Redes sociales y protección de datos

PID_00248575

Juan Pablo Aparicio Vaquero

Universitat Oberta de Catalunya

Índice

Introducción

La importancia de las redes sociales está, hoy en día, fuera de toda duda. Se trata de un servicio de la sociedad de la información (SSI) en cuya prestación es esencial el tratamiento de datos, bien sea con el simple fin de poder proporcionar el servicio (relacionar a los sujetos entre sí), bien con otros objetivos que se convierten en esenciales para la financiación del modelo de negocio, como el ofrecimiento de publicidad personalizada a sus usuarios, ya sea propia o de terceros. El prestador del servicio de red social (SRS), en tanto que responsable del tratamiento, asume una posición muy comprometida ya que debe implantar todo tipo de medidas que garanticen el cumplimiento de sus obligaciones como tal, en especial en el marco del nuevo Reglamento general de protección de datos (RGPD) como, por ejemplo, el diseño por defecto de sus sistemas de recogida de datos para que tengan en cuenta la máxima protección de los mismos (*privacy by default*, 'privacidad por defecto'). Igualmente, por su función de prestador de un SSI, en algunos casos será responsable de las actuaciones de los terceros que utilicen sus servicios, si bien ello solo en los términos muy concretos que establece la ley (se trata realmente de una responsabilidad por actos propios, no por actos de terceros).

El objetivo primordial del legislador europeo es garantizar la máxima protección a los titulares de datos, de manera que hace depender la aplicación de las normas europeas (la directiva, en primer lugar, junto con las leyes nacionales, y ahora el reglamento) de criterios amplios que obligan a todo responsable externo a la UE –y no se olvide que la mayoría de redes sociales que operan en el continente tienen su sede principal en los EE. UU.– a cumplir con el alto estándar de protección que se ha diseñado, superior al de otros países del mundo.

El criterio legitimador de todo tratamiento de datos personales en las redes sociales es el consentimiento de los usuarios titulares de los mismos, por lo que ha de prestarse especial atención a dicho consentimiento y a cómo es recabado. Incluso en los casos en los que se permite la recogida y el tratamiento al margen de la voluntad (o el conocimiento) inicial del titular (el nuevo RGPD menciona el muy amplio «interés legítimo» del responsable, por ejemplo), su consentimiento sigue siendo fundamental, pues puede oponerse o cancelar el tratamiento en todo momento, sin perjuicio de las otras consecuencias que ello tenga para la relación jurídica en cuestión. Este aspecto se torna extremadamente delicado cuando son menores de edad los que intervienen en las redes, pudiendo llegarse a plantear hasta qué punto sus padres o tutores pueden vigilar o controlar dicha actividad, en (obligado) ejercicio de sus funciones tuitivas.

En un momento de cambio normativo, las páginas que siguen tienen en cuenta tanto la LOPD (y la directiva de la que trae causa) como el nuevo RGPD. Más allá de la conveniencia de ir implantando ya las medidas que este exige, aun antes de su plena exigencia a finales de mayo de 2018, conviene destacar que en algún caso ofrece soluciones distintas a las existentes hasta el momento. Ello sucede, por ejemplo (además de en algunos otros puntos que se indicarán), en cuanto a la consideración de los usuarios de SRS y su posición en relación con los datos de terceros que tratan en el curso de su disfrute del servicio.

Objetivos

Es objetivo principal de este módulo el conocimiento de las especialidades del tratamiento de datos en el ámbito de las redes sociales. En concreto, se pretende que el alumno:

1. Sepa caracterizar los servicios de red social, su inclusión en la normativa vigente (tanto de protección de datos como de servicios de la sociedad de la información) y razonar la aplicabilidad de la misma.

2. Identifique a los diversos responsables del tratamiento de datos en el marco de la prestación de los servicios de red social, así como la posición de los usuarios y sus derechos.

3. Conozca la problemática en torno a la prestación del consentimiento en las redes sociales y, en particular, la posición de los menores y la de sus representantes legales en relación con la actuación de aquellos en dichas redes.

4. Tenga una noción básica de las responsabilidades del prestador del servicio de red social por la actividad ilícita de sus usuarios al utilizar la misma.

1. Concepto y relevancia jurídica de las redes sociales

Aunque a estas alturas resulta sumamente intuitivo el reconocimiento de la importancia de las redes sociales en la actualidad, a todos los niveles, no está de más corroborar dicha percepción con algunos datos objetivos: según el estudio anual de la consultora IAB hecho público en abril de 2017, hay algo más de 19 millones de usuarios de redes sociales en España (el estudio tiene en cuenta a usuarios de entre 16 y 65 años, que representan el 86% de los internautas españoles). Dichos usuarios utilizan una media de cuatro de tales redes, algunas por un periodo de hasta cinco horas diarias. La mitad de los encuestados reconocen que se sienten influidos en sus compras por la percepción de las marcas a través de dichas redes sociales, razón por la cual la inversión en publicidad en las mismas creció hasta más de un 21% en 2016 (*Estudio anual de redes sociales*, de IAB Spain, disponible en <http://iabspain.es/wp-content/uploads/iab_estudioredessociales_2017_vreducida.pdf>).

El concepto de «red social» surge tanto al margen del derecho como de la informática, y es utilizado por primera vez en el campo de la sociología, a finales del siglo XIX, como forma de abordar las interacciones (lazos, vínculos) de individuos y grupos en la sociedad. Desde entonces, su estudio ha sido abordado también por antropólogos y matemáticos, para acabar desembarcando en el ámbito de las tecnologías de la información y las comunicaciones (TIC). Asimismo, por su relevancia y afectación de bienes y derechos personales y patrimoniales, es objeto de regulación jurídica desde diferentes ramas del ordenamiento. Al respecto, una definición de las redes sociales, clásica pero vigente en sentido moderno y ya vinculado al uso de la tecnología digital e Internet, es la que las califica como servicios

> «que permiten al usuario 1) construir un perfil público o semi-público dentro de un sistema limitado, 2) articular una lista de otros usuarios con los que comparte una conexión, y 3) visualizar y rastrear su lista de contactos y las elaboradas por otros usuarios dentro del sistema. La naturaleza y nomenclatura de estas conexiones suele variar de una red social a otra.» (Bold y Ellison, 2007)[1].

(1)Tanta es la importancia de las redes sociales que el concepto actual, muy reciente, ya ha tenido acceso al DRAE: «plataforma digital de comunicación global que pone en contacto a gran número de usuarios».

La gestión informatizada de las relaciones sociales entre individuos y grupos a través de plataformas que facilitan los contactos interpersonales según intereses afines –en definitiva, su explotación en internet– ha permitido la aparición de nuevos modelos de negocio que podemos denominar, genéricamente, «servicios de red social» (SRS, en adelante) y que constituyen un (lucrativo) negocio para sus prestadores.

Las redes sociales se caracterizan por la interacción (en tiempo real o en diferido) entre sus usuarios (que pueden ser de todo tipo: particulares, profesionales, asociaciones, empresas, instituciones, administraciones públicas…) mediante el intercambio de información (a la postre, datos, sean estos persona-

les o no) y contenidos propios y ajenos. Normalmente, el servicio es, en apariencia, gratuito para el usuario, y el prestador obtiene su beneficio a través de la publicidad, bien sea esta de carácter general, bien sea dirigida según la actividad de los distintos usuarios. En cada red, estos quedan identificados a través de los datos de su perfil y se relacionan con otros usuarios creando o compartiendo información y/o contenidos de todo tipo: texto, vídeo y audio. Esas relaciones se dan mediante el seguimiento mutuo o unilateral (se sigue a personas y se ven sus publicaciones aunque estas no nos sigan a nosotros, por ejemplo los seguidores o *followers* de famosos, de personas que marcan tendencias o *influencers*, de páginas de empresas o institucionales, etc.). Facebook (la red social por antonomasia), Twitter, Instagram, LinkedIn, Badoo o Flickr son redes muy conocidas, incluso Whatsapp y similares hoy en día son consideradas como tales.

Se discute en ocasiones si servicios como Twitter (que es propiamente una plataforma de *microblogging*) son o no una red social. Lo cierto es que no hay problema en considerarla como tal, bien porque entre sin problemas en este concepto socio-tecnológico, bien porque, aun cuando no lo fuera en sentido estricto (hay quien dice que es un medio de comunicación en sí mismo) sí tiene herramientas de SRS. La mayoría de personas lo consideran como tal, y así suele aparecer en todas las encuestas sobre redes sociales.

Mayores problemas pueden plantear otros servicios de mensajería instantánea como Whatsapp y sus competidores (Telegram, Line, Hangouts, Spotbros…), por cuanto se dice que son simples servicios de intercambio de comunicaciones o de mensajes electrónicos. Nuevamente, la concepción más extendida hoy en día es que entran dentro del concepto de SRS, aunque sea porque integran cada vez más características de estas al permitir la creación de grupos de cientos de personas, con acceso a los listados de contactos de cada una de ellas, y el intercambio de contenido multimedia y «estados» (información pública vinculada a un perfil por la cual se informa a los demás usuarios sobre actividades, noticias propias o auténticos estados emocionales). En la actualidad hay empresas e, incluso, administraciones públicas que los utilizan para dar difusión a noticias y avisos como cualquier otra red social «clásica». Puede verse al respecto el *Dictamen CNS-24/2013, de 2 de julio, de la Autoridad Catalana de Protección de Datos*, en relación con el uso de WhatsApp y Spotbros por parte de los abogados y sus clientes, que reconoce la implantación de esas funciones.

Dentro de las redes sociales encontramos diferentes tipos: *horizontales* (abiertas a todos los usuarios y sin temática definida, como Facebook, por ejemplo) o *verticales* (especializadas por sectores o con ejes temáticos comunes a sus usuarios, como por ejemplo para intercambios profesionales, LinkedIn o Xing; para actividades de ocio, videojuegos, fans, música, etc., redes como Last.FM o Myspace; es decir, hay redes temáticas para todos los gustos y actividades). Desde otra perspectiva, se habla de redes *humanas*, dirigidas a fomentar las relaciones entre personas, o de *contenido*, en las que importan más los contenidos que se comparten que las personas y de las que serían ejemplos Flickr, para compartir fotografías, o YouTube, para vídeos de cualquier tipo. Hay otros muchos criterios de clasificación: por actividad, localización geográfica, contenidos compartidos, etc. En todo caso, la mayoría son «gratuitas» (por cuanto no cobran *dinero* por su suscripción), aunque algunas reservan contenidos o prestaciones para los usuarios que paguen por ellos, mediante modelos *premium* de negocio (un ejemplo de ello es Badoo).

Evidentemente, tanto la existencia misma de servicios de las redes sociales, como su prestación y la actividad de los usuarios en las mismas importan al derecho, que regula el fenómeno desde diferentes puntos de vista, como puede ser la contratación y prestación de dichos servicios, la propiedad intelectual de aplicaciones y contenidos, el uso de marcas y otros signos distintivos, la publicidad y las actividades de promoción, la afectación de derechos de la per-

sonalidad, la protección de datos, la comisión de posibles delitos específicos de estas formas de comunicación o en actos en las que estas aparecen como agravantes, etc.

Por lo que ahora nos interesa, en las páginas que siguen desarrollaremos la regulación jurídica del tratamiento de datos de carácter personal que se da en las redes sociales, sin perjuicio de que, para ello, hayamos de referirnos también a algunas cuestiones propias de su contratación (consentimiento), a la afectación de otros derechos de la personalidad que son, a la vez, derechos fundamentales (imagen, intimidad y honor), y a la eventual responsabilidad en la que pueden incurrir sus prestadores por la actuación ilícita de sus usuarios.

Conviene distinguir la red social como «servicio» del programa de ordenador (aplicación o *app*) o página web a través de la cual se accede a dicha red y se disfruta de dicho servicio, tal cual es prestado por su titular. Existen *apps* para los diferentes dispositivos (ordenadores, *tablets*, teléfonos móviles…) y sistemas operativos (Windows, MacOS, Linux, iOS, Android…), y es posible también acceder a tales redes a través de simples páginas web. Las aplicaciones constituyen pequeños programas de ordenador cuya regulación encontramos, fundamentalmente, en la normativa de propiedad intelectual, arts. 10.1.i y 95-104 del Texto refundido de la ley de propiedad intelectual (TRLPI). Los derechos sobre estas «obras» protegidas pertenecen a su titular, que será el prestador del SRS, con independencia de que se exploten de forma gratuita en ejercicio de los derechos de distribución o de comunicación pública. También las páginas web y la apariencia de la información o de los datos tal cual son presentados a los usuarios (*interfaz gráfica* o *look and feel*) quedan protegidos por el derecho de autor, bien como obras propiamente si el conjunto es original, bien a través de la protección dada a sus diferentes elementos. La normativa de marcas y signos distintivos se ocupará de la tutela de sus respectivos logotipos.

