarse de su incumplimiento obligan a los usuarios a ser especialmente cautos y a respetar en este caso el principio de consentimiento. Así, hay que recordar que los datos de ideología, afiliación sindical, religión o creencias, raza, salud o vida sexual afectan a la esfera más íntima de una persona por lo que su revelación en una red social –aunque sea a un círculo restringido que

31. Esta cuestión la hemos abordado en «Hacia un nuevo marco jurídico europeo de protección de datos personales», *loc. cit.*
32. El Tribunal de Justicia ha recordado que el art. 7.f) es una disposición suficientemente precisa y establece una obligación incondicional, por lo que concurren los requisitos de la jurisprudencia –sentencia del Tribunal de Justicia de las Comunidades Europeas *Simmenthal*, 1978– para atribuirle un efecto directo, de forma que puede ser invocado directamente por un particular y aplicado por los órganos jurisdiccionales nacionales, aunque no exista transposición.

no haga del usuario un responsable del tratamiento– puede suponer igualmente la vulneración del derecho a la intimidad de la persona. Por tanto, si como criterio general un usuario no debería revelar información de otras personas sin su consentimiento, esto dispone de un especial refrendo normativo cuando hablamos de datos especialmente protegidos. En todo caso, hay que recordar que una excepción a la prohibición de tratamiento de categorías especiales de datos es que el interesado los haya hecho manifiestamente públicos –art. 9.2.e) de la propuesta de Reglamento, que también se encuentra en el art. 8.2.e) de la Directiva 95/46/CE.

La mayoría de las redes sociales anima a los usuarios a que inviten a sumarse a la red social a sus contactos personales. Así, en el momento de la inscripción, los usuarios son invitados a enviar un correo electrónico a sus contactos en su agenda de direcciones electrónicas. La Directiva 2002/58/CE, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, exige como regla general el consentimiento del interesado para la recepción de comunicaciones comerciales no solicitadas. Si bien existe una invitación por parte de la red social que es la responsable del tratamiento, estamos hablando en este caso de una comunicación personal por lo que no es de aplicación la prohibición de utilizar el correo electrónico con fines de comercialización directa, siempre que se cumplan una serie de requisitos.[33] En todo caso, la inclusión de estos contactos dentro de la red social sólo puede hacerse con su consentimiento. Igualmente, las redes sociales tienen un servicio de notificación de novedades en el propio perfil o en el de sus contactos cuando, por ejemplo, alguien ha agregado su perfil a la lista de contactos de otra persona, se le invita a participar en un grupo o alguien ha etiquetado su foto. La incorporación a este servicio de notificación debe hacerse también con el consentimiento del interesado.

Es especialmente importante el cumplimiento del principio de información (art. 5 de la LOPD),[34] de forma que el titular de los datos debe ser previamente informado: en primer lugar, de la existencia de un fichero y de un tratamiento con sus datos personales –hay que informar, por tanto, de la recogida de *cookies*–, de todas las finalidades del tratamiento –debe informarse si los datos de los perfiles van a ser empleados con fines distintos de la participación en la red, como, por ejemplo, para fines publicitarios o de marketing– y de los cesionarios o destinatarios de la información –debe informarse de los niveles de acceso y de las categorías, qué tipo de datos van a ser cedidos y la finalidad, si se va a hacer publicidad de los distintos perfiles, si la información puede ser indexada por cualquier buscador o si se prevén transferencias a países no miembros de la Unión Europea que no ofrecen el mismo nivel de protección–;[35] en segundo lugar, del carácter obligatorio o facultativo de la respuesta –las redes sociales incentivan a través de impresos la incorporación del mayor número de datos posibles pero no informan de qué casillas son necesarias para la incorporación a la red social y cuáles son opcionales–; en tercer lugar, de las consecuencias de la obtención de los datos y de la negativa a suministrarlos; en cuarto lugar, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y en quinto lugar, de la identidad y dirección postal y electrónica del responsable del fichero y del servicio para el ejercicio de los derechos antes señalados –es muy importante que los proveedores de servicios de redes sociales informen a los usuarios de su identidad.[36] Es necesario que se lea y se acepte expresamente la política de privacidad antes de la publicación del perfil con datos personales en la red social. Así, no debe ser posible la introducción de ningún dato sin que el afectado haya dado su consentimiento expreso, en el que acepte los términos y condiciones de la política de privacidad de la red social. Sin embargo, no todas las redes sociales cumplen la normativa de protección de datos

