ISSN (electrónico): 2014-2242 / www.cac.cat

QUADERNS DEL CAC

Protección de datos personales y redes sociales: obligaciones para los medios de comunicación

Artemi Rallo

Catedrático de derecho constitucional de la Universitat Jaume I y ex director de la Agencia Española de Protección de Datos (2007-2011)

rallo@dpu.uji.es

Ricard Martinez

Profesor de derecho constitucional de la Universitat de València. Ex coordinador del Área de Estudios de la Agencia Española de Protección de Datos (2007–2011)

martiner@uv.es

Resumen

Las redes sociales presentan un nuevo escenario para la participación ciudadana y para la definición de un nuevo modelo de relación entre ciudadanos y medios de comunicación, pero para operar en este medio resulta fundamental tener en cuenta las normas vigentes en materia de protección de datos. Este artículo explora tanto los principios básicos que rigen en esta materia para los medios de comunicación y para los usuarios de sus espacios en redes sociales como los conflictos que puedan derivar de un ejercicio inadecuado de su libertad de expresión.

Palabras clave

Redes sociales, privacidad, protección de datos personales, libertad de expresión, derecho a la información.

Abstract

Social networks present a new scenario for citizen engagement and for defining a new model of the citizen-media relationship but, in order to operate in this medium, it's essential to take into consideration the data protection regulations in force. This article explores both the basic principles governing this area for the media and for social network users, as well as the conflicts that may arise from inadequately exercising free speech

Keywords

Social networks, privacy, data protection, free speech, right to information.

1. Los medios en las redes sociales

Las redes sociales[1] constituyen, probablemente, la mayor novedad del último decenio para los medios de comunicación, ya que los proveen de una interactividad insospechada hasta hace muy poco tiempo. Tradicionalmente era la radio el medio que con regularidad podía abrir sus micrófonos en tiempo real para los oyentes. Sin embargo, ello dependía de la disponibilidad de tiempo en la parrilla y de la naturaleza del programa. Hoy, cualquier medio de comunicación que se precie ha desembarcado en una red social, ya sea como corporación, ya sea mediante el recurso a abrir sus programas más significados a la interacción con el usuario.

Por este procedimiento, las posibilidades de dar protagonismo al seguidor se multiplican y van desde la conversación en tiempo real a la provocación. La interacción en la red social permite así integrar a la persona usuaria en la dinámica del programa, fidelizarla, pulsar el estado de opinión en tiempo real y, dada la capilaridad de estos medios, multiplicar el impacto de cada emisión.

Al fenómeno de las redes sociales debe añadirse el impacto de la llamada *blogosfera*, que, de hecho, fue previa en el tiempo.[2] Ha nacido un periodismo ciudadano de opinión –no siempre riguroso– y los medios tradicionales se han apresurado a incorporar a sus espacios en internet un espacio de blogs, ya sea conducidos por sus profesionales, ya sea abierto a los ciudadanos.

En este contexto se plantean, al menos, dos interrogantes desde un punto de vista jurídico. Qué requisitos normativos se imponen a las empresas de comunicación que deciden desembarcar en una red social –aquí nos ocuparemos esencialmente del derecho fundamental a la protección de datos–. Y, en segundo lugar, cómo se articularán los conflictos relacionados con la publicación de información u opinión por los propios usuarios.

2. Protección de datos en las redes sociales

Para la aplicación de las normas sobre protección de datos personales es fundamental un entendimiento claro del contexto.

Como en su día apuntó Castells,[3] la evolución de la red favorece la generación de comunidades, tanto por medio del traslado de grupos sociales preexistentes al mundo virtual, como mediante la creación de grupos de interés de ámbito global. Además, gran parte de los servicios vinculados a la misma se orientan al ocio y a fomentar aspectos directamente relacionados con la vida personal o privada, como compartir fotografías, escuchar música o compartir video, o expresar opinión mediante breves píldoras de 140 caracteres.[4]

A ello deben unirse un conjunto de elementos de carácter técnico cuya influencia futura es a día de hoy impredecible. En primer lugar, la ubicuidad es una de las características más destacadas en los servicios de internet. El teléfono móvil[5] se convierte en un completo gestor y organizador con funciones que van desde la agenda personal a la gestión domótica en la llamada "internet de las cosas"[6] pasando por la adopción de decisiones basadas en servicios de valor añadido, como la geolocalización. El teléfono es ahora un espacio de ocio y juego compartido, una herramienta de acceso a redes sociales o un proveedor de acceso a servicios de televisión digital interactiva.[7]

Por otra parte, también desde el punto de vista tecnológico, el universo web deja de ser un lugar pasivo para convertirse en un espacio social muy dinámico. La persona usuaria puede expresar su opinión, obtener opiniones de terceros, mostrarse a si mismo. Es un entorno complejo en el que las aplicaciones no son siempre del proveedor principal[8] y los usuarios pueden ser a la vez *betatesters* y desarrolladores.