De la misma manera, pueden ser objeto de protección los contenidos de los usuarios que estos compartan en las redes, siempre que reúnan los requisitos para ello. En particular, se protege la originalidad de los mismos en el sentido en que es contemplado dicho adjetivo por el derecho de autor y que, en nuestro ordenamiento, suele vincularse a un criterio *objetivo*, salvo excepciones. Lo problemático en estos casos es, en primer lugar, si al compartir tales contenidos se otorgan, además, derechos de explotación al prestador del SRS, conforme a las condiciones de acceso al mismo, si tales concesiones son válidas o no y hasta qué punto. El segundo problema es determinar cuál es la responsabilidad del prestador si se intercambian contenidos ilícitos, puesto que los usuarios no disponen de autorización para explotarlos. La primera cuestión excede el ámbito del presente módulo pero, respecto de la segunda, apuntaremos que la solución es, esencialmente, la misma que se dé a cualquier utilización de la red por parte de un usuario para violentar derechos de otros.

Por otra parte, conforme señala el Grupo de Trabajo del Artículo 29 (*Dictamen 5/2009 sobre las redes sociales en línea*, documento de trabajo 163), los SRS no son operadores de comunicaciones electrónicas a los efectos de la Directiva marco 2002/21, por lo que, por regla general (y salvo que añadan tal función al servicio que prestan), tampoco estarán *obligados* (sin perjuicio de que lo *puedan* hacer para la prestación de sus servicios, por ejemplo, para mantener abiertas sesiones en distintos dispositivos) a la conservación de los datos de conexión (Directiva 2006/24 que, por otra parte, ha sido anulada por la STJUE 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, dejando en muy dudosa posición, cuando no directamente anulada también, su legislación de trasposición, como la española Ley 25/2007, de 18 de octubre, de conservación de datos de comunicaciones electrónicas y de redes públicas).

1.1. Las redes sociales como «servicios de la sociedad de la información»

Desde el punto de vista jurídico, las redes sociales son propiamente «servicios de la sociedad de la información» (SSI) a los efectos de la normativa de comercio electrónico aplicable (tanto la española, la Ley 34/2002, como europea de la que aquella trae causa, la Directiva 2000/31),[2] según reconoce el propio Dictamen 5/2009 del Grupo de Trabajo del Artículo 29 (GT29). Efectivamente, cumplen a la perfección los requisitos definidos en el anexo A de la LSSICE:

1) Servicios prestados normalmente a título oneroso. Aunque *puede* (suele, incluso) *no estar remunerado de forma directa por el usuario*, no cabe duda de que el SRS es prestado por su titular como una *actividad económica* que obtiene ingresos a través de la explotación de otros aspectos de dicho servicio, singularmente, la contratación de publicidad para mostrar a los usuarios[3] o las cuentas profesionales, sin perjuicio también de que puedan existir servicios *premium* o de pago para los usuarios, que mejoran las condiciones básicas de prestación del servicio (por ejemplo, eliminando la publicidad o mejorando el posicionamiento y la visibilidad del perfil).

De hecho, a mi juicio, cabría incluso cuestionar que el contrato de suscripción o afiliación a una red social sea un contrato gratuito pues, en realidad, hay prestaciones por ambas partes de claro contenido patrimonial, en relación sinalagmática: la del servicio, de un lado, y, por lo menos, la cesión de datos que lo permite y que, en actos de ejecución posteriores, supone la propia actividad del usuario en la red; suele haber, además, cesión de *otros derechos*, como los de propiedad intelectual sobre contenidos compartidos (fotografías, imágenes, textos...), a favor del SRS. Y, por supuesto, en muchos SRS también existe la posibilidad de contratar servicios *premium* de pago, que mejoran las condiciones básicas de prestación del servicio gratuito.

La «monetización» de los datos personales (su aparente utilización como moneda de cambio de la prestación de servicios en línea gratuitos) ha sido advertida por el Supervisor Europeo de Protección de Datos (SEPD) en su *Dictamen preliminar sobre intimidad y competitividad en la era de la obtención de datos masivos* (26 de marzo de 2014, disponible en <https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf>; págs. 10 y 37), así como en su *Dictamen sobre el cumplimiento efectivo de la legislación en la economía de la sociedad digital* (23 de septiembre de 2016, disponible en <https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf>, pág. 6). Es en este sentido que la *Propuesta de directiva relativa a determinados aspectos de los contratos de suministro de contenidos digitales* (COM(2015) 634 final, de 9 de diciembre de 2015) incluso los define como aquellos en virtud de los cuales el proveedor suministra dichos contenidos y, a cambio, el consumidor paga un precio o «facilita activamente otra *contraprestación no dineraria en forma de datos personales* u otro tipo de datos» (art. 2.12). El SEPD, sin embargo, en su opinión sobre tal propuesta (Opinión 4/2017, de 14 de marzo) desaconseja esta definición del contrato en base a la entrega de datos personales, no tanto por no producirse (que sí, aunque reconoce que hay casos en los que se entregan, simplemente, para poder prestar el servicio, sin que el proveedor los explote económicamente), sino por ser algo muy distinto a una simple contraprestación (*counter-performance*): un derecho fundamental de las personas reconocido como tal en la Carta europea (art. 8) y el TFUE (art. 16), no equiparable al dinero e, incluso, distinto del valor que pueden generar tales datos (que es, además, desconocido para sus titulares consumidores). Por ello, el SEPD apunta mejores definiciones que prescinden del carácter oneroso o gratuito (en cuanto contraprestación en dinero por parte del consumidor), como la propia de la normativa de SSI (véase: <http://data.consilium.europa.eu/doc/document/ST-7369-2017-INIT/en/pdf>, págs. 8-13). En cualquier caso, aplaude el compromiso del legislador europeo y reconoce que estos contratos no son tan *gratuitos* como aparentan (con cursivas o comillas incluidas en repetidas ocasiones a lo largo del documento).

(2)«Las redes sociales son "servicios de la sociedad de la información" (SSI) según los regula la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (directiva sobre el comercio electrónico); en realidad, la definición de tales SSI se hace por remisión (art. 2.a y considerando 17 Directiva 2000/31) a la Directiva 98/34/CE, modificada por la Directiva 98/48 y actualmente codificada por la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (texto pertinente a efectos del EEE); su norma de trasposición es la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (LSSICE). Véase también el Dictamen 5/2009 sobre las redes sociales en línea del GT29, adoptado el 12 de junio de 2009, pág. 5.»

(3)A finales de 2016, solo Facebook acaparaba el 16,6 % de la publicidad mundial en internet, con tendencia al alza. A gran distancia le siguen, entre los SRS, Twitter, con un 1,9% y LinkedIn, con un 1%. Véase: <http://ecommerce-news.es/marketing-social/google-facebook-acaparan-ya-60-la-publicidad-online-nivel-mundial-52361.html>.

2) A distancia, por vía electrónica. Es la forma típica y única de prestación del SRS tal cual se concibe hoy en día en el entorno digital e Internet.

3) A petición individual del destinatario. Este requisito hace referencia a que las transmisiones de datos en que consiste el propio servicio se producen a iniciativa de los usuarios, que son (al menos, sus equipos) los que las solicitan en cada caso, determinando su momento y contenido (a diferencia de los servicios denominados «punto multipunto», como los de televisión, radio y teletexto, dado que en ellos no hay petición individual, sino una recepción simultánea por parte de un número ilimitado de destinatarios).

La Directiva 2000/31 considera que en los servicios excluidos no hay tratamiento o almacenamiento de datos (considerando 17). La actividad de los SRS se caracteriza justamente por todo lo contrario, pues la base del servicio es la recogida, el almacenamiento y el tratamiento de los datos de los usuarios del mismo (personales o no), para permitir su interacción y la disposición de publicidad por parte de terceros o del propio prestador.

Así las cosas, el proveedor de servicios de redes sociales es un «prestador de servicios de la sociedad de la información» (PSSI) y sus usuarios resultarán ser «destinatarios» del mismo, y «consumidores», o no, a los efectos oportunos. No obstante, algunos de tales destinatarios, en cuanto desarrollen a través de la red actividades profesionales, podrían ser también considerados como PSSI.

En tanto que PSSI, quien explota una red social queda sujeto a esta normativa, a sus obligaciones (véase, en particular, el art. 10 LSSICE) y a sus responsabilidades. Puede ser calificado no solo como *proveedor de servicios* o *de contenido*, sino también como *intermediario*, por cuanto facilita los medios técnicos para la actividad de los terceros (sus usuarios, del tipo que sean). En este sentido, funcionarán como proveedores de alojamiento y/o enlaces, a los efectos de lo previsto en los arts. 16 y 17 LSSICE.

En uno u otro caso, por lo que respecta al ámbito territorial (arts. 2-4 LSSICE), quedará sometido a la normativa española o europea sobre SSI, en virtud del llamado «principio de origen», si tiene *establecimiento* en España, sea este el correspondiente a su residencia o domicilio social, sea un «establecimiento permanente» a través del cual realice continuada o habitualmente toda o parte de su actividad (aunque no sea la tecnológica, sino solo, por ejemplo, la contratación de publicidad; no basta con la tenencia de medios técnicos en España para considerarlo establecido aquí). Además, como cláusula de cierre, resulta aplicable igualmente la norma española si el servicio se dirige «específicamente a territorio español»:[4]

UBER

Reciente doctrina del TJUE pone de manifiesto que si el SSI se presta como *«parte» de otro principal* que nada tiene que ver con prestaciones electrónicas a distancia, el servicio en su conjunto no puede ser considerado *auténtico* SSI: caso *Uber* (STJUE de 20/12/2017, asunto C-434/15, Asociación Profesional Élite Taxi c. *Uber Systems Spain SL*, en respuesta a una cuestión prejudicial planteada por un juzgado de Barcelona, con importantes consecuencias para la llamada «economía colaborativa»: para el TJ, la labor de Uber (que pone en contacto a clientes con propietarios de vehículos que, sin ser profesionales, prestarán a aquéllos un servicio de transporte) «(…) debe considerarse que *este servicio de intermediación forma parte integrante de un servicio global cuyo elemento principal es un servicio de transporte* y, por lo tanto, que no responde a la calificación de "servicio de la sociedad de la información" (…)».

«Nuestro objetivo es ofrecer anuncios y otro contenido comercial o patrocinado que sea valioso para nuestros usuarios y anunciantes», reza una cláusula del servicio de Facebook. En las redes sociales hay «dos servicios diferentes que completan su negocio» (R/02780/2009 y R/00508/2011 de la AEPD), por lo que la existencia de una «oficina de ventas» en territorio nacional es suficiente, a los efectos del art. 2.2 LSSICE, como

criterio de conexión para aplicar la normativa española (STS de 4 de marzo de 2013, RJ \2013\3380, FJ Cuarto, *in fine*), aproximación que corrobora el TJUE en el asunto Google Spain (STJUE de 13 de mayo de 2014, asunto C-131/12, Google Spain SL y Google Inc. contra Agencia Española de Protección de Datos y Mario Costeja González).

Por lo que respecta a la dirección de los servicios «específicamente para territorio español», no hay que entender que lo sean únicamente para nuestro país, pero tampoco que lo sean «*todos* los que resulten accesibles» desde España. Se comprende que la referencia se hace a la prestación del servicio en sí, dado que si tuvieran aquí oficinas de atención a los usuarios o de ventas, les resultaría de aplicación el criterio anterior, y tampoco es requisito suficiente la utilización de medios tecnológicos situados en territorio español. En este punto, la doctrina sentada por la STJUE del 7 de diciembre de 2010 (asuntos acumulados Pammer y Alpenhof GesmbH, C-585/08 y C-144/09), puede resultar indicativa de los factores que hay que tener en cuenta, como por ejemplo las condiciones o políticas del servicio (con mención expresa de territorios, para incluirlos o excluirlos), la lengua en que estén redactadas, la moneda en que se permite el pago (en particular, si es distinta de la propia del prestador), el empleo de nombres de dominio generales (.com) o territoriales propios (.es), y otros criterios como la distribución de sus *apps* o los programas de acceso en tiendas o mercados que, a su vez, estén dirigidos al territorio español, y la existencia de publicidad segmentada por nacionalidad (e, incluso, localidad), con prestación de servicios añadidos y/o contenidos concretos en virtud de la misma. El elemento definitivo podría ser, dadas las posibilidades técnicas, la no exclusión del propio servicio a los usuarios cuyas IP proceden de España, lo cual es tecnológicamente factible y hasta sencillo, y que llevan a cabo diversos prestadores.

Un ejemplo de ello es la personalización de las *tendencias* en Twitter, que dispone de la opción «global» (con lo que informa al usuario de los temas de actualidad a nivel mundial) y de un listado de países entre los que se encuentra España pero no, por ejemplo, Bulgaria (en el momento de escribir estas líneas, en mayo de 2017). Esto demuestra que los datos de localización de los usuarios se pueden tratar para mostrar a cualquiera de ellos un contenido muy concreto (en este caso, las tendencias, *trending topics* o temas de los que más se habla en España) que tiene en cuenta específicamente el mercado o territorio español, pero no otros países, aunque su servicio pueda ser utilizado también desde ellos. Tampoco su función de *ads* es contratable desde países sujetos a sanciones comerciales o con control de las exportaciones bajo la normativa de los EE. UU., como Rusia o Bolivia.

