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

www.uoc.edu/idp

ARTÍCULO

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

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: junio de 2013

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 2

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

(continuación)

4. El principio de calidad en el servicio de red social, la conservación de la información y las medidas de seguridad. Las obligaciones que la propuesta de Reglamento general de protección de datos personales fija al responsable del tratamiento: los *privacy impact assessment* (PIA)

Las redes sociales deben cumplir el principio de calidad como principio de finalidad –art. 4 de la LOPD–. Estas plantean riesgos potenciales de utilización de la información para otras finalidades –por ejemplo, para el *marketing* personalizado–, lo que no puede hacerse sin la información y el consentimiento del interesado. No siempre es fácil evitar los tratamientos de datos personales excesivos, sobre todo cuando el interesado es el que quiere y decide que aparezcan en su perfil personal. En todo caso, como hemos señalado, el servicio de red social no debe exigir ningún dato personal excesivo en la solicitud de inscripción en la red social, y debe indicar claramente qué datos son obligatorios y cuáles facultativos. La información en la red social frecuentemente no se encuentra actualizada –porque el usuario no lo hace–. Es importante que los datos personales sean cancelados cuando hayan dejado de ser necesarios, lo que impone un conjunto de obligaciones al proveedor del servicio en relación con la conservación de la información. La conservación de las copias por un tiempo indeterminado no es aceptable.[2] Como regla general, el responsable de la red social no puede conservar copias archivadas de los perfiles de los usuarios que han abandonado la red social para sus propias finalidades y mucho menos por un tiempo indeterminado. Igualmente, la información suprimida por el usuario al actualizar su página personal no debe conservarse por el proveedor de servicio de red social para sus propios fines. En esta dirección, algunas exigencias incluidas en el Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 que establecen límites a la conservación de la información por las redes sociales en supuestos de no utilización del servicio por el usuario van encaminadas a facilitar el control de la propia información personal.[3] Por ello, los responsables de las redes sociales solo están facultados para conservar esta información bloqueada durante el tiempo necesario para la persecución de infracciones penales o administrativas; más allá de este plazo la información debe ser suprimida. Existen supuestos donde el responsable de la red social conserva alguna información de los usuarios que han abandonado la red social como instrumento de autorregulación. Así, el Dictamen 5/2009 antes citado señala que algunos servicios de red social conservan los datos de identificación de los usuarios suspendidos del servicio, con el fin de garantizar que ya no podrán registrarse de nuevo, y debe informarse al interesado de que se realiza este tratamiento. Para el Grupo de Trabajo del Artículo 29, la única información que puede conservarse es la información de identificación y no las razones por las que se suspendió a estas personas y esta información no deberá conservarse durante más de un año. Sin embargo, este planteamiento supone un límite a las facultades de autorregulación –que también pueden garantizar el derecho fundamental a la protección de datos personales–, además de no dejar de ser un supuesto de conservación de la información «para los fines para los que fueron recogidos» –art. 6.1 de la Directiva 95/46/CE– entre los que estaría la propia autorregulación. No parece razonable exigir unas obligaciones de mantener limpia la red social al proveedor del servicio al mismo tiempo que se dificulta la penalización de las conductas infractoras o su persecución en el futuro.

La regulación que la propuesta de Reglamento general de protección de datos personales hace de los principios relativos al tratamiento de datos personales y que se desarrolla

2. El Grupo de Trabajo del Artículo 29, en su Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, emitido el 4 de abril de 2008, señala que la retención de datos personales por estos no debía superar los seis meses. Esta es una cuestión que hemos analizado en «Transparencia administrativa y protección de datos personales», *loc. cit.* págs. 67-75.
3. Así, se señala que cuando un usuario no utiliza el servicio durante un período determinado, el perfil debería desactivarse, dejando de ser visible para otros usuarios o para el exterior, y, después de otro periodo, los datos de la cuenta abandonada deberían suprimirse. En todo caso, los servicios de redes sociales antes de proceder a esta cancelación deben informar a los usuarios a través de los medios de que dispongan. Otro caso distinto es que los datos personales comunicados por un usuario cuando se registra en un servicio de red social deban suprimirse en cuanto el usuario o el proveedor de servicios de red social decidan suprimir la cuenta.

en el capítulo II –arts. 5-10– no aporta una especial novedad,[4] tampoco en lo que respecta al principio de calidad y de finalidad. En todo caso, precisa el principio de prohibición de exceso –un principio de minimización de datos, en términos de la Comisión–, que obliga a que «los datos sean limitados al mínimo necesario en relación a los fines para los que se traten» y «solo se tratarán si y siempre que estos fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales» –art. 5.c) de la propuesta de Reglamento–.[5] De esta forma, los prestadores de servicios de internet como las redes sociales tienen la obligación de limitar la recogida de datos al mínimo necesario.[6]