Por lo tanto, la Web 2.0 va mucho más allá. No se trata únicamente de un conjunto de recursos más o menos avanzados de software. Comporta el nacimiento de un universo social propio de la sociedad red, poblado de comunidades que pueden ir de lo más cercano –el grupo inmediato de amigos–, a cualquier tipo de agrupación horizontal –grupos profesionales o sociales–, vertical –espacios de trabajo en grupo– e incluso "informal", sin límites de espacio o tiempo. Probablemente por ello se afirma que la Web 2.0 "es una actitud y no precisamente una tecnología".[9]

2.1 La identidad es el elemento nuclear

En la sociedad de la información la moneda de cambio no puede ser otra que la información personal.[10] Como es sabido, al navegar el internauta deja un rastro económicamente rentable. Gracias a las rutinas de funcionamiento de internet, el rastreo de las IP, la información básica sobre las aplicaciones instaladas en nuestro ordenador, las *cookies* o los *log* de navegación, se generan perfiles de uso aprovechables con la finalidad de establecer perfiles genéricos de navegación con un determinado valor de mercado.[11]

Seguir el rastro de una navegación, incluso sin identificar de modo concreto al internauta, aporta información extraordinariamente valiosa si se contextualiza. La persona usuaria, de manera inconsciente, revela preferencias de toda clase, indica qué asuntos le interesan, qué gráficos le atraen o qué publicación prefiere. Estas huellas electrónicas aprovechan para facilitar la navegación y hacerla más rápida, para presentar la publicidad de una determinada manera y hacer estudios de mercado, o para ofrecer al cliente que se ha identificado servicios personalizados adaptados a su navegación por la web.

Si desde este punto de vista de su funcionamiento básico y "tradicional", internet presentaba un reto para la protección de la vida privada, mayor complejidad reviste en las redes sociales, donde ya no bastan los perfiles genéricos de una persona usuaria ni las identidades ficticias. Para ser eficaz en una red social, para conseguir sus objetivos, el individuo se identifica. Y en este contexto la identidad posee un valor extraordinario, porque gracias a ella la información, el mensaje o la publicidad son personalizados. Se tendrá la capacidad de establecer o identificar círculos de confianza[12] y gracias a ello la viralidad de los mensajes multiplica la eficiencia y la eficacia de los tratamientos.

En ningún caso debe ponerse en duda la contribución de las redes sociales al debate público; los recientes ejemplos de democratización en países del norte de África constituye una prueba evidente. Ello no significa que la actuación de los proveedores y de los propios usuarios no esté sometida a reglas.[13]

Por ello, la primera cuestión que debemos plantearnos es si existen principios aplicables a Internet, y en particular a las redes sociales. Y la respuesta no puede ser sino afirmativa. Por tanto, la cuestión en sus aspectos nucleares no estriba tanto en determinar si existen o no principios básicos aplicables, que evidentemente existen, sino si realmente se tienen en cuenta desde el diseño inicial de las aplicaciones.[14]

2.2 La aplicación de normas sobre protección de datos personales

Los tratamientos de información personal constituyen el elemento nuclear de las redes sociales. Y ello es así tanto desde la perspectiva de los proveedores de servicios, cuyo negocio se basa precisamente en los beneficios que produce la explotación de esta información, como desde la de los usuarios, que exponen su información y se exponen con ella personal y profesionalmente. Por ello, el derecho por excelencia en este contexto no podría ser otro que el derecho a la protección de datos.

2.2.1 El estándar Lindqvist

Sin ningún género de dudas, el caso Bodil Lindqvist constituye una referencia de primer orden cuando se trata de establecer criterio para aplicar las normas sobre protección de datos en las redes sociales.[15] En este sentido, puede decirse que el Tribunal de Justicia ha definido con claridad los criterios a seguir ante un tratamiento de datos personales en una página web.