(4)Con independencia de la aplicación de la legislación sobre tratamiento de datos, no cabe duda de que a los SRS (a la mayoría de los existentes que permiten el acceso desde España) se les aplica la LSSI española (Directiva 2000/31 europea) como *prestadores de servicios de la sociedad de la información que son*.

1.2. El tratamiento de datos (personales) como base de la actividad de prestación de servicios de red social

Todo SRS se basa en la aportación de información y contenidos por parte de sus usuarios. Mucha de esa información, que puede ser relevante desde diferentes perspectivas jurídicas (derechos de la personalidad, propiedad intelectual, etc.), será además calificable de «dato personal», puesto que no se debe olvidar que el servicio que presta la red social es, básicamente, de relación entre individuos. Estos actúan a través de un «perfil», descripción propia que ya contiene datos personales y que es visible para los demás ya sea fuera de la propia red, para cualquier internauta, o de forma más restringida. Además, en un perfil público los contactos propios, identificados a su vez por sus respectivos datos personales, son también accesibles para terceros...

Mas junto a los datos personales fácilmente perceptibles como tales por cualquiera (nombre, dirección física, fotografías propias, informaciones sobre estudios, localizaciones expresamente compartidas, mención de enfermedades o particularidades físicas, etc.), existen otros más «opacos» al propio usuario pero que, no por ello, dejan de ser también «personales» y que convierten al sujeto en «identificable» a los efectos de la LOPD o el RGPD, arts. 3.a y 4.1, respectivamente. Entre estos datos del usuario figuran la dirección IP de los

distintos dispositivos desde los que accede a la red, las fotografías (y metadatos de las mismas) en las que, aunque no aparezca su imagen, permiten relacionarlo con él y/o su localización (la de su domicilio, por ejemplo), los propios ficheros que va generando con su actividad e interacción con otros usuarios y los contenidos de terceros (al pulsar «me gusta», «retuiteando», etc.), todo lo cual pone de manifiesto su personalidad y sus gustos. En ocasiones, un dato que en apariencia es irrelevante jurídicamente o de tal generalidad que no queda vinculado a una persona en concreto se convierte en «personal» por su relación con otro cualquiera de los cientos o miles de informaciones concretas que cada individuo o sus contactos comparten o hacen públicas.

A principios de 2015 tuvo gran repercusión la noticia de unos investigadores de la Universidad de Cambridge que, tras analizar las interacciones de 8.000 usuarios de Facebook, crearon un programa capaz de «conocer» a una persona incluso mejor que sus propios allegados. Con solo 10 «me gusta», el *software* podía establecer los rasgos anímicos y gustos de una persona con mayor precisión que un simple compañero de trabajo. Con algunos más (150), lo hacía mejor que un amigo y, con 300, mejor que el cónyuge. Véase <http://www.abc.es/tecnologia/redes/20150113/abci-facebook-conoce-mejor-familia-201501131202.html>. Y eso, en 2015...

A título de ejemplo, son datos personales los siguientes:

- el nombre, los apellidos y el domicilio,
- el DNI (SAN 27 de octubre de 2004, JUR 2005\222326),
- los números de teléfono (SAN 26 de enero de 2005, JUR 2005\223032, aunque con matices, SAN 17 de septiembre de 2008, JUR 2008\307282),
- los datos relativos al ejercicio de una profesión (SAN 11 de febrero de 2004, RJCA 2004\421),
- la dirección de correo electrónico y hasta la IP (STS 3 de octubre de 2014, RJ 2014\4718; Informe 327/2003 de la AEPD; el art. 4.1 RGPD cita el «identificador en línea» como ejemplo de dato que hace identificable a una persona),
- la información genética (véase la Recomendación del Comité de Ministros del Consejo de Europa (97)5, de 13 de febrero de 1997, expresamente recogida en el art. 9 RGPD, junto con los datos biométricos, como categoría especial de datos),
- la imagen de la persona (STC 14/2003, de 30 de enero),
- las cuentas bancarias y los datos de solvencia patrimonial (arts. 29 LOPD y 38-44 RLOPD).

No es aconsejable hacer públicas muchas de estas informaciones, aunque no es menos cierto que, por ejemplo, una fotografía puede mostrar mucho más de lo que aparenta, puesto que la imagen del individuo en un perfil nos informa no solo de su edad, sexo, raza, sino también, según el contexto, de su procedencia, afiliación política (si ha sido tomada con una pancarta, en un mítin, con un comentario sobre su candidato preferido), su estado de salud (si la foto es en un hospital, al identificar a quien hace un comentario puede estar mostrando que sufre una afección o que se está sometiendo a un tratamiento…), sus preferencias sexuales… Muchas de estas informaciones son datos objeto de una especial protección que, además, podrían ser facilitados por otros usuarios (por ejemplo, a través del etiquetado de las personas que salen en la foto que uno de ellos sube a la red). Los SRS disponen de servicios de notificaciones automáticas de tales circunstancias, de manera que el interesado etiquetado o que ha sido nombrado en una conversación puede pedir la eliminación del dato o borrarlo directamente. Aun cuando se trate de «usos privados» de los usuarios, no cabe olvidar que el SRS es el responsable también de esas menciones por parte de terceros (véase más adelante), por lo que tendrían que ser suprimidas en el caso de una reclamación de otro titular.

> Aunque el propio GT29 no se muestra partidario de considerar las meras imágenes en Internet como «datos sensibles», es consciente de que algunos Estados miembros sí les dan un tratamiento especial, por cuanto sirven para determinar el origen racial o étnico de los fotografiados, o bien porque a partir de ellas se pueden deducir sus creencias religiosas o datos relativos a su salud (apdo. 3.4 Dictamen 5/2009).

Así pues, en el marco de un SRS, los datos personales de todo tipo se recogen, registran, organizan y estructuran siguiendo procedimientos automáticos o no. Son ejemplos de ello los datos de los dispositivos de acceso, las relaciones entre los usuarios y los contenidos que sugiere el sistema según las preferencias; cabe también mencionar la introducción manual de datos por parte de los propios usuarios al suscribir el servicio o al manifestar sus gustos. Posteriormente, el propio SRS conserva dichos datos para la prestación del servicio y los usuarios los consultan y difunden. Tras la baja del usuario, los datos deben ser suprimidos, destruidos o anonimizados (e, incluso, durante su tratamiento, a los efectos que sea: «disociación», *ex* art. 3.f LOPD, o «pseudonimización», art. 4.5 RGPD). Para ofrecer la prestación del servicio, internamente dichos datos quedan almacenados en «ficheros» (arts. 3.b LOPD y 4.6 RGPD) y se crean «perfiles» distintos de los creados por los propios usuarios como presentación en la red social. Nos referimos propiamente a la evaluación interna de los datos que realiza el prestador con el fin de analizar preferencias personales, intereses, comportamiento, ubicación o movimientos de los usuarios, de manera que se puedan servir a los usuarios contenidos personalizados, incluidos los publicitarios, así como sugerirles nuevos contactos según sus afinidades, localización, amigos comunes, etc. (art. 4.4 RGPD).

En definitiva, en los SRS se dan plenamente los requisitos para considerar que hay «tratamiento de datos», a los efectos de la normativa vigente (tanto la LOPD, art. 3.c, como el RGPD, art. 4.2). Por ello, en principio ese tratamiento debería hacerse bajo el principio del «consentimiento» del usuario afectado o titular de tales datos personales (en el sentido de los arts. 3.e y 3.h LOPD, y 4.1 y 4.11 RGPD), puesto que existe un «responsable de dicho tratamiento» (indudablemente, el prestador del SRS, pero ¿también los usuarios?; véase más adelante) que ha de incluir, asimismo, las posibles cesiones o transferencias de datos (incluso de carácter internacional, dado que muchas de estas redes sociales están ubicadas fuera de la Unión Europea[5]).

[5] La actividad del prestador de SRS constituye, sin duda, un «tratamiento de datos» a los efectos de la normativa europea aplicable, que convierte a dicho prestador en «responsable del tratamiento», sin perjuicio de su posible concurrencia con otros responsables.

1.3. La aplicación de la normativa europea (y española) de protección de datos

En el apartado anterior hemos concluido la existencia de un tratamiento de datos objeto de regulación conforme a las normas europeas (y españolas que traen causa de aquellas), lo cual, de forma intuitiva, no plantea ningún problema para el caso de que las redes sociales estuvieran domiciliadas o tuvieran un establecimiento en territorio europeo (caso del RGPD), incluido el español (la todavía vigente LOPD, o la norma que la sustituya). En este caso, como para cualquier otra empresa, el ámbito territorial no constituye un problema y es el principio general consagrado por dicha normativa. Así, el RGPD expresamente contempla su aplicación «al tratamiento de datos personales en el contexto

de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no» (art. 3.1). Es irrelevante que el tratamiento, en sentido técnico-informático, se realice en territorio europeo o no, pues lo importante es su imputación a un responsable o encargado *establecido* en el mismo.

El art. 2.1.a) LOPD, en el mismo sentido, señala que «cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento».

Obsérvese que, en ambos casos, es el principio general consagrado también en la LSSI, derivado de la Directiva 2000/31, como se ha visto antes.

Sobre el concepto de «establecimiento», véase el considerando 22 del RGPD: «implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto». Si hubiera varios, el «establecimiento principal» se determinará conforme al art. 4.16.

Téngase en cuenta, además, que el reglamento no protege propiamente a los «ciudadanos europeos», sino a cualquier persona que se encuentre en territorio de la Unión Europea, con independencia de su nacionalidad (art. 3.2 y considerando 14 RGPD).

Sucede, sin embargo, que muchos de los SRS son prestados por empresas fundadas y establecidas fuera de nuestro continente (sin ni siquiera una filial con personalidad jurídica o una simple sucursal que sirviera de criterio de anclaje normativo conforme al considerando 22), aunque dirijan su actividad también a usuarios europeos. Según el criterio anterior, por lo tanto, quedarían excluidos del reglamento los ciudadanos residentes en la Unión Europea, por lo que estarían desprotegidos. Evidentemente, el legislador europeo pretende evitar tal resultado y, en consecuencia, a continuación extiende el ámbito territorial de aplicación de la norma para incluir todo tratamiento de datos personales

«de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión».

Queda claro, por lo que respecta a los SRS, que se aplicará el reglamento a todos los que, de alguna manera, dirijan sus servicios a usuarios residentes en Europa, con independencia del lugar desde el que operen. Los servicios se ofrecen a interesados de los Estados miembros, de forma que las personas son objeto de un seguimiento, sea cual sea el origen de los datos, incluso si se recogen de registros públicos o de anuncios accesibles desde fuera de la Unión, y puesto que dichos datos se usan, entre otros aspectos, para elaborar un perfil que muestra o predice sus preferencias personales, comportamientos y actitudes (véanse los considerandos 23 y 24 RGPD).

La nueva solución legislativa supone un cambio de paradigma respecto del factor de conexión existente hasta el momento y esta modificación, como señala Troncoso Reigada (2012b, pág. 66), tiene en cuenta una «necesaria orien-

tación hacia las personas» (en terminología del Dictamen 8/2010 sobre derecho aplicable, emitido por el GT29 el 16 de diciembre de 2010). Efectivamente, en la normativa europea y estatal vigente hasta la efectividad plena del reglamento (Directiva 95/46 y LOPD), más allá del *establecimiento* en el territorio (arts. 4.1.a Directiva 95/46 y 2.1.a LOPD), el criterio de cierre es el *lugar de realización del tratamiento*, y también será aplicable la norma interna cuando el responsable no esté establecido en España (o en la Comunidad, según la directiva) pero recurra para el tratamiento *a medios, automatizados o no, situados en territorio español*, salvo que sean únicamente con fines de tránsito (arts. 4.1.c Directiva 95/46 y 2.1.c LOPD). No hay duda de que esta circunstancia se da, por la propia naturaleza del servicio, cuando este está dirigido a ciudadanos españoles (europeos). Tales medios son los propios dispositivos desde los cuales los usuarios suscriben y acceden al servicio (esencialmente, PC, móviles y *tablets*), crean sus perfiles, y en los que quedan instaladas u operan sus aplicaciones, *cookies*, robots, etc., todos ellos elementos que tienen acceso a sus datos, IP, agendas, contactos, calendarios, vídeos, fotografías…

Señala el GT29 en su *Dictamen 1/2008 sobre asuntos relativos a la protección de datos vinculados a las herramientas de búsqueda*, de 4 de abril de 2008: «el ordenador del usuario puede considerarse un medio en el sentido del artículo 4 (1) de la Directiva 95/46/CE. Se encuentra situado en el territorio de un Estado miembro. El responsable decide recurrir a este medio con el fin de tratar datos personales y, según se ha explicado en apartados anteriores, se producen diversas operaciones técnicas sin el control del interesado. El responsable de tratamiento controla el equipo del usuario y este equipo no se utiliza exclusivamente con fines de tránsito por el territorio de la Comunidad Europea». El criterio ya había sido adelantado en el *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* (WP56, aprobado el 30 de mayo de 2002), y es reiterado posteriormente en los *Dictámenes 8/2010* (con varios ejemplos) y *02/2013*. En este último, en relación con los dispositivos móviles, se concluye que «dado que el dispositivo resulta fundamental para el tratamiento de los datos personales del usuario y sobre él, este criterio suele cumplirse (en la medida en que la aplicación genera tráfico de datos personales con los responsables del tratamiento de datos)». Véase también el citado *Dictamen CNS-24/2013* de la Autoridad Catalana de Protección de Datos, en relación con las aplicaciones de mensajería instantánea.