La propuesta de Reglamento sí fija un conjunto de obligaciones al responsable del tratamiento –capítulo IV, arts. 22 al 37–, que no estaban en la Directiva 95/46/CE y que son aplicables a los servicios de red social, como la documentación del respeto a los principios y derechos en el tratamiento de datos personales,[7] el cumplimiento de requisitos en materia de autorización o consultas previas con la autoridad de control o la realización de una auditoría independiente externa o interna de la observancia de la normativa y no limitada a las medidas de seguridad. La propuesta de Reglamento introduce como obligación del responsable la realización con carácter previo de una evaluación de impacto relativa a la protección de datos –los *privacy impact assessment* (PIA)–, cuando los tratamientos entrañen riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance o fines –art. 33–, y se establece incluso en estos supuestos la necesidad de que el responsable o el encargado obtenga con carácter previo al tratamiento de estos datos una autorización o lleve a cabo una consulta a la autoridad de control –art. 34–. La evaluación de impacto sería necesaria porque los servicios de red social llevan a cabo un tratamiento a gran escala de datos de aficiones, de datos especialmente protegidos –de vida sexual o de salud cuando los incluye el usuario–, de menores y suponen una evaluación indirecta de aspectos personales o de las preferencias personales de los usuarios, sin perjuicio de que los servicios de red social no vayan a tomar medidas que produzcan efectos jurídicos o afecten significativamente a las personas.[8] La propuesta de Reglamento incluye también la obligación de designar un delegado de protección de datos personales –*data protection officer*– con la función de velar por el cumplimiento de la normativa de protección de datos personales en el ámbito interno del responsable cuando la actividad principal del responsable consista en operaciones de tratamiento que, en razón de su naturaleza, alcance o fines requieran un seguimiento periódico y sistemático de los interesados –art. 35.1.c)–, algo que se aplica a las empresas que prestan servicios de red social.

La Directiva 95/46/CE dejaba un amplio margen de maniobra a los Estados a la hora de implementar la seguridad de los tratamientos de datos personales. La propuesta de Reglamento regula la seguridad entre las obligaciones del responsable y del encargado del tratamiento. Una de las novedades que presenta la regulación de la seguridad de los datos en la propuesta de Reglamento es la necesidad de realizar una evaluación de riesgos, que permita adoptar las medidas para proteger los datos contra su destrucción accidental o ilícita, su pérdida accidental o cualquier tratamiento ilícito como la comunicación, la difusión, el acceso no autorizado o la alteración de los datos personales. Existe una preocupación específica no solo por impedir cualquier acceso no autorizado sino también por evitar cualquier forma no autorizada de comunicación, lectura o copia. Además, se establece la obligación de notificación de la

4. De hecho, el considerando 7 de la Propuesta de Reglamento, recogiendo el parecer de las consultas previas a las partes interesadas, señala que los principios generales de la Directiva 95/46/CE «siguen siendo válidos y actuales».
5. Estos criterios también se aplican a los tratamientos para fines de investigación histórica, estadística o científica –art. 83 de la propuesta de Reglamento–. El principio de calidad como principio de prohibición de exceso lo hemos analizado en «El principio de calidad de los datos», A. Troncoso Reigada (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, cit. págs. 344-360.
6. De hecho, la propuesta de Reglamento establece como novedad que el responsable del tratamiento no está obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir las disposiciones del Reglamento –art. 10.
7. Establece que el responsable del tratamiento de datos «para cada operación de tratamiento, garantizará y demostrará el cumplimiento de las disposiciones del presente Reglamento» –art. 5.f)–, lo que transforma las obligaciones del responsable del capítulo IV en un principio general de responsabilidad.
8. La exposición de motivos de la propuesta de Reglamento prevé que la evaluación de impacto abarque aplicaciones o plataformas comunes de tratamiento o cuando se plantee introducir una aplicación o un entorno de tratamiento común en un sector para una actividad horizontal de uso generalizado –considerando 72–. Este informe de evaluación de impacto en la privacidad debe contener la descripción general del tratamiento, los riesgos para los derechos y libertades de los interesados y las medidas contempladas para hacer frente a los riesgos y para garantizar el cumplimiento de la normativa y el respeto de los derechos e intereses legítimos de las personas afectadas.

violación de los datos personales a la autoridad de control y su comunicación al interesado –arts. 31-32–, más conocida por brechas de seguridad –las llamadas «BCR»–. La propuesta de Reglamento no incluye una referencia a niveles de seguridad ni tampoco un conjunto de medidas de seguridad que se deban implementar sino que, al igual que el artículo 9 de la LOPD que prevé su desarrollo reglamentario, y a diferencia de la Directiva, faculta a la Comisión para realizar los actos normativos necesarios para especificar las medidas técnicas y organizativas, lo que incluye la referencia a sectores específicos y situaciones de tratamiento de datos específicas –entre los que están, sin duda, los servicios de red social–, teniendo en cuenta no solo la evolución de la tecnología, sino también las soluciones de privacidad desde el diseño y la protección de datos por defecto. Hasta que entre en vigor la propuesta de Reglamento y su desarrollo normativo, las redes sociales tienen que implantar las medidas de seguridad establecidas en las legislaciones nacionales, en virtud de la tipología de datos personales sometidos a tratamiento, algo especialmente importante en nuestro país ya que desde el año 1999 la normativa obliga a establecer unas concretas medidas de seguridad –artículo 9 de la LOPD, desarrollado primero por el Real Decreto 994/1999, de 11 de junio, ya derogado, y ahora por el Real Decreto 1720/2007, de 21 de diciembre–. Inicialmente puede parecer que las redes sociales deben adoptar medidas de seguridad de nivel medio ya que son tratamientos que ofrecen un perfil de las personas y permiten evaluar aspectos de su personalidad. Sin embargo, a nuestro juicio es necesario implantar medidas de seguridad de nivel alto ya que en muchas ocasiones se tratan datos de origen racial, ideología, orientación sexual, lo que implicaría, entre otras cosas, la existencia de un registro de accesos y la encriptación de las comunicaciones. Hay que señalar que la voluntad del titular de los datos de compartir una determinada información con un círculo de personas significa la determinación de excluir al resto de los miembros de la red social del conocimiento de esta información, lo que obliga a establecer herramientas que garanticen esta confidencialidad. Evitar los accesos indebidos a la información de los perfiles debe constituir una de las principales preocupaciones de las redes sociales. En todos los ámbitos de la sociedad de la información –comercio electrónico, administración electrónica, redes sociales virtuales–, la seguridad de la información es un elemento esencial para la confianza de los usuarios y para el desarrollo de la economía digital.