33. Para que estas invitaciones que hacen los usuarios cumplan la excepción de las comunicaciones personales, el dictamen 5/2009 del Grupo de Trabajo del Artículo 29 señala que el servicio de red social debe cumplir los siguientes criterios: no incentivar al remitente ni al destinatario; el proveedor no debe seleccionar a los destinatarios; la identidad del remitente debe mencionarse claramente; y el remitente debe conocer todo el contenido del mensaje que se enviará en su nombre.
34. Estas exigencias son aplicables para las redes sociales sometidas a la LOPD ya que las obligaciones de información de la Directiva son más flexibles.
35. El dictamen 5/2009 del Grupo de Trabajo del Artículo 29 incide en la importancia de que se informe de la utilización de los datos con fines de comercialización directa; de la posible distribución de datos a categorías específicas de terceros; de una reseña de los perfiles –su creación y sus principales fuentes de datos– y de la utilización de datos sensibles.
36. Cfr. el documento del Grupo de Trabajo del Artículo 29 «Recomendación sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea», aprobado el 17 de mayo de 2001. Este documento señala que la no mención de los destinatarios equivale al compromiso de no comunicar información personal. Cfr. también el documento del Grupo de Trabajo del Artículo 29: «Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea», adoptado el 21 de noviembre de 2000.

personales en este punto. La política de privacidad no está destacada suficientemente en las páginas de inicio y en las fases de registro.[37] No existe un conocimiento de quién posee mis datos, para qué finalidad; tampoco se informa de los derechos del afectado ni se conocen de manera completa las posibles cesiones y el almacenamiento de *cookies*.[38] Existe una apariencia de consentimiento pero el incumplimiento del principio de información implica que no existe un consentimiento informado.[39]

La propuesta de Reglamento general de protección de datos personales introduce el principio de transparencia –que los datos serán tratados de manera transparente en relación con el interesado del art. 5.a)–, lo que tiene consecuencias para los servicios de redes sociales en relación con la información al interesado y, como señalaremos más adelante, con el derecho de acceso. Así, la información al interesado debe incluir no sólo los fines del tratamiento sino también el interés legítimo del responsable; debe contener, además, información sobre el plazo dentro del cual se conservarán los datos personales, la fuente de la que proceden los datos –esto ya estaba en la LOPD–, el derecho a presentar una reclamación ante la autoridad de control y, en su caso, la intención del responsable de efectuar una transferencia internacional y el nivel de protección del tercer país.

Cita recomendada

TRONCOSO REIGADA, Antonio (2012). «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte una». En: «Retos y oportunidades del entretenimiento en línea» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. Número 15, pág. 61-75. UOC. [Fecha de consulta: dd/mm/aa]
<http://idp.uoc.edu/ojs/index.php/idp/article/view/n15-troncoso/n15-troncoso-es>
DOI: http://10.7238/idp.v0i15.1646
ISSN 1699-8154

37. Muy pocas personas leen la política de privacidad –donde se señala la explotación de la información por intereses económicos–, especialmente los jóvenes. Hay que destacar que los *digital natives* son objeto de un interés específico por las compañías de publicidad.
38. Cfr. el Informe de la Agencia Española de Protección de Datos sobre buscadores de Internet, de 1 de diciembre de 2007, accesible en la web de la Agencia.
39. Algunos de los criterios relativos a la protección de datos personales en la Administración electrónica son también trasladables a las redes sociales. Cfr. nuestro trabajo «La Administración electrónica y la protección de datos personales», *loc. cit.*

Sobre el autor

Antonio Troncoso Reigada
antonio.troncosoreigada@uca.es
Profesor Titular de Derecho Constitucional de la Universidad de Cádiz

Es profesor titular de Derecho constitucional de la Universidad de Cádiz. Ha sido director de la Agencia de Protección de Datos de la Comunidad de Madrid de 2001 a 2010, habiendo sido designado para un segundo mandato por unanimidad de todos los grupos políticos y centrales sindicales. Ha tenido el primer Premio Nacional de terminación de estudios universitarios y el premio extraordinario de licenciatura en la Universidad Complutense (1991). Es doctor en Derecho por la Universidad de Bolonia con la calificación *summa cum laude*. Ha obtenido el premio Nicolás Pérez Serrano a la mejor de tesis doctoral de derecho público del año 1993. Ha recibido el Premio Nacional de investigación del Ministerio de Justicia 2010 por el tratado *La protección de datos personales: en busca del equilibrio*, Tirant lo Blanch, Valencia, 2010. Es miembro del Consejo Consultivo de la Agencia Española de Protección de Datos en representación del Consejo de Universidades. Ha sido también director general de Calidad de los Servicios y del Instituto de Estadística de la Comunidad de Madrid en el gobierno de Ruiz Gallardón; director del Gabinete Técnico de la Subsecretaría del Ministerio de Sanidad y Consumo, y secretario general de la Universidad de Cádiz.

Facultad de Derecho.
Universidad de Cádiz
Avda. de la Universidad s/n
Campus de la Asunción, 111405 JEREZ.