Los dispositivos móviles (*smartphones* y *tablets*) son, a fecha de hoy, el principal medio de acceso y, por lo tanto, de recogida de datos personales en las redes sociales. No se trata únicamente de que sean el medio preferido para el acceso a Internet (51,3% frente al 48,7% de los ordenadores de escritorio, a nivel mundial; en España llegan al 54,9%; véase <http://gs.statcounter.com/press/mobile-and-tablet-internet-usage-exceeds-desktop-for-first-time-worldwide>), sino que se accede a las redes sociales preferentemente desde este tipo de dispositivos (por ejemplo, según las estadísticas de Twitter, de sus 313 millones de usuarios activos, el 82 % eran usuarios desde móviles en junio de 2016; véase <https://about.twitter.com/es/company>). La movilidad implica que el usuario lleva su dispositivo encima, por lo que el suministro de datos a la red (como la identidad del dispositivo, su localización mediante diferentes nodos y redes de comunicaciones, las entradas de eventos, fotografías, etc.) es constante y desde distintos lugares (lo cual, en sí mismo, ya permite, de forma menos transparente para dicho usuario, generar perfiles publicitarios *ad hoc*).

Así, incluso en casos como Snapchat, en los que parece que la empresa es reacia a establecerse en países o nuevos mercados como España (<http://www.lavanguardia.com/tecnologia/20170413/421677482201/snapchat-evan-spiegel-snap-facebook-juicio.html>), se aplicaría nuestra legislación, puesto que el acceso a la red está habilitado desde nuestro territorio, con acceso en (perfecto) «español» (de España, a juzgar por los términos empleados en las traducciones) y con posibilidad de introducir geofiltros con condiciones de uso *ad hoc* (aunque en inglés) para la Unión Europea.

En cuanto al criterio general de conexión del *establecimiento*, en el citado caso *Google Spain* de 2014, el TJUE dejó claramente sentado que se aplica la norma europea (o nacional de transposición) cuando el responsable dispone de algún establecimiento que, aunque no vinculado directamente con la prestación del servicio tecnológico (o la atención a sus usuarios como tales), sí se ocupa de «garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro» (apdo. 60). Más allá de que los SRS dispongan de buscadores, no hay que olvidar que esta sentencia interpreta el precepto de la directiva (art. 4) aplicable a todo tratamiento y responsable, por lo que no cabe duda de su extensión a estos servicios. En consecuencia, cualquier establecimiento o filial que tuviera el prestador del SRS en España para la gestión de sus actividades comerciales o publicitarias permitiría, de por sí, la aplicación de la legislación española.

En definitiva, es difícil pensar en supuestos en los que no resulte de aplicación tanto la legislación española de protección de datos como el reglamento europeo a proveedores de SRS cuando estos se dirigen a (o permiten el acceso de) usuarios que físicamente se encuentren en territorio español, con todo lo que ello conlleva respecto al cumplimiento de tales normas, las responsabilidades que de ellas se deriven y la sujeción a las autoridades de control nacionales (AEPD) y europeas.

2. El prestador de SRS como responsable del tratamiento de datos

El titular de la red social es quien oferta el servicio que se provee a los usuarios, disponiendo los *medios técnicos* al efecto y decidiendo *sobre la finalidad, el contenido y el uso del tratamiento de los datos que tales usuarios suministran, o que de ellos* (a través de su propia actividad en la red, de manera más o menos consciente) *se recaban*.

El prestador controla todas las intervenciones hechas por cada usuario en la red, desde su suscripción (y cualquier entrada posterior) hasta los cierres de sesión y la eventual cancelación del servicio, y lo hace conforme a la finalidad que él mismo define al crear la red y/o añadirle nuevas funciones; cuando menos, la de promover la comunicación entre sus usuarios, pues en eso consiste la esencia de toda «red social» y para ello se ordenan los recursos tecnológicos que la hacen posible. En virtud de ello, el prestador relaciona perfiles, preferencias, mensajes, etc., creando una gran base de datos que actúa, en cada momento y respecto de cada petición individual (de las cientos o miles de millones que pueden darse en un segundo), como un auténtico buscador que provee enlaces entre los diferentes usuarios e, incluso, hacia fuera del propio SRS (según la configuración del perfil del usuario, puede ser accesible e indexable desde buscadores externos). A partir de ahí, la especialización de ciertas redes permitirá un mayor/mejor intercambio de ciertos datos y no de otros (por ejemplo, solo fotografías o textos breves, o bien permite otros contenidos que el enfoque de esa red no tiene en cuenta de forma prioritaria).

También hay otra finalidad que, si bien pudiera considerarse accesoria en cuanto al objeto mismo de la red social, es, sin embargo, principal por lo que al negocio del prestador del SRS respecta y que de hecho, hoy en día, está en el origen de la creación de nuevas redes. Se trata de la obtención del beneficio económico que se conseguirá, por lo general (y más allá de puntuales servicios *premium* o *freemium*, de cobro directo a algunos usuarios), a través de la publicidad orientada a los usuarios y servida a cada uno de ellos de forma personalizada, según su actividad, localización y sus preferencias. Nuevamente, el prestador es quien decide que los datos de sus usuarios puedan ser explotados comercialmente, bien por él mismo, bien por terceros que contratan sus servicios de anuncios o publicidad (esto es, colocan su publicidad en la red a través de los ficheros de actividad de los usuarios que controla el prestador).

Es más, la mayoría de SRS disponen de aplicaciones o *apps* para dispositivos «inteligentes» (teléfonos móviles, *tablets*, e, incluso ya, algunos *wearables*, como relojes o accesorios para prendas de ropa). En relación con este tipo de *software*, el *Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes* adoptado el 27 de febrero de 2013 por el GT29, dejó claro que los desarrolla-

dores de tales aplicaciones (que, en lo que nos ocupa, pueden ser los propios SRS o terceros) son «responsables del tratamiento», pues «deciden la medida en que la aplicación accederá y procesará las distintas categorías de datos personales en el dispositivo y/o a través de recursos informáticos remotos (unidades informáticas de los desarrolladores o de terceros)».

En definitiva, sea cual sea el aspecto de la actividad de la red que se tenga en cuenta, está claro que el prestador de un SRS *es* un «responsable del tratamiento» a efectos legales (art. 3.d LOPD y 4.7 RGPD), con todas las obligaciones (la mayoría de las cuales son configuradas como *«de resultado»*) y responsabilidades que ello comporta y que, con carácter general y sin perjuicio de acotar algunos aspectos en los apartados siguientes, ya han sido expuestas en anteriores módulos.

2.1. Proactividad y seguridad

Como responsables del tratamiento, la clave de la actuación de un prestador de SRS es la «proactividad». Es decir, ha de poder demostrar el cumplimiento de todos sus deberes u obligaciones (*accountability*, en los arts. 5.2 y 42 RGPD, entre otros), y ha de implantar todo tipo de medidas para garantizar el correcto ejercicio de sus obligaciones.

Las redes sociales están sujetas a continuos ataques informáticos, por lo que la seguridad en las mismas es sumamente importante. Manejan, además, muchas clases de datos y, por consiguiente, han de adoptar medidas de seguridad del máximo nivel. Por lo que respecta al nuevo RGPD, deben notificar, por ejemplo, las brechas de seguridad cuando se produzcan (arts. 33 y 34), aunque lo cierto es que, hasta el momento, siempre han sido muy reacias a admitirlas.

Así, Yahoo! ha tardado años en reconocer que sus servidores habían sido comprometidos hasta en dos ocasiones y que habían sido robadas hasta 1500 millones de cuentas (*logins* y claves) que se utilizaban para acceder a sus servicios (entre ellos, redes sociales como Flickr) o a los de terceros (véase <http://www.lavanguardia.com/tecnologia/20161215/412628014394/yahoo-robo-datos-mil-millones-cuentas.html>).

2.2. Importancia de la «privacidad por defecto» en los SRS

En el marco del RGPD, más que simples obligaciones (aunque como tales aparecen también reguladas en su art. 25), la «privacidad desde el diseño» (*privacy by design*) y la «privacidad por defecto» (*privacy by default*) constituyen principios básicos que han de presidir las políticas internas que siga cualquier responsable del tratamiento y así se contemplan en los considerandos 78 y 108 y en el art. 47.2.d.

Según el art. 25.2 RGPD, «el responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales

medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas».

Por su parte, la *privacidad desde el diseño* supone la obligación del responsable del tratamiento de implantar la política de protección de datos en todos sus extremos desde el comienzo de cualquier proyecto (valorando, por ejemplo, las posibilidades de *anonimización* o *seudonimización* de los datos), y no como una última capa o revisión añadida una vez dicho proyecto está prácticamente listo, tal como ocurre muchas veces en la actualidad. En definitiva, la protección de datos debe ser un elemento más a considerar en cualquier nuevo plan de negocio o medida de desarrollo, en igualdad de condiciones que los demás factores técnicos, económicos o de oportunidad.

La privacidad por defecto implica que al cliente o usuario se le ofrezca el servicio, desde el principio, con el mayor nivel de privacidad posible, de manera que sea él mismo quien, si lo desea, la rebaje mediante expresos actos de voluntad que serán considerados manifestaciones de consentimiento al correspondiente nivel de difusión y tratamiento de sus datos personales.

Por lo que ahora nos ocupa, y en un rápido e intuitivo ejemplo, un prestador de SRS deberá dar a una nueva cuenta, por defecto, el nivel más alto de privacidad, haciendo «públicos» (es decir, accesibles al resto de usuarios), en principio, la menor cantidad posible de datos, y abriendo el perfil solo cuando el usuario expresamente lo permita (y con la extensión que quiera) a través de las opciones de configuración de dicha cuenta. En definitiva, el perfil inicial del nuevo usuario deberá ser lo más restringido posible en relación con quién puede ver sus datos y publicaciones (solo él o, a lo sumo, solo sus contactos, mostrándose para el resto únicamente el *nick* o 'nombre de usuario', que puede no coincidir con el real, y la página en blanco o «no disponible»), el tiempo (en su caso) que permanecen visibles o desactivadas las opciones para que los demás lo busquen para contactarle, etc., de tal manera que sea el propio usuario quien modifique cada uno de esos extremos durante el proceso de configuración de su cuenta, o bien que en cualquier momento posterior pueda volver a dicha configuración de máxima privacidad (como forma de retirada del consentimiento inicialmente dado o de oposición a determinados tratamientos).

Así contemplado, lo cierto es que esta privacidad por defecto *parece* contraria al funcionamiento mismo de una red social esencialmente colaborativa y tendente a fomentar el número de relaciones entre sus usuarios. De hecho, en sus inicios, la apertura tradicional de una cuenta presentaba activadas por defecto todas las opciones de contacto y difusión, incluso fuera de la propia red (quedando la cuenta accesible desde Internet en general). En un segundo periodo, las cuentas se presentaron más cerradas, limitadas a la red social, pero en modo «público» o con visibilidad para «amigos de amigos» (a los contactos de los contactos del usuario). La forma actual, en la mayoría de casos, consiste en presentar la opción más cerrada pero ofreciendo ya las casillas premarcadas de la configuración pública estándar (o el *encarecido* «consejo» de marcarlas).

Todas estas técnicas habrán de desaparecer y deberá presentarse al usuario, desde el inicio (durante la apertura de la nueva cuenta), un perfil claro y cerrado, transparente, no condicionante de su decisión y sin casillas premarcadas (el consentimiento debe ser mediante declaración expresa o «acción afirmativa», art. 4.11; véase más adelante).

2.3. Transferencia internacional de datos

Las grandes redes sociales son, esencialmente, internacionales, siendo las redes «locales» una excepción en este tipo de servicios. Ello hace imprescindible su sujeción a la normativa sobre transferencias internacionales de datos, es decir, la obligación de recabar los correspondientes consentimientos al respecto (arts. 34 LOPD y 47 RGPD) y/o mantener amparadas por las autorizaciones de las Agencias de Protección de Datos las «garantías adecuadas» del art. 46 RGPD o los acuerdos suscritos por la UE.