5. Los derechos de las personas y las vías de reclamación. El derecho al olvido en internet y a la portabilidad de los datos en la propuesta de Reglamento general de protección de datos personales. La protección de los menores. La autorregulación

El derecho de acceso permite al interesado conocer sus datos personales sometidos a tratamiento, el origen de ellos y las comunicaciones realizadas o que se prevé hacer a terceras personas –art. 15 de la LOPD–. Igualmente, el interesado tiene derecho a rectificar sus datos si son inexactos o incompletos y a cancelarlos –art. 16 de la LOPD–. El titular de los datos también puede revocar el consentimiento para el tratamiento, así como ejercer el derecho de oposición –art. 6 de la LOPD–, notificándoselo al responsable. En especial, los responsables de los servicios de red social tienen que respetar el ejercicio del derecho de cancelación cuando los usuarios desean hacer desaparecer parte de la información que han publicado en su perfil personal o darse de baja de la propia red social,[9] sin perjuicio de las obligaciones de bloqueo que tiene el responsable o de la necesidad de conservar determinada información a efectos de autorregulación, como antes hemos señalado. También el responsable del servicio de red social tiene que respetar el derecho de oposición del usuario a determinados tratamientos de datos personales –por ejemplo, para finalidades comerciales, o cuando desea modificar el nivel de acceso a su perfil personal para restringirlo o para impedir la indexación por los buscadores–. Lógicamente, el ejercicio de estos derechos no se limita a los usuarios de la red social sino también a todas las personas cuyos datos personales son sometidos a tratamiento, entre los que pueden estar personas que

9. El responsable del servicio de red social debe resolver la solicitud de cancelación y hacerla efectiva en un plazo máximo de diez días a contar desde su recepción. Transcurrido este plazo sin que se responda a la petición de manera expresa, esta puede entenderse desestimada. En el caso de que el responsable no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo –art. 32 del RPDP.

no son miembros de la red social. Los responsables de los servicios de red social no deben limitarse a garantizar estos derechos sino que deben facilitar su ejercicio, aunque no sea a través del procedimiento previsto expresamente por el responsable –incluso a través de los servicios de atención al público y de reclamaciones–, adoptando las medidas oportunas para que todas las personas de su organización informen al interesado del procedimiento que ha de seguir para ejercer sus derechos –art. 24 del RPDP–. Así, como señala el Dictamen 5/2009, del Grupo de Trabajo del Artículo 29, «como mínimo, en la página inicial de los SRS debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos».

Lógicamente, el ejercicio de estos derechos de acceso, rectificación, cancelación y oposición se realiza ante el responsable del tratamiento, que serán las empresas proveedoras del servicio de red social,[10] no ante el resto de usuarios de la red social, salvo que estos tengan también el carácter de responsables del tratamiento. Sin embargo, como ya hemos señalado, en muchas ocasiones el interesado detecta el tratamiento de sus datos personales –por ejemplo, su fotografía– por parte de otros usuarios sin su consentimiento. Las redes sociales tienen procedimientos de denuncia para oponerse al tratamiento de datos personales por parte de otros usuarios.[11] Si bien estos tratamientos se encuentran excluidos del ámbito de aplicación de la LOPD al tratarse de ficheros personales o domésticos, los usuarios deben respetar en todo caso los derechos a la intimidad, al honor o a la propia imagen de otras personas. Comentarios de naturaleza injuriosa o calumniosa sobre la vida profesional, publicación de fotografías íntimas, creación de perfiles falsos, por poner solo algunos ejemplos, pueden ser delitos o faltas tipificados en el Código Penal –arts. 205 y 208–[12] o dar lugar a una responsabilidad civil por vulneración del derecho al honor, a la intimidad personal y familiar y a la propia imagen, desarrollados en la Ley Orgánica 1/1982, de 5 de mayo. En todo caso, hay que señalar que los titulares de redes sociales tienen una gran dificultad técnica para llevar a cabo una cancelación efectiva de los datos personales. Así, si bien las redes permiten dar de baja el perfil o borrar parte de la información, persisten en los perfiles de los demás usuarios los comentarios, los mensajes cruzados o los etiquetados de fotografías, por lo que la cancelación de datos personales es difícil de implementar.

El principio de transparencia que introduce la propuesta de Reglamento general de protección de datos personales –la obligación del responsable de ofrecer una información transparente y de fácil acceso y comprensión– tiene consecuencias en el ejercicio del derecho de acceso, también en el ámbito de las redes sociales. Cuando el interesado solicite el ejercicio del derecho de acceso, el responsable tendrá ahora que facilitar información sobre el plazo durante el cual se conservarán los datos personales –plazo para la supresión que también está sometido a una obligación de documentación en virtud del art. 28.2.g)– y el derecho a presentar una reclamación ante la autoridad de control. La propuesta de Reglamento también mejora el ejercicio de los derechos de acceso, rectificación y cancelación de datos personales en el ámbito europeo, fijando plazos de respuesta a las peticiones de las personas afectadas, autorizando el ejercicio de estos derechos por vía electrónica y obligando a motivar las denegaciones –arts. 11-15–.[13] La propuesta de Reglamento general de protección de datos personales se preocupa específicamente de dar respuesta a algunos problemas que tienen los interesados para el control de sus datos personales frente a los tratamientos que llevan a cabo empresas que prestan servicios en internet, como los servicios de redes sociales. Así, ante las dificultades que tienen los interesados para suprimir o para recuperar sus datos personales, se reconoce expresamente el derecho al olvido en internet y el derecho a la portabilidad de los datos –arts. 17 y 18–.[14] Se atribuye al interesado el derecho a que el responsable suprima los datos personales que le