Es importante tener en cuenta que la conducta consistente en publicar una foto, un video o un texto escrito en una red social no difiere en términos materiales en absoluto del caso Lindqvist: es exactamente la misma situación. Simplemente, la tecnología ha avanzado y permite hacerlo sin conocimientos técnicos previos y en un entorno cooperativo. En Lindqvist, el Tribunal de Justicia concluyó que se daban las condiciones para aplicar la Directiva 95/46/CE. A saber:

1. Que existía tratamiento

"27. Por tanto, procede responder a la primera cuestión que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46".

Para ello, aludió a las categorías de tratamiento que –debe subrayarse– incluyen la comunicación por transmisión y la difusión, conceptos incardinables en el de cesión.

"25. En cuanto al concepto de "tratamiento" de dichos datos que utiliza el artículo 3, apartado 1, de la Directiva 95/46, éste comprende, con arreglo a la definición del artículo 2, letra b), de dicha Directiva, "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales". Esta última disposición enumera varios ejemplos de tales operaciones, entre las que figura la comunicación por transmisión, la difusión o cualquier otra forma que facilite el acceso a los datos. De ello se deriva que la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole".

2. Que no resultaba aplicable la excepción de vida privada[16]

"47. En consecuencia, esta excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares; evidentemente, no es éste el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas".

3. Que el conflicto entre el derecho a la protección de datos y la libertad de expresión o el derecho a la información debe ser resuelto por la autoridad o el juez nacional competente

"90. Por tanto, procede responder a la sexta cuestión que las disposiciones de la Directiva 95/46 no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión o a otros derechos y libertades vigentes en la Unión Europea y que tienen su equivalente, entre otros, en el artículo 10 del CEDH. Incumbe a las autoridades y a los órganos jurisdiccionales nacionales encargados de aplicar la normativa nacional que adapta el Derecho interno a la Directiva 95/46 garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario".

Por tanto, si aplicamos literalmente las conclusiones de este caso a una opinión en el "muro" de una red social es evidente que, bajo ciertas condiciones, existirá un tratamiento sujeto a la Directiva. Y lo mismo sucederá si se etiqueta una fotografía o se publica un vídeo que concierna a personas identificadas o identificables.

En la práctica, como veremos a continuación, la excepción de *vida privada* únicamente será aplicable cuando el espacio en la red social se configure de un modo tal que sólo sea visible a un grupo de amigos expresamente autorizado. De lo contrario, se daría plenamente el supuesto de Lindqvist.

2.2.2 La opinión del Grupo de trabajo del artículo 29

En el Dictamen 5/2009 sobre las redes sociales en línea,[17] el Grupo de trabajo establece las condiciones de aplicación de la Directiva 95/46/CE[18] partiendo de la consideración de que, en "sentido jurídico, las redes sociales son servicios de la sociedad de la información". Es evidente que para el funcionamiento de este tipo de servicios resulta necesario tratar datos personales primero en el registro y para la configuración del perfil de la persona usuaria. Por otra parte, y puesto que el objetivo final de una red social es interactuar con otros usuarios, cada uno de ellos aporta información en forma de descripciones, opiniones, fotografías etc., y la red social les provee de herramientas –listas de usuarios, mensajería privada, correo electrónico etc.– que la facilitan y para las que se requiere desarrollar algún tipo de tratamiento.

Desde este punto de vista, no existe duda alguna respecto a la aplicabilidad de la Directiva. De ahí que el Grupo de trabajo centre sus esfuerzos en desmenuzar cada uno de los elementos de tales tratamientos. En esta línea, hay un aspecto que no ofrece dudas: "las disposiciones de la Directiva relativa a la protección de datos se aplican en la mayoría de los casos a los proveedores de SRS (servicios de red social), aunque su sede se encuentre fuera del EEE".[19] No obstante, la complejidad de este tipo de servicios obliga a fijar criterios que identifiquen otros posibles responsables. Lo serán los proveedores externos de aplicaciones cuando traten datos y también podrían serlo los propios usuarios bajo ciertas condiciones:

- Cuando la red social se utiliza como una plataforma de colaboración para una asociación o una empresa.
- En segundo lugar, según el Grupo, "cuando el acceso a la información del perfil va más allá de los contactos elegidos, en particular, cuando todos los miembros que pertenecen al SRS pueden acceder a un perfil o cuando los datos son indexables por los motores de búsqueda, el acceso sobrepasa el ámbito personal o doméstico. Del mismo modo, si un usuario decide, con perfecto conocimiento de causa, ampliar el acceso más allá de los "amigos" elegidos, asume las responsabilidades de un responsable del tratamiento de datos. En la práctica, se aplica entonces el mismo régimen jurídico que cuando una persona utiliza otras plataformas tecnológicas para publicar datos personales en Internet".
- Por último, se plantea no aplicar la excepción doméstica cuando se traten datos de terceros sin su conocimiento y/o consentimiento, particularmente cuando se trate de datos especialmente protegidos.