Al respecto, el nuevo *Privacy Shield* (Decisión de la Comisión C(2016) 4176 final, de 12 de julio de 2016) regula las transferencias con los Estados Unidos (origen de la mayoría de las redes sociales que operan en Europa) en sustitución del anterior régimen del Puerto Seguro (*Safe Harbor*, aprobado por Decisión de la Comisión 2000/520/CE, de 26 de julio de 2000), que el Tribunal de Justicia, en su sentencia de 6 de octubre de 2015 (asunto C-362/14, caso Schrems), declaró no conforme con el derecho europeo. Bajo la prohibición de que la Comisión impidiera las competencias de las autoridades nacionales para la valoración del nivel de protección que ofrecen los países destinatarios de los datos, el Tribunal sancionaba la nulidad del acuerdo alcanzado entre la misma y los Estados Unidos por no garantizar un nivel de protección suficiente («adecuada») para los ciudadanos europeos. Efectivamente, era palmario que las empresas estadounidenses gozaban de grandes privilegios (así, por ejemplo, certificaban sus propios procedimientos de protección) y las autoridades estadounidenses tenían grandes poderes de acceso a los datos. Frente a ello, el nuevo acuerdo entre Europa y los EE. UU., que se desarrollará como «decisión de adecuación» prevista en el art. 45 del reglamento (equivalente al vigente artículo 25 de la directiva que lo ampara en la actualidad), permitirá la transferencia de datos sin necesidad de autorizaciones específicas, toda vez que el gobierno estadounidense ha garantizado (o, al menos, lo había hecho antes de la llegada del presidente Trump…) el no acceso generalizado a los datos e impone a sus empresas unas obligaciones de cumplimiento más rigurosas, al tiempo que se prevén mecanismos para que los ciudadanos europeos puedan reclamar frente a posibles vulneraciones.

SRS como Facebook o Twitter ya cumplen con los principios del *Privacy Shield* y puede consultarse el listado de empresas que lo han suscrito en <https://www.privacyshield.gov/participant_search>.

2.4. El delegado de protección de datos

El reglamento europeo recoge una nueva figura que, bajo el principio de actuación autónoma e independiente, tiene por función informar y supervisar el tratamiento de datos que hace la empresa, así como servir de punto de contacto con la autoridad de control. Es el delegado de protección de datos (DPO, por sus siglas en inglés, *data protection officer*), regulado en los arts. 37 a 39.

La novedad de esta figura es relativa. Es nueva para España, cuya legislación actual (LOPD) no la recoge, pero no para otros Estados miembros en los que ya existía con carácter obligatorio (Alemania) u opcional (Austria u Holanda). En un término medio, el reglamento europeo no ha impuesto una obligación general de nombramiento de un DPO para todo responsable o encargado del tratamiento, pero sí para las administraciones públicas (salvo la judicial en el desempeño de su función) y para las entidades que, como los SRS, son responsables del tratamiento de datos personales a gran escala, en particular si lo hacen sobre categorías especiales de datos (art. 37).

Dado que el DPO puede desarrollar otras funciones y otros cometidos además de los que le son propios, es posible que sus funciones sean asumidas o compartidas por los delegados de *compliance* (*compliance officers*) de la empresa. Ciertamente, son figuras distintas cuyas funciones, por lo que respecta a la protección de datos, pueden ser redundantes, de ahí el aprovechamiento del personal dedicado a ellas, en especial en empresas no muy grandes. No obstante, en grandes redes sociales de carácter internacional, creo que la mejor opción es mantener separadas ambas figuras, por la propia relevancia del papel del DPO para el servicio, por ser el tratamiento de datos no un instrumento para la consecución de sus fines sociales, sino su propio objeto de negocio.

2.5. Régimen de infracciones y sanciones

El régimen de responsabilidad no presenta mayores especialidades por el hecho de ser el responsable del tratamiento un prestador de SRS. La LOPD recoge tanto la responsabilidad civil (art. 19) como la administrativa (art. 43.1 y 44 y siguientes, en cuanto a ficheros de titularidad privada), que pueden ser concurrentes o no. En el RGPD se regulan en los arts. 77 y sigs.

En la normativa vigente (LOPD) cabe, en los casos de infracción grave o muy grave, la inmovilización de los ficheros, si no se atiende el requerimiento para cesar el uso ilícito, en tanto se restauren los derechos de los afectados. Una sanción de este tipo a un prestador de SRS supone, *de facto*, la paralización de su actividad, dado que su fichero de usuarios *es* su negocio.

El órgano sancionador será la AEPD (art. 37.1.g), pues sus posibles equivalentes autonómicos no tienen competencias sobre ficheros privados, como son los de los SRS. Parece tendencia de la AEPD reservar los procesos sancionadores para

los casos más graves y apostar, en primer lugar, por el ejercicio del derecho de cancelación como método para la resolución de conflictos entre el responsable y el afectado.

Como más adelante se verá, el consentimiento es esencial en el tratamiento de datos que realiza no solo el SRS, sino sus propios usuarios. No obstante, en la resolución del PS/00508/2008 puede leerse, en relación con su exigencia, que su aplicación estricta paralizaría Internet (cursivas mías) «o la convertiría en una red profusa en vulneraciones de datos personales de millones de personas accesibles fácilmente usando un mero buscador y de los que no cabe aportar el consentimiento previo». Es por ello que «debe considerarse el principio según el cual, cuando el ordenamiento jurídico ofrece varias soluciones, sea más adecuado el agotamiento de otras fórmulas alternativas en el caso de que sea posible, razón por la que *el uso del derecho de cancelación de datos tendente al cese del tratamiento de datos personales debe priorizarse*. Se trataría de un procedimiento que posibilita la corrección con celeridad del dato incluido con objeto reparador con carácter previo a una tutela por incumplimiento o a la incoación, en su caso, de un procedimiento sancionador, que reviste naturaleza punitiva si no se hiciera desaparecer». Ahora bien, en determinados supuestos, como el denunciado (divulgación de vídeos de menores en YouTube), sí procede la apertura de expediente sancionador, dada su especial gravedad, lo que fue ratificado por la posterior SAN de 20 de octubre de 2011 (RJCA 2011\927).

La *responsabilidad civil* (arts. 19.1 LOPD y 79 y 82 RGPD) es exigible ante la jurisdicción ordinaria y sin necesidad de previa reclamación ante la AEPD.

Responsabilidad civil y administrativa son distintas, sin que la civil dependa, siquiera, de la apreciación previa de infracción por parte de la AEPD. Así, en la R/00836/2015 de la AEPD, la cual, aun estimando la existencia de infracción, procede al archivo del caso frente al fotógrafo profesional usuario de Facebook que subió a dicha red una fotografía, dada la inmediata satisfacción de la cancelación solicitada por la denunciante en nombre de su hijo menor. En dicha resolución se da noticia de las actuaciones que sobre ese mismo caso se habían seguido ante el JPI frente a la fotógrafa que había entregado dicha imagen al denunciado ante la AEPD, y que habían dado ya lugar a la SJPI nº 4 de Albacete de 23 de julio de 2014, por la que se condenó al pago de una indemnización de 500 €. Posteriormente, y aunque ya no lo recoge la AEPD, fue incrementada esa cantidad en apelación hasta 6.000 € (SAP de Albacete de 14 de enero de 2015, JUR 2015\76843).

Cualquier otro perjuicio que derive de la afectación de otros derechos (incluso generado a partir de la misma conducta que infringe la protección de datos) será reclamable conforme a las disposiciones generales contenidas en el Código Civil u otra legislación especial que resulte de aplicación (por ejemplo, honor, intimidad e imagen, según lo dispuesto en la LO 1/1980).

Por lo que respecta a su *concurrencia con otros posibles responsables*, así como a la *responsabilidad del prestador por los usos ilícitos de su servicio por parte de los usuarios*, nos remitimos a los apartados 3.2 y 5, respectivamente, de este mismo tema.

3. Los usuarios de redes sociales como responsables, o no, del tratamiento

Básicamente, hay dos tipos de usuarios de redes sociales: los *particulares* (personas físicas individuales) que los utilizan para fines simplemente personales (a efectos de la normativa pertinente, pueden tener la calificación de «consumidores» o «usuarios») y los *profesionales* o *corporativos* (empresas, asociaciones, administraciones…) que utilizan la red como plataformas para el desarrollo de actividades comerciales, políticas, sociales o de servicio público. ¿Cuál es su posición en relación con los datos de terceros que manejan (sus contactos, seguidores, personas a las que siguen, etiquetan, etc.)?

3.1. La posición de los usuarios particulares

En el nuevo Reglamento general de protección de datos, la posición de los usuarios particulares en las redes sociales parece clara, en cuanto *se beneficiarán de la excepción de tratamiento personal* o *doméstico* que prevé la norma, aun cuando en dichos ámbitos realicen actividades propias de un tratamiento de datos (recaban datos de contactos con los que interactúan, comparten sus publicaciones, las marcan como favoritas, contestan, etiquetan a terceros o se refieren a ellos extendiendo las relaciones…). Tal es el sentido del art. 2.2.c) según lo explica su considerando 18 (cursivas mías):

> «El presente reglamento *no se aplica* al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, *sin conexión alguna con una actividad profesional o comercial*. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o *la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades* (…)».

El reglamento se ha posicionado, así, claramente a favor de los usuarios de redes sociales «como tales», no como «interesados» (afectados por el tratamiento hecho por sus pares) ni como «responsables» de los que ellos realizan.

A diferencia del RGPD, con la normativa vigente hasta su plena eficacia en 2018 (directiva y, en España, LOPD) la solución contraria (considerarlos como auténticos «responsables del tratamiento») era (es) prácticamente obligada pues, como ya había advertido el GT29 (Dictamen 5/2009) en aplicación de la doctrina de los casos Lindqvist (STJUE de 6 de noviembre de 2003, asunto C-101/01, Göta hovrätt contra Bdoil Lindqvist) y Satamedia (STJUE de 16 de diciembre de 2008, asunto C-73/07, Tietosuojavaltuutettu contra Satakunnan Markkinapörssi Oy y Satamedia Oy), bajo ciertas circunstancias (que acaban siendo la regla general en el funcionamiento de un SRS) los usuarios particulares no podrían beneficiarse de la excepción de tratamiento personal o doméstico cuando: 1) voluntariamente dieran acceso a sus perfiles a todos los usuarios de la red e, incluso, de Internet (perfiles abiertos); 2) el gran número

de contactos y el desconocimiento real de quiénes son pusiera de manifiesto que se excede el ámbito personal; o 3) se refirieran a datos de terceros particularmente sensibles.

En su virtud, muchos (¿la mayoría?) de los usuarios de SRS acababan siendo auténticos *responsables* de cuantos datos de terceros vinculasen de alguna manera a su perfil o recogieran en sus páginas o muros (fotografías, vídeos, comentarios, publicaciones, etiquetados, reenvíos, etc.), pues no resultaría aplicable la excepción personal (Campuzano Tomé, 2011, pág. 633 y Roig 2009, pág. 46), casi como consecuencia necesaria de lo que es una red social y de cómo se utilizan en la actualidad.

Tal concepción, insisto, es superada por el reglamento general europeo.

> De la SAN 15 de junio de 2006 (JUR 2006\195237) podemos deducir que el tratamiento en el «ámbito exclusivamente personal o doméstico» es aquel que se realiza para surtir efectos solo en dicho ámbito, no implica que sea hecho por un solo individuo, pero sí excluye el uso profesional. Para la AEPD (Informe 615/2008, págs. 4-5, cursivas mías), «para que nos hallemos ante la exclusión prevista en el artículo 2 LOPD, lo relevante es que se trate de una *actividad propia de una relación personal o familiar, equiparable a la que podría realizarse sin la utilización de Internet*, por lo que *no lo serán* aquellos supuestos en que la publicación se efectúe en una *página de libre acceso* para cualquier persona o cuando el *alto número de personas invitadas a contactar* con dicha página resulte indicativo de que dicha actividad se extiende más allá de lo que es propio de dicho ámbito».

> No obstante, las obligaciones (y consiguientes responsabilidades) de los usuarios particulares al respecto quedarían muy limitadas, pues su control sobre el medio tecnológico es muy reducido. De esta manera, entiendo que se centrarían esencialmente en *informar* a terceros en el caso de que hagan públicos sus datos (generalmente, fotografías o vídeos en los que son reconocibles, lo cual, dicho sea de paso, lo hace en muchos SRS la propia plataforma que notifica al interesado cuándo es mencionado o compartido), o los etiquete (para lo cual, al igual que en el caso anterior, el propio SRS suele tener un protocolo al respecto), o *suprimirlos* de su muro, perfil o publicaciones *si así se lo piden*. Además, concluía el Dictamen 5/2009, «aunque la excepción doméstica no se aplique, el usuario de SRS puede beneficiarse de otras exenciones, como la exención con fines periodísticos, artísticos o literarios. En estos casos, debe establecerse un equilibrio entre la libertad de expresión y el derecho a la intimidad» (pág. 7).

> En la línea del dictamen del GT29, la propuesta original del RGPD incluyó dentro de su ámbito a las ventas privadas o a los datos «que no guarden conexión alguna con una actividad profesional o comercial» (propuesta de considerando 15). El art. 2.2.d), tras su enmienda por el Parlamento (12 de marzo de 2014), eliminó las referencias al «interés lucrativo» y mencionaba simplemente que la excepción se aplicaría (cursivas mías) a «los datos personales cuando quepa esperar razonablemente que *solo accederán a ella un número limitado de personas*». El definitivo y más sencillo art. 2.2.c), así como su explicación en el considerando 18, son tributarios del Planteamiento general del Consejo sobre la propuesta, de 11 de junio de 2015 (9398/15), por lo que la interpretación de la norma, atendiendo a su génesis, no deja lugar a dudas: pretende descargarse a los usuarios de obligaciones y responsabilidades derivadas del tratamiento de datos, incluso cuando actúan en las redes sociales, calificando este ámbito también de personal o doméstico.