10. Las dificultades que plantea la cancelación de la información personal en internet han sido analizadas en «Transparencia administrativa y protección de datos personales», *loc. cit.* págs. 67-75.
11. Basta que el afectado se oponga a la publicación de su dato personal para que esta deba ser cancelada.
12. La Policía dispone de una unidad de delitos tecnológicos que sigue los rastros que estas conductas dejan en internet. *Cfr. Presente y futuro de la seguridad en la sociedad de la información,* Fundación Policía Española 2004, págs. 101-159.
13. Tanto la información como el ejercicio de los derechos son gratuitos, salvo que la solicitud sea tan claramente excesiva por su carácter repetitivo, que justifique, en su caso, la aplicación de una tasa, en cuyo caso el responsable asume la carga de la prueba de la demostración del carácter excesivo de la solicitud.
14. El derecho al olvido en internet es una cuestión que hemos analizado recientemente en «Hacia un nuevo marco jurídico europeo de protección de datos personales», cit.

conciernan y se abstenga de utilizarlos cuando el interesado retira el consentimiento o se oponga al tratamiento. De esta manera, se reconoce el derecho de los usuarios de redes sociales a exigir a los proveedores de estos servicios de internet que borren completamente sus datos personales cuando el cliente se dé de baja en el servicio o cuando dejen de ser necesarios para los fines para los que se recabaron. Además, se establece expresamente que cuando el responsable haya hecho públicos los datos personales, este esté obligado a adoptar las medidas razonables –incluidas las técnicas– en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que están tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a estos datos personales, o cualquier copia o réplica de ellos. Así, la propuesta de Reglamento establece una obligación del responsable no solo de suprimir los datos personales sino de comunicar a terceros que el interesado solicita que se suprima cualquier enlace, copia o réplica de ellos, relacionando una cosa con la otra.[15] Además, se establece que cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de la publicación. Así, frente a quienes han mantenido que el derecho al olvido en internet debía pivotar sobre el derecho de oposición ejercido sobre los motores de búsqueda como responsables de sus propios tratamientos –esta sería la posición de la AEPD en las Resoluciones de tutela de derechos frente a Google–, la propuesta de Reglamento construye el derecho al olvido en internet sobre las obligaciones del responsable principal –de la web máster– que ha hecho público los datos.[16] También merece destacarse en la propuesta de Reglamento el reconocimiento del derecho a la portabilidad de los datos, de manera que cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado –también cuando el interesado los haya facilitado con su consentimiento y en virtud de un contrato–, el interesado tiene derecho a obtener del responsable una copia de los datos en un formato electrónico que le permita seguir utilizándolos. De esta forma, el reconocimiento que hace la propuesta del Reglamento de la portabilidad de los datos supone el derecho de los interesados a retirar sus datos –fotos o una lista de amigos– de una aplicación o un servicio y transferirlos a otra aplicación sin que los responsables del tratamiento inicial puedan bloquearlo.

El interesado al que se le deniegue total o parcialmente el ejercicio de estos derechos tiene una acción de tutela ante la Agencia Española de Protección de Datos –art. 18 de la LOPD–. Hay que recordar que cualquier vulneración de la legislación de protección de datos personales debe ser denunciada ante la Agencia Española de Protección de Datos; están tipificadas un conjunto de infracciones en el artículo 44 de la LOPD a las que se les aplica las sanciones establecidas en el artículo 45 de la LOPD.[17] La propuesta de Reglamento general de protección de datos personales refuerza tanto la independencia como la capacidad coercitiva de las autoridades administrativas de protección de datos personales, mejorando los poderes de investigación y de sanción, lo que incluye importantes sanciones económicas. Además, la propuesta de Reglamento es más exigente con quien, como las empresas que prestan servicio de redes sociales, tiene los tratamientos de datos personales como actividad principal de carácter comercial –valorando también su volumen de negocios en el ámbito mundial, como hacía la LOPD– y es, en cambio, más flexible con la mayoría de las pequeñas y medianas empresas que no llevan a cabo

15. El artículo 13 de la propuesta de Reglamento establece también la obligación del responsable del tratamiento de informar a los destinatarios a los que haya comunicado sus datos –incluyendo al encargado del tratamiento–, de cualquier rectificación o supresión de datos en virtud del ejercicio de los derechos de los interesados, lo que tiene gran importancia en relación con el derecho al olvido en internet.
16. Esta es la posición que hemos mantenido desde el año 2008 en nuestros trabajos «Transparencia administrativa y protección de datos personales», *loc. cit*. págs. 23-188, esp. págs. 101-112. Lógicamente, la Comisión está a la espera de que el Tribunal de Justicia resuelva la cuestión prejudicial ya citada planteada por la Audiencia Nacional en relación con las Resoluciones de tutela de derechos frente a Google.
17. C. Vela Sánchez-Merlo, abogada del Departamento de Nuevas Tecnologías de Ernst & Young, recuerda que «para poder efectuar correctamente la denuncia y aportar pruebas suficientes, es importante recoger toda la información y todas las evidencias del tratamiento de nuestros datos. Por ejemplo, una impresión de las pantallas del sitio web donde se publica nuestra información personal, los e-mails de comunicación que este portal o página web tenga con nosotros, desde la confirmación de haber creado una cuenta, los e-mails publicitarios recibidos o cualquiera de nuestras interacciones con el portal web, así como otros e-mails, comunicaciones, etc. que creamos que pueden estar relacionados y contengan datos personales nuestros o indicios de que conocen nuestra información personal, y que no hayan sido directamente recibidos del propio portal web. De esta manera tendremos gran parte de la información del tratamiento y podremos demostrar las presuntas finalidades con las que se están usando nuestros datos, y con ello dispondremos de las pruebas suficientes para poder iniciar una acción contra el vulnerador que está infringiendo nuestros datos personales» –*loc. cit.* págs. 266-267.