Finalmente, el Grupo de trabajo recuerda que puede haber casos en los que la exención doméstica no se aplique, pero prevalezcan derechos como la libertad de expresión, el derecho a la información o las libertades de creación artística o literaria. Del mismo modo, tampoco excluye la aplicación de las disposiciones generales del derecho civil o penal nacional.

2.2.3 Aportaciones de la Agencia Española de Protección de Datos

La autoridad española ha desarrollado diversas acciones en este ámbito promocionando y participando en estudios,[20] emitiendo informes o actuando en aplicación del régimen sancionador. Deben destacarse aquellos documentos que de algún modo contribuyen a definir una posición de la institución en esta materia. En este sentido, deben leerse atentamente las *Recomendaciones a usuarios de Internet 2009*. Este documento apunta un interesante cambio de óptica. En ediciones anteriores se concebía a la persona usuaria como un sujeto pasivo cuyos datos eran objeto de tratamiento. Sin embargo, las recomendaciones contenidas en los puntos X y XI del documento apuntan un nuevo enfoque. En primer lugar, se parte de la base que un uso normal de los recursos de la Web 2.0 puede determinar tratamientos de datos e imágenes de personas que no los han consentido y recomienda poner un especial cuidado.[21]

Por otra parte, el documento considera también a los internautas que conscientemente utilizan los recursos de la Web 2.0 con fines informativos, y a este respecto las *Recomendaciones* del epígrafe duodécimo son muy concretas y apuntan claramente en la línea de concienciar a la persona usuaria sobre las condiciones de ejercicio del derecho a la información en internet.[22]

Además de esta actividad promocional, la Agencia ha adoptado decisiones con trascendencia jurídica en la medida en la que sus informes y resoluciones sirven para orientar la actuación de los prestadores. Así, se ha emitido un informe sobre esta materia, el 615/2008,[23] relativo a algo tan común como "la actuación de unos particulares que comparten, utilizando para ello sus páginas web, fotos de sus hijos realizando actividades extraescolares".

El informe analiza, en primer lugar, si se dan las condiciones de aplicación de la excepción doméstica. A tal respecto, apunta dos conclusiones. La primera, con cita del caso Bodil Lindqvist, es que no se aplica tal excepción por no encontrarnos en el ámbito de la vida privada o familiar de los particulares cuando la publicación de la información se proyecta más allá del ámbito doméstico, lo que respecto a las imágenes en internet se constata cuando "no existe una limitación de acceso a las mismas". Un segundo criterio, coherente con el del Dictamen 5/2009 citado anteriormente, a la hora de considerar qué indicios apuntan la existencia de un tratamiento sometido a la Directiva, concluye que "para que nos hallemos ante la exclusión prevista en el artículo 2 de la 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.

Por consiguiente, la aplicación de lo hasta aquí dicho al presente caso supone que, cuando la actividad del consultante quede limitada, en los términos vistos, al ámbito personal o familiar no será de aplicación la LOPD. Por el contrario, cuando no opere la exclusión prevista en el artículo 2 de dicha Ley, esto es, cuando la actividad supere dicho ámbito, dicha norma será aplicable, debiendo solicitarse el consentimiento de los padres o de los propios menores cuando estos tengan capacidad para prestarlo, tanto para la obtención de la imagen como para su publicación en la página web, en tanto que ésta última constituye una cesión o comunicación de datos de carácter personal tal y como viene definida por el artículo 3 j) de la LOPD, esto es, como 'Toda revelación de datos realizada a una persona distinta del interesado'".

En conclusión, la configuración del espacio web es muy relevante al efecto de determinar la aplicabilidad de la legislación sobre protección de datos.