En definitiva, con la plena vigencia del RGPD, *los usuarios de un SRS no serán responsables por los eventuales tratamientos de datos personales de terceros que puedan realizar en el curso de sus actividades en la red social*, con independencia del número de sus contactos, de sus prácticas de aceptación de los mismos o del tipo de datos que manejen.

Mas, advertido lo anterior, concluye de manera rotunda el citado considerando 18 afirmando (como no podía ser de otra manera, para no vaciar de contenido la normativa) que el reglamento *sí* «se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales *relacionados* con tales actividades personales o domésticas». El prestador del SRS sí será responsable por el tratamiento de datos de terceros (ajenos o no a la red) que hagan los usuarios particulares de su servicio, por cuanto él, al disponer de la plataforma informática, es quien controla los fines de la recogida y del fichero resultantes.

> Además, al producirse un perjuicio por un uso ilícito de esos datos, aun en dicho entorno personal, puede derivarse responsabilidad para el prestador del SRS conforme a otras normas, como las relativas a su condición de intermediario en la prestación de un servicio de la sociedad de la información.

Y, por supuesto, los usuarios particulares sí responderían, en su caso, por el uso de los datos de terceros conforme a cualquier otra disposición legal, singularmente (pero no solo), la de protección al derecho al honor, la intimidad personal o familiar e imagen, tanto en su perspectiva civil como penal, según sus respectivas reglas (de imputación, plazos, etc.).

3.2. El usuario profesional o corporativo

Establecida la excepción personal o doméstica, *a sensu contrario*, queda claro que todo usuario que no pueda beneficiarse de ella por utilizar el SRS para desarrollar actividades profesionales o comerciales queda incluido en la norma y, por lo tanto, puede ser considerado como «responsable del tratamiento» de los datos de terceros (otros usuarios particulares de la red) que maneje. Y ello, tanto bajo la directiva (y la LOPD) como en el RGPD, aunque con una diferencia muy importante entre la normativa antigua y la nueva: siendo también «responsable» el prestador del SRS, en el reglamento (art. 26) queda asentado, sin lugar a dudas, el carácter solidario de ambas responsabilidades concurrentes.

Para el GT29 (Dictamen 5/2009, pág. 6) «si un usuario de SRS actúa en nombre de una empresa o de una asociación o utiliza el SRS principalmente como una plataforma con fines comerciales, políticos o sociales, la exención no se aplica. En este caso, el usuario asume la plena responsabilidad de un responsable del tratamiento de datos que revela datos personales a otro responsable del tratamiento de datos (SRS) y a terceros (otros usuarios de SRS o incluso, potencialmente, a otros responsables del tratamiento de datos que tienen acceso a ellos)».

Por otra parte, el prestador del SRS es, en todo caso, «responsable», puesto que decide sobre el fichero (su misma creación), la finalidad de los datos recabados y su posible vinculación a actividades de este tipo. No hay problema en considerar la concurrencia de ambos sujetos como «responsables», pues la de-

finición del RGPD (art. 4.7, concordante con el art. 2.*d* de la directiva) señala que es «responsable del tratamiento» quien determina los fines y medios del tratamiento «solo o junto con otros».

La LOPD obvió esa mención a la decisión conjunta, aunque ha de llegarse a ella por el principio de interpretación conforme con la directiva. Además, al definir al «responsable del fichero o tratamiento», no queda claro si nuestra ley utiliza ambos como sinónimos o si pretende mantener una vieja distinción hecha en la LORTAD, como defienden la AEPD y la jurisprudencia. Si así fuera, y dado que tienen el mismo régimen de responsabilidades (civiles y administrativas, *ex* arts. 19 y 43 LOPD) a fecha de hoy, esa diferencia vendría a tener sentido, por ejemplo, en el ámbito que nos ocupa: el «responsable del fichero» sería el prestador del SRS, por lo que resultaría «responsable del tratamiento» el usuario profesional o corporativo que utiliza la red social, sus ficheros y medios, para sus actividades comerciales.

En todo caso, el Reglamento de desarrollo de la LOPD (art. 5.1.q) añadió a la definición de «responsable del fichero o del tratamiento» los elementos que le faltaban a la ley: «persona física o jurídica (...) que, solo o conjuntamente con otros, decida sobre la finalidad, el contenido y el uso del tratamiento, aunque no lo realice materialmente». De esta forma pretendía recoger la jurisprudencia sobre tal concepto, que muy claramente plasmaba, entre otras muchas, la SAN 16-X-2003 (RJCA 2004\271), que fue luego confirmada por la STS de 5 de junio de 2004 (RJ 2004\5849): «el responsable del fichero es quien decide la creación del fichero y su aplicación, y también su finalidad, contenido y uso, es decir, quien tiene capacidad de decisión sobre la totalidad de los datos registrados en dicho fichero. El responsable del tratamiento, sin embargo, es el sujeto al que cabe imputar las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica. Se trataría de todos aquellos *supuestos en los que el poder de decisión debe diferenciarse de la realización material de la actividad que integra el tratamiento*» (cursivas mías; véase también SSTS 28 de febrero de 2005, RJ 2005\1861 y 26 de abril de 2005, RJ 2005\3928; y SAN 15 de diciembre de 2005, JUR 2006\238282).

El *Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»* del GT29 (adoptado el 16 de febrero de 2010) propone el caso de las redes sociales entre sus ejemplos para la explicación del elemento «solo o conjuntamente con otros» que integra la definición de «responsable del tratamiento» (págs. 19-27, en particular, págs. 23-24). Puntualiza también que «conjuntamente» no significa que la intervención de los distintos responsables se haga en términos de igualdad y simultaneidad, sino que se pueden dar muchas formas y combinaciones. Por lo tanto, cabría delimitar ámbitos de actuación distintos, pues cada responsable, aun actuando conjuntamente, puede determinar fines propios y a alguno de ellos (en el caso que nos ocupa, al usuario profesional) le podría resultar muy difícil cumplir todas las obligaciones que la normativa imponga con carácter general. Tanto el propio fichero que contiene los datos de los usuarios como los medios técnicos se encuentran en poder del prestador del SRS que es quien, realmente, provee los instrumentos para realizar esa actividad comercial o de promoción (incluido el ejercicio de los derechos, como puede ser el de cancelación). En definitiva, y como concluye el propio GT29, en el ámbito de la Directiva (y, por lo tanto, de la LOPD) la concurrencia de responsables no debe implicar, a pesar de los términos normativos (que no distinguen entre ambos), idénticas obligaciones y responsabilidades solidarias (Dictamen 1/2010, pág. 25).

Otro posible caso que puede darse en el entorno de un SRS ocurre cuando una empresa usuaria del mismo contrata el servicio de publicidad de la red social (o de cualquier otra empresa de marketing fuera incluso de Internet), utilizando como destinatarios a los usuarios de esta, pero sin tener (la comitente) acceso a sus datos. Hablamos, por ejemplo,

de «contenidos patrocinados» o, en terminología del GT29 (*Dictamen 2/2010 sobre publicidad comportamental en línea*, adoptado el 22 de junio de 2010), de «comercialización contextual» (según los contenidos que se visiten), «segmentada» (según la pertenencia a un grupo o información comunicada previamente) o «de comportamiento» (en función del análisis de la actividad del usuario), según los casos. Dicha publicidad se inserta en el muro o *timeline* de los usuarios particulares a partir de las instrucciones dadas por la comitente, sin que esta llegue a tener materialmente ningún fichero de (potenciales) clientes.

Pero, nuevamente, el RGPD se aleja aquí de lo dispuesto en la normativa anterior, y su art. 26.3 sí reconoce, frente a los interesados, la solidaridad de todos los que sean responsables o «corresponsables» del tratamiento (pueden ejercer sus derechos «frente a, y en contra de, cada uno de los responsables», dice literalmente), sin perjuicio de que, entre ellos, delimiten sus responsabilidades de mutuo acuerdo y de forma transparente, y puedan incluso acordar sus funciones y relaciones respectivas frente a aquellos. En el marco de los SRS, básicamente, dicho acuerdo será la aceptación por parte de los usuarios profesionales de las condiciones impuestas por el prestador (véase, a título de ejemplo, las del servicio de Twitter Ads para Europa en <https://ads.twitter.com/terms/uk>).

En todo caso, *desde el punto de vista práctico*, frente al usuario-responsable, lo más eficaz es dirigirse, en el ejercicio de los derechos de oposición, rectificación o cancelación, a través de los propios mecanismos previstos por el SRS. De forma simultánea, o si esta petición no fuera atendida conforme a dichos mecanismos y plazos (pueden ser instantáneos y en ocasiones es tan sencillo como dejar de seguirlos o denunciar una publicidad concreta rechazando que vuelva a aparecer en su muro), los afectados podrían dirigirse al titular del SRS puesto que, según hemos visto, también es responsable. Al no darles satisfacción, se procedería después acudir a la AEPD en procedimiento de tutela de derechos o para el inicio de un expediente sancionador, o bien directamente ante los tribunales, frente a cualquiera de ellos o frente a ambos. No obstante, aun establecida esa solidaridad en su aplicación a las redes sociales, debe tenerse en cuenta que solo el proveedor de dicho SRS puede dar satisfacción real e inmediata en caso de producirse ineficiencias en la prestación del servicio, fallas en la información al suscribirlo o en la seguridad de los datos, mantenimiento de los mismos a pesar de su cancelación o fin de la prestación del servicio, falta de inscripción del fichero (en tanto sea obligatoria), filtraciones fuera de la red a pesar de la configuración de seguridad, etc. En casos como estos, la reclamación (al menos, de forma exclusiva) al usuario-responsable, salvo perfecto funcionamiento y sintonía en su relación interna con el prestador del SRS (de manera que sea este quien materialmente acabe dando solución), no permitirá la satisfacción del derecho del interesado.

Por supuesto, si el usuario profesional incorpora a sus propios sistemas los datos recabados (tiene acceso a ellos y los «saca» del SRS), sí resultará ser responsable «del tratamiento» en toda su extensión, con todas sus obligaciones. En la información facilitada debiera constar todo uso externo a la red social que vaya a realizarse con los datos recabados de la actividad de los seguidores (como figura en el citado *Informe 0241/2011* de la AEPD).

4. El consentimiento como legitimador del tratamiento de datos personales que se produce en las redes sociales

4.1. El consentimiento

Salvo ciertas excepciones, el tratamiento de datos personales en general, y en las redes sociales en particular, se basa en el consentimiento prestado por sus titulares. O, dicho de otra manera, el consentimiento legitima la mayoría de tratamientos de datos.

En la actualidad, estando vigente la LOPD, existen *otros criterios de legitimación del tratamiento*, tales como el ejercicio de las funciones propias de la administración, las relaciones negociales que lo justifican (sin dicho tratamiento es imposible llevarlas a cabo), el interés vital (servicios médicos) o su recogida de fuentes accesibles al público. Por lo que respecta a esta última excepción, sí cabe precisar que las redes sociales, a mi juicio, *no* son «fuentes de acceso público», en la misma línea de lo defendido por la AEPD en su Informe 0342/2008 (en referencia a Internet, en general) o la Resolución 007574/2005. Aunque, como la propia Internet, *contengan* medios de comunicación social (fuente de acceso público, *ex* art. 3.j LOPD), no creo (ni lo estimo conveniente) que las redes puedan ser calificadas, en sí mismas, de tales (en contra, Mª. R. García Sanz, 2011).

De esta manera, el hecho de que los usuarios dispongan de perfiles abiertos no supone una forma de consentimiento que faculte para recoger o tratar sus datos o, al menos, no lo supone *fuera* de dichas redes sociales (véase más adelante lo que se dirá sobre la STS 15 de febrero de 2017). Dentro de ellas, cada usuario en particular gestiona la posibilidad de compartir contenidos, citar a otras personas, etiquetarlas, etc., pues, incluso bajo la exigencia del consentimiento «afirmativo» del reglamento europeo, unido a la *privacy by default*, el propio usuario define (activamente, en el momento de la suscripción, o en cualquier otro posterior) lo que permite ver a los demás y que estos puedan o no compartir sus contenidos. En estos casos hay auténtico consentimiento a todos los efectos (además, revocable a través de las propias herramientas del SRS, que permiten el borrado del contenido o deshacer el etiquetado cuando se notifica), lo cual legitima incluso el uso de los datos personales por parte de los demás usuarios. A mayor abundamiento, nótese que tales usos hechos por otros usuarios de la red no constituyen «tratamientos» a los efectos del reglamento, como se ha explicado.

En el caso del reglamento europeo, no hay mención de las «fuentes de acceso público», pero puede suponer una importante brecha a la exigencia del consentimiento previo la licitud de los tratamientos cuando los responsables tengan un «interés legítimo», *ex* art. 6.1.f). Parece que ello hace perder control al titular sobre sus datos, por lo que habrá que ver cómo se interpreta dicho requisito (en particular, las autoridades de protección), teniendo en cuenta que supone un cambio radical en el paradigma de legitimación del tratamiento muy favorable a los responsables, dicho sea de paso. Esta legitimación ya no viene dada por la procedencia de los datos, sino por el carácter (lícito o no) de la recogida y el procesamiento de los mismos, de tal manera que, de concurrir dicha legitimidad, sería indiferente su procedencia.