tratamientos de datos personales como actividad principal. La propuesta de Reglamento refuerza a las autoridades de protección de datos y equipara sus poderes. De esta forma, elimina las diferencias normativas existentes entre las distintas leyes nacionales que indudablemente perjudicaban a las empresas sometidas en algunos Estados a un más intenso control y régimen sancionador, con lo cual suprime una de las disfunciones principales que existían para un correcto funcionamiento del mercado interior.

Los tratamientos de datos personales en los servicios de redes sociales tienen un carácter transnacional. Hemos analizado anteriormente cómo la propuesta de Reglamento aborda el ámbito de aplicación territorial y, en especial, la problemática de ley aplicable que plantean las corporaciones internacionales que ofrecen servicios de red social y tienen su sede fuera de la Unión Europea –Facebook, MySpace–. La propuesta de Reglamento aclara también cuestiones de competencia y jurisdicción de autoridades de control cuando el tratamiento de datos personales sea llevado a cabo por un responsable o encargado en varios Estados miembros, y señala como competente la autoridad donde esté situado el establecimiento principal.[18] Además, trata de fortalecer la cooperación y la coherencia entre autoridades de control de la Unión Europea entre sí y con la Comisión, una cuestión a la que dedica todo el capítulo VII –arts. 55-72–, que contiene una regulación muy novedosa que no existía en la Directiva.[19] La propuesta materializa la cooperación entre autoridades de control en un conjunto de deberes de asistencia mutua –como facilitarse información útil– y medidas de control como solicitudes de autorización y consulta previa, inspecciones, comunicación rápida de información sobre la apertura de expedientes, lo que incluye medidas represivas para que se proceda al cese o a la prohibición de las operaciones de tratamiento, todo ello dentro de plazos concretos y prohibiendo la negativa a las solicitudes de asistencia. De esta forma, se introducen normas explícitas sobre asistencia recíproca obligatoria, que incluyen las consecuencias del incumplimiento de la solicitud de otra autoridad de control –art. 55–. También se prevén operaciones conjuntas –investigaciones, medidas represivas– en las que participen autoridades de control de distintos Estados miembros, y se establece una interesante regulación sobre la relación entre las autoridades de control del país de origen y del país de acogida, especialmente en relación con la presencia del personal de la primera autoridad, sus inspecciones y la responsabilidad sobre sus actos –art. 56–. La propuesta de Reglamento no se queda en la cooperación sino que fija un marco de mecanismos de coherencia, que trata de facilitar la libre circulación de datos personales en el territorio de la Unión al mismo tiempo que se respeta la protección de datos personales, y establece herramientas que aproximen las divergencias entre autoridades de control. La propuesta de Reglamento incluye también mecanismos de coordinación entre órganos jurisdiccionales, de manera que si un órgano jurisdiccional competente de un Estado miembro tiene motivos razonables para creer que se están llevando procedimientos judiciales paralelos en otro Estado miembro, se ponga en contacto con el órgano jurisdiccional competente y pueda suspender el procedimiento –art. 75.

Muchos de los usuarios de las redes sociales son menores por lo que estos servicios deben respetar especialmente la legislación de protección jurídica de los menores. El RPDP señala que «podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres

18. Esta solución es calificada por la exposición de motivos de la propuesta de Reglamento como «principio de ventanilla única», con la finalidad de velar por una aplicación uniforme.
19. Buena muestra de las discrepancias en la aplicación de las normas de protección de datos personales en los diferentes Estados miembros ante el mismo supuesto de hecho y la necesidad de actuar de manera coordinada ha sido el caso de Google Street View, que ha sido sometido a exigencias de privacidad más duras en Alemania que en otros Estados miembros. Como es sabido, entre mayo de 2007 y mayo de 2010 Google recopiló los datos de redes wifi en muchos países como parte de su proyecto Street View, que ofrece a los usuarios de Google Maps y Google Earth la posibilidad de ver a nivel de calle las imágenes de las estructuras y los terrenos adyacentes a las carreteras y autopistas. Sin embargo, Google también recogió las contraseñas, historial de uso de internet y otros datos personales sensibles que no eran necesarios para su proyecto, según advirtió la Comisión Federal de Comunicaciones (FCC) de los Estados Unidos de América. Google reconoció públicamente en mayo de 2010 que los coches que utilizaban para tomar las fotos para Street View habían recogido datos privados, la mayoría de ellos fragmentados. Ello dio lugar a una investigación de la FCC acerca de si se había violado la Ley de Comunicaciones.