Por ultimo, cabe referirse a distintas resoluciones dictadas en el marco de procedimientos sancionadores y/o tutelas de derechos que afectan a servicios propios de la Web 2.0. En primer lugar, se han planteado supuestos de emisión de imágenes en portales que sirven archivos de video. En éste ámbito, la Agencia Española de Protección de Datos se ha servido de la doctrina del artículo 29 del Dictamen 4/2004, de 11 de febrero, del Grupo de trabajo relativo al tratamiento de datos personales mediante vigilancia por videocámara, y ha concluido que "los datos constituidos por imagen y sonido son personales". El carácter identificable de tales datos "puede resultar de la combinación de los datos con información procedente de terceras partes o, incluso, de la aplicación, en el caso individual, de técnicas o dispositivos específicos". A partir de esta premisa se concluye que:

> "La captación y reproducción de imágenes de los transeúntes en la calle, que constituyen datos de carácter personal, y su publicación en *"YouTube"*, accesible para cualquier usuario de Internet, se encuentra sometida al consentimiento de sus titulares, de conformidad con lo dispuesto en el artículo 6.1 de la LOPD".[24]

Este planteamiento ha sido matizado y adaptado a la realidad de internet apostando por priorizar el ejercicio de derechos de cancelación como método para la resolución de conflictos reservando el aparato sancionador para los supuestos más graves.[25]

2.3 Recomendaciones de actuación

A la vista de los planteamientos de tribunales y autoridades de protección de datos personales, una primera conclusión parece evidente: un medio de comunicación que abra un espacio en Facebook vendrá obligado a cumplir algunos principios normativos básicos en esta materia.

Estudiados seis de los principales medios de comunicación,[26] y salvo error de los autores, resulta que sólo uno de ellos –la cadena SER– dispone de algún tipo de reglas[27] para sus usuarios:

"Normas de participación

El objetivo de las páginas de Facebook gestionadas por la Cadena SER es establecer una relación directa entre la radio y sus diferentes programas y sus seguidores.

Para conseguirlo, se establecen las siguientes normas de participación, que se suman a las normas de Facebook. Estas últimas se pueden consultar en *http://www.facebook.com/terms.php?locale=ES:*

- Todas las opiniones son bienvenidas, pero evita insultos y un lenguaje que incite al odio, a la discriminación, a la promoción de actividades ilegales, que sea ofensivo, racista, violento o xenófobo. Publica tu opinión, pero con respeto al resto de usuarios y a la Cadena SER.
- Escribe tus comentarios sólo una vez y evita las mayúsculas, que en Internet se consideran gritos. Escribir de forma abusiva será considerado spam.
- En el caso de que se proponga un tema de debate, cíñete a él. Internet tiene muchos otros lugares donde podrás discutir sobre lo que quieras.
- Las páginas en Facebook gestionadas por la Cadena SER no admiten publicidad de empresas, eventos de cualquier tipo o propaganda política. Tampoco promoción de otros grupos o páginas de Facebook u otras redes sociales que no pertenezcan a la Cadena SER u otras empresas del Grupo Prisa.
- No compartas contenido protegido por copyright sin la autorización del propietario de los derechos.
- No publiques datos personales, ya que estarán a la vista de todos los visitantes.[28]

El equipo de administración de las páginas de Facebook gestionadas por la Cadena SER se reserva el derecho de eliminar cualquier mensaje o contenido que no cumpla estas normas o de bloquear a cualquier usuario si las viola de forma reiterada, y no se hace responsable de su incumplimiento ni de las consecuencias que este conlleve".

Como puede apreciarse, se trata de políticas de uso propias de un foro y sólo una de ellas hace alusión vagamente a la protección de datos personales.

Sin embargo, si consultamos el espacio de la Agencia Española de Protección de Datos[29] generado con motivo de la celebración de una conferencia internacional, podemos leer la siguiente información:

"Al hacerte fan de esta página, consientes: 1) en el tratamiento de tus datos personales en el entorno de Facebook conforme a sus <http://www.facebook.com/policy.php?ref=pf> políticas de privacidad; 2) el acceso de la AEPD a los datos contenidos en la lista de fans; y 3) a que las noticias publicadas sobre el evento aparezcan en tu muro.

La AEPD no utilizará los datos para otras finalidades ni para enviar información adicional. Si quieres darte de baja, sólo tienes que pinchar sobre el hipervínculo que aparece abajo a la derecha "Dejar de ser fan". Puedes ejercer los derechos de acceso, rectificación, cancelación y oposición en cualquier momento, mediante escrito, dirigido a la Agencia Española de Protección de Datos, Secretaría General, C/ Jorge Juan n 6, 28001 Madrid o enviando un e-mail a la dirección privacyconference2009@agpd.es, acompañado de fotocopia de documento oficial que te identifique. En caso de ejercerse por correo electrónico el documento deberá firmarse digitalmente en el mensaje o adjuntar un documento oficial escaneado. En el contexto de este tratamiento debes tener en cuenta que la Agencia Española de Protección de Datos únicamente puede consultar o dar de baja tus datos como fan. Cualquier rectificación de los mismos debes realizarla a través de la configuración de tu usuario.