Obsérvese que, en todo caso, los supuestos de tratamiento lícito al margen del consentimiento no lo excluyen de manera absoluta pues, una vez recabados los datos de fuentes accesibles al público, sus titulares pueden oponerse con posterioridad a dicho tratamiento (art. 6.4 LOPD) e, incluso, hay que informarles sobre la recogida de dichos datos (en particular, en el nuevo reglamento, art. 14). El considerando 47 pone como ejemplo el del contrato previo o la mercadotecnia (*in fine*), pero fuera de ello no da más que un criterio muy general: prevalece el interés del titular cuando este, a partir de las circunstancias concurrentes, no puede prever razonablemente un tratamiento ulterior. En las

redes sociales, los datos son recabados con fines publicitarios, entre otros, por lo que podría considerarse que hay incluso un interés legítimo al margen del consentimiento del titular, lo que permitiría, en apariencia, no recabarlo. No creo que sea una interpretación correcta, máxime cuando es sencillo informar al respecto, la mayoría de SRS lo hacen y, además, cabría oposición (art. 21.1, en relación con el art. 17.1.c).

La obligación de notificar sobre los fines del tratamiento y el hecho de que este haya de ser indispensable para tales fines son dos de los aspectos que son objeto de evaluación en el caso de la cesión de datos entre Whatsapp y Facebook, a raíz de la compra de aquella por esta en 2014. Los términos originales de Whatsapp no contemplaban la recogida de datos para su cesión a terceros con fines publicitarios sin la concreta autorización de los usuarios (a diferencia de Facebook, que lo incluye como cláusula genérica sobre la finalidad de uso de los datos que recoge), y la forma en que se recabó dicho consentimiento, una vez formalizada la compra y cambiadas las condiciones del servicio en 2016 (las nuevas incluyen expresiones como «las sugerencias de amigos serán mejores y verás publicidad relevante en Facebook»), es más que dudosa. En octubre de 2016, el GT29 envió una carta a Whataspp poniendo en cuestión la cesión de datos entre ambas compañías, aun siendo del mismo grupo. A este respecto, a finales de abril de 2017 un tribunal de Hamburgo ratificó la paralización de la cesión de datos entre ambas que había acordado la autoridad alemana (véase la noticia en La Vanguardia, <http://www.lavanguardia.com/vida/20170425/422046259543/tribunal-aleman-no-permite-a-facebook-acceder-a-los-datos-de-whatsapágs.html>).

En definitiva, por lo que respecta al control del titular de los datos, también (o «especialmente») en el marco de las redes sociales, su consentimiento ha de ser *libre*, *informado*, *inequívoco*, *revocable*, *expreso* en ciertos casos (como el de los datos sensibles) y, tras el nuevo reglamento europeo, *transparente*, *positivo* (art. 4.11 y Cdo. 32) y *verificable* (art. 7). Efectivamente, a diferencia de ciertas prácticas ahora toleradas, no cabe obtener el consentimiento del titular en base a su inacción o silencio, sino que se exigirá una declaración expresa o acción afirmativa por su parte, tras haber recibido la oportuna información. Ello implica un adiós a las casillas premarcadas («si no desea que sus datos sean tratados, desmarque esta casilla») como práctica extendida que existe actualmente. La verificabilidad, por su parte, obliga a quienes recojan los datos a tratar de demostrar que el titular consintió efectivamente.

Se ha extendido la costumbre, en el ámbito de las redes sociales y otros SSI, de exponer las condiciones del servicio en forma de preguntas y respuestas («Preguntas Frecuentes» o FAQ, *frequently asked questions*) o bien en lenguaje vulgar, sencillo y de fácil acceso para cualquier persona. Esta práctica está avalada por las propias autoridades de protección de datos, que la recogen entre sus prácticas recomendadas (así, la AEPD, la APDCat y la Agencia Vasca, en su *Guía para el cumplimiento del deber de informar* para el correcto cumplimiento del RGPD, de enero de 2017; accesible en <https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf>). Se insiste en una información por capas, facilitada en lenguaje claro, conciso, transparente, de fácil acceso, y evitando el «abuso de citas legales, "jerga" confusa, o términos ambiguos o con escaso sentido para las personas destinatarias». Un ejemplo de estas prácticas por una red social lo tenemos en la página <https://www.flickr.com/help/guidelines>, de Flickr, con remisión también a un listado FAQ y a la política de privacidad de Yahoo, redactada en este lenguaje «amigable»: <https://policies.yahoo.com/ie/es/yahoo/privacy/index.htm>.

Aunque pareciera que nada hay que objetar a tan encomiable esfuerzo divulgativo en aras de la transparencia informativa, sí conviene hacer una importante *precisión*: en todo caso, debiera facilitarse acceso al contrato de prestación del servicio en términos técnicos, en cumplimiento de la normativa sobre contratación a distancia (LSSI, TRLGDCU y LCG). Entre ambos (el contrato redactado en la «incomprensible» jerga jurídica y el presentado en forma «amigable») ha de haber una total correspondencia, sin que ninguno de ellos pueda encubrir u ocultar prácticas en perjuicio de los usuarios. De hecho, en caso de divergencia (y dijera lo que dijera el prestador), debieran aplicarse al usuario los términos que le fueran más favorables (aunque resultaran derivarse de una mala «explicación clara», pues toda oscuridad ha de imputarse al predisponente: arts. 1288 CC y 80.2 TRLGDCU). El prestador del SRS debe tener particular cuidado a la hora de actualizar las

distintas «versiones» de sus contratos y términos del servicio, así como las traducciones a los distintos idiomas, de manera que se mantengan sincronizadas.

Téngase en cuenta, además, que el consentimiento dado lo es no solo a los efectos de la protección de datos, sino también del ejercicio de otros derechos de la personalidad, como los de intimidad o imagen e, incluso, de derechos de propiedad intelectual (supone, cuando se comparten obras propias, el ejercicio del derecho de comunicación pública, art. 20.2.i TRLPI).

En todo caso, el ámbito de dicho consentimiento queda limitado a la propia red social, como se pone de manifiesto (al menos, para los derechos de la personalidad y los datos personales, pero entiendo que también para el resto, pues la declaración de voluntad se da en el marco del SRS y a los solos efectos de su prestación) en la STS 15 de febrero de 2017 (RJ 2017\302) sobre el caso de un periódico que publicó la foto del perfil de Facebook de un hombre para ilustrar la noticia de un delito del que había sido víctima. Al respecto, señala el alto tribunal (FD 5.3) que el hecho de haber subido una fotografía propia a una red social y que, como consecuencia de ello, dicha foto «sea accesible al público en general, no autoriza a un tercero a reproducirla en un medio de comunicación sin el consentimiento del titular, porque tal actuación no puede considerarse una consecuencia natural del carácter accesible de los datos e imágenes en un perfil público de una red social en Internet. *La finalidad de una cuenta abierta en una red social en Internet es la comunicación de su titular con terceros y la posibilidad de que esos terceros puedan tener acceso al contenido de esa cuenta e interactuar con su titular, pero no que pueda publicarse la imagen del titular de la cuenta en un medio de comunicación*». El tribunal condenó al periódico al pago de 15.000 € de indemnización por intromisión ilegítima en la imagen del demandante, aunque consideró que no había habido intromisión en su intimidad por la publicación de otros datos que permitían su identificación, al ser hechos graves y noticiables, acomodándose la noticia a los cánones de este tipo de informaciones.

Para el TS (cursivas mías), FD. 5.3, «aunque este precepto legal [se refiere al art. 2.2 LO 1/1982], en la interpretación dada por la jurisprudencia, no requiere que sea un consentimiento formal (por ejemplo, dado por escrito), sí exige que se trate de un consentimiento inequívoco, como el que se deduce de actos o conductas de inequívoca significación, no ambiguas ni dudosas.

Esta sala ha declarado en reiteradas ocasiones (sentencias 1225/2003, de 24 de diciembre, 1024/2004, de 18 de octubre, 1184/2008, de 3 de diciembre, 311/2010, de 2 de junio) que *el consentimiento dado para publicar una imagen con una finalidad determinada (en este caso, como imagen del perfil de Facebook) no legitima su publicación con otra finalidad distinta (en este caso, ilustrar gráficamente el reportaje sobre el suceso violento en que se vio envuelto el demandante)*. En la sentencia 746/2016, de 21 de diciembre, afirmamos que aunque hubiera sido cierto que la fotografía publicada por el medio de información hubiera sido 'subida' a Facebook por la persona que en ella aparece, "[…] esto no equivaldría a un consentimiento que […] tiene que ser expreso y, además, revocable en cualquier momento".»

FD 5.5.: «Que el titular de una cuenta en una red social en Internet permita el libre acceso a la misma y, de este modo, que cualquier internauta pueda ver las fotografías que se incluyen en esa cuenta, no constituye, a efectos del art. 2.1 de la Ley orgánica 1/1982, un "acto propio" del titular del derecho a la propia imagen que excluya del ámbito protegido por tal derecho la publicación de la fotografía en un medio de comunicación. *Tener una cuenta o un perfil en una red social en Internet, en la que cualquier persona puede acceder*

a la fotografía del titular de esa cuenta, supone que el acceso a esa fotografía por parte de terceros es lícito, pues está autorizada por el titular de la imagen. Supone incluso que el titular de la cuenta no puede formular reclamación contra la empresa que presta los servicios de la plataforma electrónica donde opera la red social porque un tercero haya accedido a esa fotografía cuyo acceso, valga la redundancia, era público. Pero no supone que quede excluida del ámbito protegido por el derecho a la propia imagen la facultad de impedir la publicación de su imagen por parte de terceros, que siguen necesitando del consentimiento expreso del titular para poder publicar su imagen.»

4.2. El consentimiento de los menores y el control parental

El otro gran problema del consentimiento es su prestación por parte de los menores. Ciertamente, en relación con las redes generalistas y de suscripción «gratuita», parece que no hay duda de que pueden crear sus propios perfiles, al tratarse de «servicios de la vida corriente propios de su edad de conformidad con los usos sociales» (art. 1263 CC). La creciente autonomía del menor conforme va cumpliendo años parece que, hoy en día, incluye la posibilidad de celebrar este tipo de contratos, máxime cuando igualmente se reconoce no solo la titularidad de los derechos a su honor, intimidad, imagen y expresión, sino su propio ejercicio conforme a sus condiciones de madurez (así, arts. 3.1 LO 1/1982, 2, 4 y 8 LOPJM), debiendo interpretarse restrictivamente toda limitación de su capacidad de obrar (art. 2.1, 2º LOPJM).

Lo mismo sucede con la protección de datos, en la que, a pesar del silencio de la LOPD (un defecto no menor de la misma), el art. 13 de su reglamento de desarrollo establece la edad de 14 años como aquella a partir de la cual el menor puede disponer de sus propios datos personales (pero no de los de otros miembros de su familia). El RGPD europeo señala que solo a partir de los 16 años pueden los menores dar consentimiento válido para el tratamiento de sus datos en relación con servicios de la sociedad de la información. No obstante, dicha edad puede ser rebajada por los legisladores nacionales (lo cual rompe el principio de unidad del reglamento) hasta los 13 años. La normativa vigente en España, además de ser más general (se refiere al ejercicio por el menor de su derecho sobre sus datos personales en cualquier ámbito, no solo en relación con los SSI), supone, en su estado actual, un desarrollo concreto de esta posibilidad que ofrece el legislador europeo, reduciendo la edad a los 14 años. Más allá de lo inapropiado de que sea establecida en una simple norma reglamentaria de desarrollo, en la actualidad puede ser una edad razonable para que el menor empiece a ejercitar sus derechos con una cierta autonomía, y es considerada como edad mínima para acceder a muchas redes sociales sin necesidad de consentimiento paterno.

En consecuencia, está claro que cualquier menor mayor de 14 años, aun no estando emancipado (en la actualidad la edad de emancipación son los 16 años cumplidos), puede apuntarse por sí mismo a una red social (al menos, a la mayoría, puesto que no podría cuando el prestador exija una edad superior o se dirija exclusivamente a adultos, como Badoo) y operar en ella disponiendo de sus propios datos personales (y exclusivamente de ellos, lo que supone una cierta limitación cuando tales datos sean, además, personales de otros miembros de su familia, tales como la indicación de su domicilio). La exigen-

cia de verificabilidad, no obstante, impone al prestador del SRS la obligación de comprobar de alguna manera «razonable» (por utilizar la terminología del reglamento europeo), «teniendo en cuenta la tecnología disponible», que el consentimiento es prestado por alguien con edad suficiente o, si no la tiene aún, que lo hace con autorización del titular de la patria potestad (o por este en su lugar). Las consecuencias de no hacerlo recaerán sobre el responsable, que sufrirá igualmente la posibilidad de que los representantes soliciten la nulidad del contrato por falta de capacidad del menor.