o tutores».[20] No tiene sentido elevar la edad para permitir a los jóvenes integrarse en una red social porque a partir de los 14 años el menor tiene capacidad de obrar para muchas cosas, incluso para emanciparse, si bien es a partir de los 16 años cuando los jóvenes tienen una mayor capacidad de decisión en ámbitos como el educativo, el sanitario o los servicios sociales. No podemos caer en un exceso de paternalismo que suprima la autonomía de los menores, algo necesario para el libre desarrollo de la personalidad. No obstante, parece razonable obligar a las redes sociales a restringir al máximo grado de privacidad el acceso a los perfiles de los menores, y limitar, además, el número de «amigos». Hay que tener en cuenta que el 95% de los pederastas conocen a sus víctimas a través de los chats o de redes sociales.[21] Además, cuando las redes sociales vayan a registrar datos de menores de edad deben expresar la información prevista en el artículo 5 de la LOPD en un lenguaje fácilmente comprensible –art. 13.3 del Reglamento–. Tradicionalmente las redes sociales, si bien requerían el dato de la edad, no establecían ninguna medida para la verificación de esta o de la autenticidad del consentimiento prestado por los padres o tutores. El artículo 13.4 del Reglamento obliga al responsable del tratamiento a articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales. Es, por ello, necesario que se establezcan medidas que permitan el control de la edad o del consentimiento de los padres o tutores, si bien hay que evitar un tratamiento masivo de datos identificativos por los servicios de redes sociales, que puede ocasionar un problema mayor.[22] El Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 establece un conjunto de directrices relativas a los tratamientos de datos personales de menores por parte de las redes sociales: no pedir datos sensibles en el formulario de registro, no realizar comercialización directa destinada específicamente a los menores, establecer grados adecuados de separación lógica entre las comunidades de niños y de adultos, etc.

La propuesta de Reglamento general de protección de datos personales que ha presentado recientemente la Comisión incluye una regulación relativa a los tratamientos de datos personales de los niños. Así, en el apartado de definiciones considera niño a toda persona menor de 18 años, lo que está en contradicción, como acabamos de señalar, con el artículo 13 del RPDP, que acertadamente permitía el tratamiento de los datos de los mayores de 14 años con su consentimiento, sin perjuicio de los casos en los que la Ley exija la asistencia de los titulares de la patria potestad o tutela, y con la legislación que reconoce el ejercicio de los derechos y la autonomía de la voluntad del menor maduro, también en el ámbito sanitario. No obstante, la propuesta de Reglamento incluye también una regulación específica de los tratamientos de los datos personales relativos a los niños –art. 8– que contiene una excepción a esta mayoría de edad de 18 años en relación con la oferta directa de servicios de la sociedad de la información, que permite que el consentimiento o la autorización del padre o tutor solo sea necesaria en los tratamientos de datos personales relativos a niños menores de 13 años, lo que facilita el funcionamiento de las redes sociales virtuales, que tienen fijada la edad en 14 años –Tuenti– o 13 años –Facebook–.[23] Existen otras previsiones en la propuesta de Reglamento de la Comisión que tratan de proteger a los menores: la necesidad de que el responsable facilite especialmente cualquier información dirigida a niños de manera inteligible, sencilla, clara y adap-

20. La redacción de este precepto, obra de Piñar Mañas, ha sido especialmente feliz. Igualmente, los derechos de acceso, rectificación, cancelación y oposición son personalísimos y deben ser ejercidos por el afectado, salvo que se encuentre en una situación de minoría de edad que le imposibilite el ejercicio personal de ellos, en cuyo caso podrán ejercitarse a través de su representante legal. La problemática del consentimiento para el tratamiento otorgado por los menores y el ejercicio de los derechos por estos y por sus padres han sido analizados en A. Troncoso Reigada, «Introducción y Presentación» en *Protección de datos personales en centros educativos públicos*, cit. págs. 61-67 y 81-85; y «La confidencialidad de la historia clínica«, *Cuadernos de Derecho Público,* núm. 27, 2006, págs. 119-130.
21. *Cfr*. el informe sobre «Protección legal de los menores en el uso de Internet», del Instituto Nacional de Tecnologías de la Información, cit.
22. El artículo 13.4 del RPDP ha sido analizado en la sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Supremo, de 15 de julio de 2010 –Sección Sexta–, y se ha confirmado su legalidad. La AEPD tiene un acuerdo con Tuenti para que solicite el DNI a los usuarios respecto de los que sospeche o tenga indicios de que su edad es inferior a 14 años. También ha acordado con Facebook que no inscribirá a menores de 14 años. *Cfr.* las notas de prensa sobre las reuniones que la Agencia Española de Protección de Datos ha mantenido con representantes de Facebook –el 26 de marzo de 2009– y de Tuenti –2 de abril de 2009– en www.aepd.es.
23. Téngase en cuenta que la *Children's Online Privacy Protection Act* (COPPA) de EE. UU. considera menores únicamente a aquellos que no han cumplido todavía 13 años.

tada a interesado –art. 11–;[24] el reconocimiento especial del derecho al olvido en internet y a la supresión de los datos proporcionados siendo niño –art. 17–; la toma en consideración de que el interesado sea un niño en la ponderación entre la satisfacción del interés legítimo del responsable del tratamiento y los derechos y libertades fundamentales que requieran la protección de los datos personales –art. 6– o la exigencia de que el responsable de tratamientos de datos personales en ficheros a gran escala relativos a niños, al igual que en el caso de los datos biométricos o genéticos, lleve a cabo una evaluación de impacto en la protección de datos personales –art. 33.