Dirección de correo electrónico: ciudadano@agpd.es".

¿A qué responde esta significativa diferencia? Es evidente que, en el momento en que una empresa actúe en una red social vendrá obligada a cumplir con las previsiones del derecho vigente.[30]

Pueden diferenciarse diversos escenarios, aunque el más común consiste en registrar un usuario en los espacios más utilizados, esto es, Facebook, Tuenti, Twitter y, eventualmente, YouTube. En este caso se trata de una situación híbrida, ya que, por una parte, se actúa como un usuario más de la red social y, por otra, se asumen responsabilidades jurídicas por la actuación que se desarrolla. Así, cuando se abre un espacio en una red social, la organización actuará como lo que la Agencia Española de Protección de Datos y la jurisprudencia han definido como *responsable* de un tratamiento:

"Se desprende asimismo de los repetidos apartados del art. 3, como ya se ha manifestado, la diferenciación de dos responsables en función de que el poder de decisión vaya dirigido al fichero o al propio tratamiento de datos. Así, 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".[31]

Como consecuencia de dicha sentencia, en el artículo 5 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD), se ha definido esta figura como:

"q. Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados".

Por lo tanto, se da aquí la circunstancia definida en la sentencia y el precepto. Se trata de un tratamiento en el que la persona usuaria que abre su cuenta carece de todo control sobre el fichero titularidad de la red social. Por ello, las obligaciones que se derivan para la organización en materia de cumplimiento de la LOPD resultan limitadas y, por ejemplo, no existe deber de inscribir un fichero ni de formalizar un contrato de acceso a datos por cuenta de terceros.

Hay que partir de la base de que en este tipo de supuestos el uso se limita exclusivamente al alta en la red social y al empleo de las herramientas que en ella existen y no existe ninguna capacidad de decisión sobre la estructura, ordenación o gestión material de los datos distinta de la propia de la red social. Para poder afirmar que se actúa como una persona usuaria más deberían darse además otras condiciones:

- Comportarse como una persona usuaria que interactúa en el sistema de red social.
- No incorporar datos personales a recursos propios.
- No contratar ninguna prestación de servicios para el desarrollo o mantenimiento del espacio con el proveedor de la red social.
- No pactar servicios adicionales con el proveedor, como el análisis del comportamiento, seguimiento o elaboración de perfiles de persona usuaria, asociados o no, a la emisión de publicidad comportamental.[32]

En tal caso, para garantizar un adecuado cumplimiento de la LOPD, el medio de comunicación debería:

- Cumplir con el deber de información, ya que, puesto que existe un tratamiento, deben respetarse los principios y obligaciones derivados del artículo 5 de la LOPD. Para ello, resulta recomendable:
  - Ubicar una información breve en el espacio de la cuenta que facilite la red social con la información básica sobre la identidad y localización de la persona responsable, finalidad que se persigue y formas de ejercicio de los derechos.
  - Articular un procedimiento de bienvenida a nuevos amigos con un mensaje de correo electrónico que incluya esta información.
  - Hiperenlazar a políticas de privacidad corporativas.

Y, como señala el Grupo del artículo 29 en el Dictamen 5/2009 citado anteriormente, informar en particular sobre:

- La utilización de los datos con fines de comercialización directa.
- La posible distribución de datos a categorías específicas de terceros.
- El uso de datos sensibles.
- La integración en el entorno de aplicaciones de terceros que capten y/o traten los datos de los "amigos" cuando dicha integración dependa de la voluntad de la persona usuaria responsable de la cuenta.

En segundo lugar, cabe señalar que la causa que legitima el tratamiento de los datos personales en este ámbito no puede ser otra sino el consentimiento del artículo 6 de la LOPD.[33] Debe entenderse que este se manifiesta cuando se solicita "hacerse amigo de" o cuando se acepta una invitación. Cabe tener en cuenta que:

- El consentimiento únicamente afecta a los datos de la persona que se agrega, nunca a los de aquellos terceros relacionados con "el amigo" cuyo perfil se encuentre abierto.
- La posible existencia de excepciones a la regla del consentimiento deberán examinarse caso por caso y con pleno respeto a la regulación.
- Un perfil abierto "no implica consentimiento". Debe recordarse que, conforme señala la Agencia Española de Protección de Datos en su Informe 0342/2008, internet, y por ello las redes sociales, no son fuentes accesibles al público.
- La incorporación de datos, como la dirección de correo electrónico, a los propios sistemas constituye un tratamiento sujeto a la LOPD y su accesibilidad en un entorno de red social no es necesariamente una causa de legitimación para el tratamiento.
- La garantía de los derechos de los "amigos" tiene un contenido limitado. Rigen los derechos de acceso, rectificación, cancelación y oposición al tratamiento. No obstante:
  - El contenido del derecho de acceso vendrá definido por las posibilidades que ofrezca la red y la capacidad de acceso a información del perfil de cada persona usuaria concreta. Por tanto, prácticamente bastará con ofrecer, a quién ejerza el derecho, los pantallazos en los que se muestre a qué datos se accede.
  - El derecho de oposición, rectificación y cancelación se encontrará modulado. La persona responsable del tratamiento debería satisfacerlo sobre aquellos aspectos de la aplicación que se encuentren bajo su control, como por ejemplo modificar o eliminar un comentario del propio muro. La rectificación de aspectos relativos al perfil de la persona usuaria normalmente se ejercen ante la persona proveedora. La cancelación u oposición, cuando consiste en "dejar de ser amigos", podría ser ejercida por ambas partes.

- Existirán límites en cuanto al uso de los datos. El principio de finalidad constituye un límite infranqueable y vendrá definido por:
  - Las condiciones de uso de la red social, que podría prohibir usos concretos.

- La información disponible y efectivamente facilitada "al hacerse amigos".

- Rigen los principios de seguridad y secreto para cualquier persona usuaria del responsable del tratamiento, pero deberán adaptarse a las condiciones propias del entorno y afectarán únicamente a los tratamientos efectivamente realizados.

3. Opinión e información de los usuarios de una red social

Para finalizar con el examen de las cuestiones relacionadas con el uso de redes sociales, resulta conveniente examinar lo que sin duda resulta el objetivo esencial de estos espacios: favorecer que sus usuarios manifiesten libremente su opinión.

En principio, y dada la naturaleza del entorno, esto es, un espacio de un medio de comunicación vinculado al ejercicio ciudadano de los derechos del artículo 20 de la Constitución española, se dan condiciones para la exclusión de la aplicación de las normas sobre protección de datos personales.[34] En este sentido, habitualmente, la Agencia Española de Protección de Datos ha reconocido la prevalencia de los derechos del artículo 20 de la CE.[35] No obstante, debe señalarse que, al menos en un caso, la Audiencia Nacional ha considerado prevalente el derecho a la protección de datos al considerar que la información publicada no requería del acompañamiento de la imagen de una de las víctimas del 11–M y aplicar un juicio de proporcionalidad.[36]

Cuando quien trata datos personales es una persona usuaria en su propio muro, la Agencia suele reconducir la cuestión al procedimiento de tutela de derechos del artículo 18 LOPD, ordenando la cancelación de los datos a la persona responsable de la red social.[37]

Todos los criterios expuestos nos permiten una aproximación a la naturaleza jurídica de las opiniones vertidas en el muro de un medio de comunicación basada en dos categorías de juicio. En primer lugar, un juicio sobre el contenido permitirá determinar si la persona usuaria está ejerciendo su derecho a informar o a expresar su opinión y se dan las condiciones de prevalencia del mismo respecto a los derechos de terceros. Esto es, que la información se base en hechos ciertos, o percibidos como tales, y posean relevancia pública para la conformación de la opinión pública.

El segundo criterio de aproximación se basa en la determinación de la responsabilidad de la persona titular del muro. Aquí el punto de vista de la Agencia se enmarca en la línea definida por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y apuntada por el Dictamen 5/2009, de considerar a la persona titular de una red social como proveedora de servicios de la sociedad de la información.

Se da aquí una diferencia sustancial con la responsabilidad de la persona editora, por ejemplo, en las tradicionales cartas al director. La STC 3/1997 sintetiza de modo muy preciso el criterio del Tribunal, que, partiendo del hecho de la existencia de un examen previo de las cartas que publica, requiere de algún modo la aplicación de un doble filtro sobre la identidad de la persona remitente y sobre la relevancia del contenido cuando la identificación no resulte fiable. Por ello, considera la persona editora responsable de estos contenidos.[38]

En resumen, y utilizando un razonamiento analógico elemental, en aquellos espacios de internet en los que los contenidos son directamente desarrollados por la persona titular, dejando un espacio a la participación, la responsabilidad se centraría en verificar la identidad del lector o lectora que publica su opinión. Esta doctrina sería inaplicable al contexto de una red social, ya que su modo de funcionar impide a día de hoy cualquier identificación y, además, la celeridad en la publicación de comentarios y el número de estos hace imposible su control, si no es a posteriori.