Sin embargo, siendo así las cosas, ¿pueden los padres (o tutores) controlar el uso que los menores hacen de las redes sociales? En este ámbito no hay ninguna norma especial más allá de las generales sobre el ejercicio de la patria potestad (o tutela), que siempre ha de hacerse en beneficio del menor. La labor de los padres como representantes de los hijos, en ejercicio de la patria potestad (auténtica «función» o «responsabilidad parental», en terminología que ya encuentra reflejo incluso en el Código Civil y que apunta no tanto a la parte de «derecho» cuanto de «deber» para con la prole) ha de acomodarse siempre a la personalidad y madurez de sus hijos, y con respeto a sus derechos (art. 154 CC).

Sobre la tensión entre los derechos del menor y la función de los padres, ya ha tenido ocasión de pronunciarse el Tribunal Supremo (Sala de lo Penal), en sentencia del 10 de diciembre de 2015 (RJ 2015\6401). En este caso se dio validez a las pruebas obtenidas por la madre, que entró en la cuenta de Facebook de su hija sin el permiso previo de esta (no se explica cómo consiguió la contraseña, pero de los hechos se deduce la anuencia *ex post* de la hija), cuando existía una fundada sospecha («signos claros», dice el TS) de que estaba siendo víctima de un acoso sexual a través de la red. El derecho del menor a su privacidad existe (expresamente, como he dicho, en el art. 4 LOPJM), incluso frente a sus padres, pero tiene límites en la propia función tuitiva sobre el menor. Acota el tribunal que «no puede el ordenamiento hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de controlar en casos como el presente, en el que las evidencias apuntaban inequívocamente en esa dirección. La inhibición de la madre ante hechos de esa naturaleza, contrariaría los deberes que le asigna la legislación civil». Aun con todos los matices que hace el TS en el caso (se trataba de un delito vivo, no agotado), es posible defender, por lo tanto, que en casos claros de atentado al menor, el deber paterno es actuar para evitarle un mal grave, aunque sea «lesionando» su derecho a la privacidad, que tiene incluso frente a sus padres, según sus condiciones de madurez.

Si la necesidad de control surge en el centro educativo, la Audiencia Nacional (sentencia de 26 de septiembre de 2013) ha estimado correcto que el director del mismo, con asistencia del fefe de estudios, solicite del menor (en ese caso, con 12 años) la clave de acceso al móvil cuando hay fundadas sospechas de que, a través del mismo, se estaban intercambiando fotos comprometidas de otros menores, sin necesidad del consentimiento paterno (en el supuesto juzgado, fueron los padres del menor dueño del móvil los que denunciaron al colegio). Para la AN, el derecho a la protección de datos encuentra en

este punto su límite en la misión de interés público que el centro tiene asignada y para la cual ha de proteger también los derechos de los demás menores.

Cuando hayan de intervenir, *ambos* titulares de la patria potestad deberán tomar las decisiones sobre lo que el menor haga, comparta o siga en las redes sociales, como en cualquier otro ámbito. En caso de que hubiera desacuerdo entre ellos, no es la autoridad de protección de datos, sino los órganos judiciales quienes tendrían que determinar a quién de ellos corresponde la capacidad de decisión (véase R/00686/2015 de la AEPD; art. 156 CC).

5. Breve apunte sobre la responsabilidad del prestador del SRS por las conductas ilícitas de sus usuarios

Un usuario puede cometer diversos ilícitos en el marco de su utilización de la red social. En este caso, y más allá de la propia responsabilidad del usuario conforme a la normativa aplicable (aunque no proceda como responsable del tratamiento de datos personales, sí puede derivarse para él en virtud de otros derechos lesionados cuando, por ejemplo, difunde, sea de forma originaria o al compartir, informaciones reservadas a la intimidad, injurias, contenidos protegidos por la propiedad intelectual, etc.), nos interesa ahora la del propio prestador en tales casos, como intermediario en la prestación de un SSI (Directiva 2000/31 y LSSI).

Como se ha comentado anteriormente, el prestador de un SRS puede operar, de forma simultánea, como prestador de servicios y contenidos o como simple intermediario, en particular, de espacio (alojamiento o *hosting*) y de enlaces (buscador). Como intermediario, pone los medios para la relación entre las personas, por lo que podría dudarse de su responsabilidad por el uso que sus usuarios hagan de la plataforma.

Pero, sin entrar en mayores consideraciones, ha de afirmarse dicha responsabilidad incluso en estos casos, pues así lo recoge, con carácter general y horizontal, la propia LSSI en sus arts. 16 y 17, incluso tras asegurar que no existe ninguna obligación de supervisión o control de las informaciones o de los datos (entendidos aquí en sentido puramente informático) que manejan (art. 15 Directiva 2000/31), ni ninguna presunción de conocimiento de su carácter lícito o ilícito. Los citados arts. 16 y 17, aplicables a proveedores de alojamiento y enlaces, recogen normas imperativas que marcan, según sean leídos, criterios de imputación o (quizá mejor) de exención de responsabilidad, frente a los que no cabe exoneración ninguna, a pesar de los términos de los contratos de suscripción (las cláusulas al respecto son nulas), establecidos sobre la base de una pretendida gratuidad del servicio (y, como tal, los contratos gratuitos las permitirían, aunque no lo son propiamente, como se ha venido afirmando).

> Las condiciones de suscripción del servicio pretenden, entre otros fines, las mayores exenciones posibles de responsabilidad para el prestador. Más allá del respeto a la normativa de protección de datos, queda claro su interés en recabar el consentimiento de sus usuarios a tales otros efectos.

En el marco de los servicios de alojamiento o enlace prestados por un prestador de SRS en el ámbito de su actividad, dicho prestador podrá alegar como causas de exoneración de su responsabilidad:

1) la ausencia de «conocimiento efectivo» por su parte sobre el carácter ilícito de los contenidos suministrados por su usuario, o

2) en su defecto (esto es, conociendo dicho carácter), la retirada diligente de los mismos, o haber hecho imposible su acceso.

Obsérvese que la responsabilidad del intermediario no deriva, en puridad, de la responsabilidad de su usuario (no es una responsabilidad por hecho ajeno), sino de su propia actuación ante la constatación del ilícito que dicho usuario ha cometido (responsabilidad por hechos propios).

Para evitar responsabilidades (lo que, a la vez, sirve para determinar la existencia de conocimiento efectivo tal cual es interpretado por la jurisprudencia, y también a los efectos de los procedimientos de conocimiento que contemplan ambos artículos) los prestadores de SRS han ido incorporando botones o funcionalidades de «denuncia». Utilizados por un usuario-afectado, y si se sigue de forma evidente la ilicitud del contenido, su no retirada por el prestador será determinante de su responsabilidad (al menos, civil), con independencia de la del usuario-infractor en cuestión.

En el marco del ejercicio de acciones civiles de responsabilidad («acción por daños y perjuicios», en la terminología de la directiva), en el art. 14.1.a) el conocimiento no se refiere a la *ilicitud* de la actividad (aunque en verdad lo sea, como hace inmediatamente antes para las acciones penales, por ejemplo), sino a *hechos o circunstancias que revelen ese carácter*. Es obvio que la diferente expresión revela una exigencia menor en el conocimiento requerido, el cual puede deducir el propio PSI de los hechos o circunstancias que rodean la actividad o información, como la denuncia de un afectado sumada al contenido de la información. El art. 16 LSSI (y, en su consecuencia, el 17, que lo copia) olvidó esa diferencia de trato que hace la directiva, lo que ocasionó líneas jurisprudenciales contrarias al exigir una de ellas que en toda reclamación frente a un intermediario pudiera acreditarse la previa declaración judicial de ilicitud. A partir de la STS de 9 de diciembre de 2009 (RJ 2010\131), el TS es constante en su interpretación de tales preceptos conforme a la norma comunitaria y no exige, en el ámbito de acciones civiles de reclamación de daños y perjuicios (y cese de la conducta), más que la concurrencia de «hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate» (véase, entre otras, SSTS de 18 de mayo 2010, RJ 2010\2319; 10 de febrero de 2011, RJ 2011\313; y 7 de enero de 2014, RJ 2014\773).

En base a todo ello, por lo tanto, podríamos demandar (civilmente) a una red social por la no retirada de comentarios que estimamos injuriosos o de un contenido (o enlaces al mismo) sobre el que tenemos los correspondientes derechos de propiedad intelectual.

En cuanto al incumplimiento de las condiciones del servicio (incumplimiento contractual), el prestador podría suspender o excluir del mismo al infractor (resolución del contrato), posibilidad contemplada expresamente en todos los clausulados generales de acceso. Terminado así el servicio, y con independencia de cómo afecte ello a los contenidos de dicho usuario en la red, por lo que a sus datos personales respecta procedería su cancelación o anonimización (arts. 4.5 LOPD y 5.1.e y 89.1 RGPD).

Bibliografía

Aparicio Vaquero, J. P. (2015). «Cuestiones de derecho aplicable y responsabilidad de los prestadores de servicios de red social y de sus usuarios». En: Aparicio Vaquero, J. P. y Batuecas Caletrío, A. (coords.). *En torno a la privacidad y la protección de datos en la sociedad de la información* (págs. 187-231). Granada: Comares.

Batuecas Caletrío, A. (2015). «El control de los padres sobre el uso que sus hijos hacen de las redes sociales». En: En: Aparicio Vaquero, J. P. y Batuecas Caletrío, A. (coords.). *En torno a la privacidad y la protección de datos en la sociedad de la información* (págs. 137-170). Granada: Comares.

Campuzano Tomé, H. (2011). «Marco regulador de la protección de datos de carácter personal en las redes sociales digitales». *Actualidad Civil* (n.º 6, págs. 623-653).

García Sanz, R. Mª. (2011). «Redes sociales *online*: fuentes de acceso público o ficheros de datos personales privados (aplicación de las directivas de protección de datos y privacidad en las comunicaciones electrónicas)». *Revista de Derecho Político* (n.º 81, págs. 101-154). UNED.

Gil Membrado, C. (2015). «El consentimiento en las redes sociales». En: En: Aparicio Vaquero, J. P. y Batuecas Caletrío, A. (coords.). *En torno a la privacidad y la protección de datos en la sociedad de la información* (págs. 105-136). Granada: Comares.

Grimalt Servera, P. (1999). *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada: Comares.

Guerrero Picó, Mª. C. (2006). *El impacto de Internet en el derecho fundamental a la protección de datos de carácter personal*. Madrid: Thomson Civitas.

Orenes Ruiz, J. C. (2014). «La responsabilidad de los medios digitales. A propósito de la sentencia Delfi contra Estonia». *Actualidad Jurídica Aranzadi* (n.º 877, págs. 2-3).

Paniza Fullana, A. (2010). «El alcance de la responsabilidad de los prestadores de servicios de la sociedad de la información (a propósito de la sentencia del Tribunal Supremo de 18 de mayo de 2010)». *Aranzadi Civil* (n.º 4, págs. 27-36).

Peguera Poch, M. (2007). *La exclusión de responsabilidad de los intermediarios en Internet*. Granada: Comares.

Rallo Lombarte, A.; Martínez Martínez, R. (eds.) (2013). *Derecho y Redes Sociales* (2ª ed.). Madrid: Civitas.

Rallo, A.; Martínez, R. (2011). «Protección de datos personales y redes sociales: obligaciones para los medios de comunicación». *Quaderns del CAC* (37, vol. XIV (2), págs. 41-51).

Rodríguez de las Heras Ballell, T. (2010). «Intermediación en la red y responsabilidad civil. Sobre la aplicación de las reglas generales de la responsabilidad a las actividades de intermediación en la red». En: AA. VV. *I Congreso sobre las Nuevas Tecnologías y sus repercusiones en el seguro: Internet, biotecnología y nanotecnología* (págs. 13-50). Madrid: Fundación Mapfre.

Roig, A. (2009). «E-privacidad y redes sociales». *IDP (Revista de Internet, Derecho y Política)* (n.º 9, págs. 42-52).

Rubí Puig, A. (2010). «Derecho al honor *on line* y responsabilidad civil de ISP. El requisito del "conocimiento efectivo" en las SSTS, Sala Primera, de 9 de diciembre de 2009 y 18 de mayo de 2010». *InDret*, 4/2010 (disponible en <http://www.indret.com/pdf/776_es.pdf>, consultado el 1 de mayo de 2017).

Sempere, F. J. (2015). «Normas aplicables al uso de WhatsApp por las Administraciones». *Privacidad Lógica* (blog), disponible en <http://www.privacidadlogica.es/2015/05/21/normas-aplicables-al-uso-de-whatsapp-por-las-administraciones/>, consultado el 1 de mayo de 2017.

Troncoso Reigada, A. (2012a). «La protección de los datos personales en las redes sociales virtuales». En: Bauzá Reilly, M. y Bueno de Mata, F. (coords.). *El Derecho en la sociedad telemática* (págs. 231-269). Santiago de Compostela: Andavira.

Troncoso Reigada, A. (2012b). «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales» (parte una). *IDP* (n.º 15, págs. 61-75).

Troncoso Reigada, A. (2013). «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales» (parte dos). *IDP* (n.º 16, págs. 27-39).