Las redes sociales, salvo la española Tuenti, radican –o se extienden– en EE. UU. o en otros países donde no es fácil la aplicación de la normativa europea de protección de datos personales. Por ello, cobra especial relieve la autorregulación de las propias empresas, especialmente mientras no estén aprobados unos estándares internacionales sobre protección de datos personales. En muchas ocasiones, dadas las dificultades existentes para aplicar la normativa de protección de datos personales o la demora de una resolución estimatoria en un procedimiento administrativo o jurisdiccional –consecuencia de la necesidad de respetar unos plazos para hacer efectivo el principio de contradicción o la práctica de la prueba–, lo más efectivo para hacer desaparecer una intromisión ilegítima en los derechos de las personas es acudir a los propios canales de denuncia de las redes sociales o de los sitios webs. Estas frecuentemente suprimen un comentario si se trata de un insulto, si hay sexo explicito o si tiene un contenido xenófobo, o cancelan una fotografía si no existe consentimiento por el interesado. A las propias empresas privadas les supone una ventaja competitiva el buen funcionamiento de los canales de denuncia. Por ello, las redes sociales deben facilitar estos canales de denuncias, garantizando la respuesta a las solicitudes en un plazo breve de tiempo y eliminando el comentario o la fotografía lesiva con la intimidad de las personas o sobre la que se ha ejercido un derecho de oposición. Las redes sociales deben también sancionar en el ámbito de su comunidad virtual a aquellas personas que vulneren la intimidad o la protección de datos personales de terceros, publicando fotografías o vídeos de otras personas con su oposición o realizando comentarios que sean poco respetuosos con terceras personas. Es imprescindible facilitar a los usuarios medios de control de comentarios y sistema de bloqueo de cuentas de forma que puedan evitar insultos o comentarios inadecuados de aquellos usuarios con los que puedan tener conflictos. Si bien la responsabilidad civil les correspondería a los autores de la vulneración del derecho a la intimidad y a la protección de datos personales de terceras personas, las redes sociales también tendrían una responsabilidad al ser titulares del medio donde se publica la información, especialmente cuando no son diligentes en la cancelación de esta si ha sido solicitada previamente por el perjudicado.[25]

Las redes sociales deben tener en cuenta las exigencias de privacidad en el diseño de sus servicios y sistemas de información, estableciendo también políticas de privacidad que incluyan, por defecto, parámetros que sean más respetuosos con esta. Hay que tener en cuenta que la propuesta de Reglamento general de protección de datos que ha presentado la Comisión ha convertido en obligaciones para el responsable del tratamiento algunas medidas que hasta ahora estaban en el ámbito de la autorregulación, como es el caso de la privacidad por defecto y de la privacidad en el diseño. Así, la propuesta de Reglamento establece la obligación del responsable del tratamiento de establecer mecanismos que permitan que, por configuración inicial, solo sean objeto de tratamiento los datos necesarios para cada fin específico, de manera que no se recojan ni se conserven datos más allá del mínimo necesario para los fines, tanto en lo que respecta a la cantidad de los datos como a la duración de su conservación, y se establecen, asimismo, mecanismos que garanticen que, por defecto, los datos personales no sean accesibles a un número indeterminado de personas –art. 23–. La propuesta de Reglamento también establece la privacidad en el diseño o *privacy by design*, y señala la obligación de que la protección de datos

24. La propuesta de Reglamento de la Comisión introduce un conjunto de garantías para la protección de los datos de menores de edad que ya se encuentran en el art. 13 del RPDP, en especial, que la información sea comprensible y que existan procedimientos que garanticen que se ha comprobado de manera efectiva la edad del menor y la autenticidad del consentimiento de los padres o tutores.
25. Las fotografías suelen ser una fuente de conflictos, no solo por su publicación sin consentimiento de los usuarios sino también por la revocación del consentimiento prestado en su momento. Si bien la red social no deja de ser un canal neutral al que no corresponde la resolución de disputas entre sus usuarios, basta que exista una oposición de un interesado a la publicación de una fotografía para que esta deba ser cancelada por la empresa proveedora del servicio de red social de manera automática.

personales sea tenida en cuenta en el momento del diseño del sistema de información; es decir, que las exigencias en materia de privacidad –especialmente frente a las amenazas más frecuentes– sean un elemento que se deba tener en cuenta en el diseño de los servicios en internet, también en los servicios de redes sociales. Por ello, las redes sociales deben avanzar en la privacidad en el diseño y en la privacidad por defecto en cuestiones como, por ejemplo, los niveles de acceso a los datos personales publicados en el perfil –uno de los principales parámetros de confidencialidad– o el establecimiento de canales de denuncia, como hemos analizado anteriormente. Así, es necesario que las redes sociales modifiquen sus configuraciones por defecto relativas al nivel de acceso a las páginas personales, evitando que la configuración inicial prevea que toda la información esté en abierto, limitando el nivel de publicidad para que la información sea accesible únicamente para los amigos y no para los amigos de estos. Téngase en cuenta que muy pocos usuarios modifican los parámetros establecidos por defecto. Si no se establecen restricciones al acceso, cualquier tercero puede acceder a los datos personales de los usuarios, no solo los miembros de la red social sino también no miembros a través de los motores de búsqueda –cuando el servicio de red social así lo prevea–. Con esta medida de privacidad por defecto, los usuarios se ven obligados a aceptar expresamente que personas distintas de sus contactos van a acceder al perfil, lo que reduce el riesgo para su privacidad.[26] Sin embargo, en la actualidad la mayoría de las redes sociales establece por defecto la accesibilidad del perfil no solo para los amigos sino también para los amigos de los amigos –las personas que forman parte de la lista de contactos de los amigos–. Hay que tener en cuenta que en las redes sociales el consentimiento se ejerce habitualmente aceptando la política de privacidad establecida por defecto.

La propuesta de Reglamento incide también en la importancia de los códigos de conducta, dirigidos a contribuir a la vigencia de este derecho fundamental en sectores de tratamiento específicos –art. 38–. Sería, pues, conveniente que las redes sociales aprobaran también un código de conducta que incluyera que los usuarios no pueden ceder datos de otras personas en la página personal –por ejemplo, fotografías o su etiquetado– sin su consentimiento, la protección de los niños, la transparencia de la información al interesado o la inclusión de los mecanismos de supervisión y garantía, como procedimientos extrajudiciales y de resolución de conflictos, que permitan resolver las controversias entre los responsables y los interesados, sin perjuicio de la posibilidad de acudir a las autoridades de control y a los tribunales. De hecho, el propio Grupo de Trabajo del Artículo 29, en su Dictamen 5/2009, aconsejaba también la aprobación de códigos de buenas prácticas de los proveedores de servicios de redes sociales que incluyeran medidas de ejecución eficaces y sanciones disciplinarias.[27] Por último, hay que tener en cuenta que, en el caso de que sea difícil aplicar la normativa europea de protección de datos a una empresa que presta un servicio de red social, el incumplimiento de la política de su privacidad o del código de conducta al que está adherido representa la violación de un compromiso con el usuario que puede tener consecuencias legales graves para el responsable en muchos países –por ejemplo, en EE.UU.–.[28] El Grupo de Trabajo del Artículo 29, en el Dictamen 5/2009 incluye otras recomendaciones dirigidas a las empresas proveedoras de servicios de red social. Entre estas destaca la implantación de tecnologías en defensa de la privacidad –PET– como los programas informáticos de verificación de la edad o que establezcan instrumentos de control de los padres sobre el acceso de los menores a internet o la aparición de venta-

26. Recientemente Google+ ha lanzado una nueva función para los usuarios de la red social, de forma que todos los usuarios que tengan una cuenta y utilicen el servicio de Google Contact para gestionar su libreta de direcciones puedan ver la información de sus contactos desde su perfil de la red social, integrándola dentro de ella. No obstante, en este caso esta información solo puede ser vista de forma privada por el usuario y no será un dato al que tengan acceso sus contactos de Google+.
27. El RPDP al regular los códigos tipo también incluye como garantía de su cumplimiento la existencia de procedimientos de supervisión y el establecimiento de un régimen sancionador adecuado, eficaz y disuasorio –art. 75.
28. Recientemente el presidente Obama ha presentado una *Consumer Privacy Bill of Rights*, que reconoce derechos a los consumidores y supone una modificación de la posición americana en este ámbito que pivotaba sobre la autorregulación. Este texto apuesta por la autorregulación vinculante y, en el caso de que esta no se cumpla, apuesta por la regulación. *Cfr*. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 23 de febrero de 2012. Hemos analizado recientemente la comparación entre los distintos modelos de protección de datos en el ámbito internacional y la importancia que tiene en EE. UU. la autorregulación. *Cfr*. «El desarrollo de la protección de los datos personales en Iberoamérica desde una perspectiva comparada», y «Presentación» en *Revista Internacional de Protección de Datos*, núm. 1 (en prensa).

nas emergentes de advertencia en fases sensibles. Llama la atención especialmente la recomendación relativa a un mejor cumplimiento del principio de adecuación, pertinencia y prohibición de exceso previsto en el artículo 6.1.c) de la Directiva 95/46/CE en relación con la posibilidad de permitir a los usuarios de redes sociales actuar bajo un seudónimo, una medida que se ha aconsejado tradicionalmente para preservar la privacidad en internet.[29] En general, se echa en falta un adecuado diseño de las plataformas de las redes sociales para reducir los problemas relacionados con la privacidad. Por ello, es imprescindible que las autoridades de control eviten las posiciones frentistas en relación con las redes sociales y sean capaces de generar entornos de colaboración, lo que no significa ceder ante la industria –que no deja de ser un *stakeholder*– sino de alcanzar un diálogo que permita la *privacy by design*.

29. «En este contexto, cabe señalar que el SRS puede tener necesidad de registrar algunos datos de identificación de sus miembros, pero no es preciso que publique su verdadero nombre en Internet. Por tanto, los SRS deberían considerar si pueden justificar el hecho de obligar a sus usuarios a actuar bajo su verdadera identidad en vez de bajo un seudónimo. Son argumentos de peso para que los SRS dejen la elección a este respecto a los usuarios, y es una exigencia legal al menos en un Estado miembro. Estos argumentos son especialmente sólidos cuando el SRS en cuestión tiene miembros en todo el mundo. El artículo 17 de la Directiva relativa a la protección de datos exige que el responsable del tratamiento aplique las medidas técnicas y de organización adecuadas para la protección de los datos personales. Tales medidas de seguridad incluyen, en particular, el control del acceso y mecanismos de autenticación que pueden aplicarse aunque se utilicen seudónimos».

Cita recomendada

TRONCOSO, A. (2013). «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales. Parte dos». *IDP. Revista de Internet, Derecho y Política*. Núm. 16, pág. 27-39. UOC. [Fecha de consulta: dd/mm/aa]
‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n16-troncoso/n16-troncoso-es›
DOI: http://10.7238/idp.v0i16.1927

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, y fue 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 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