Por ello, como bien señalaba el Dictamen 5/2009, en este caso se trata de la prestación de un servicio de la sociedad de la información sujeto a lo dispuesto por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI). Por lo tanto, cuando resulte de aplicación la legislación española, la responsabilidad de la persona proveedora, en lo que a este documento respecta, se regirá por los artículos 16 y 17 de la LSSI. Por consiguiente, es necesaria la concurrencia de dos elementos para que exista responsabilidad:

- Conocimiento efectivo. Éste se producirá cuando se notifique la reclamación a través del espacio de denuncias de la red social o cuando una autoridad, como la AEPD, requiera de algún tipo de actuación.
- Ausencia de diligencia en la retirada de la información.

En cualquier caso, se trata de una realidad compleja que traslada una cierta responsabilidad ética a los medios. Puesto que se ha producido una democratización mediante la extensión de la posibilidad de ejercer la libertad de opinión a cualquier ciudadano, y ya que los propios medios facilitan estos espacios en las redes sociales, sería muy aconsejable que promoviesen la formación de los usuarios mediante códigos éticos o reglas de uso.[39]

Ello resulta particularmente necesario en un contexto de ausencia de una normatividad específica. Ni la Ley orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, ni la Ley orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación, ofrecen soluciones adecuadas para resolver estos problemas. Buena prueba de ello es que, cada vez con mayor frecuencia, el ciudadano acude al ejercicio del derecho de cancelación del artículo 16 de la LOPD en este tipo de supuestos.

Los conflictos en esta materia desbordan con mucho las redes sociales y se extienden al periodismo ciudadano y a los blogs, y al llamado *derecho al olvido*. La Directiva 95/46/CE faculta-

ba a los estados miembros para desarrollar esta materia en el ámbito de los medios de comunicación. Tal vez ha llegado el momento de afirmar que este desarrollo resulta indispensable.

Notas

1. Este artículo es, en gran medida, deudor de una monografía previa. Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. Cizur Menor (Navarra): Civitas, 2010.

2. Cerezo, J.M. L*a blogosfera hispana: pioneros de la cultura digital* [En línea]. Biblioteca de la Fundación France Telecom España, 2006. <http://fundacionorange.es/areas/25_publicaciones/publi_253_9.asp> (Disp. 19/03/2010)

3. Muy gráficamente, Castells señala:

> "Internet es una extensión de la vida tal como es, en todas sus dimensiones y modalidades. Es más, incluso en los juegos de rol y en los chat room informales, las vidas reales (incluidas las vidas reales on line) son las que determinan, definen, el modelo de interacción online"

Castells, M. *La galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*. Barcelona: Areté, 2001, pág. 139. Para comprender la capacidad de las redes para definir espacios de comunidad resulta particularmente interesante el capítulo dedicado en este trabajo a las comunidades virtuales (págs. 137-158).

4. Véase <http://twitter.com/>

5. Véase Martínez Martínez, R. "¿Interrogantes jurídicos ante los smartphone?". *Actualidad Jurídica Aranzadi*, núm. 822, pág. 13.

6. Véase <http://www.theinternetofthings.eu/>

7. Cuando de la mano de la televisión digital terrestre se produzca una verdadera interactividad se multiplicarán los tratamientos de datos personales a través de este canal. Martínez Martínez, R. "Los contenidos audiovisuales en la multidifusión digital. Nuevos retos para la protección de datos personales". En: Francés i Domenech, M. (coord.). *Hacia un nuevo modelo televisivo. Contenidos para la televisión digital*. Barcelona: Gedisa, 2009, págs. 83-95.

8. Resultan particularmente relevantes a este respecto los hallazgos de la autoridad canadiense de protección de datos en las indagaciones realizadas respecto a Facebook:

> 148. According to Facebook's developer blog (June 4, 2009):
>
> "The growth we have seen on Platform has been tremendous. Today there are over 350,000 active applications on Platform from over 950,000 developers living in more than 180 countries. These range from simple applications created by single users to share with their friends to impressive businesses employing hundreds of people and reaching tens of millions of users every month and generating tens of millions of dollars of revenue. For example, close to 10,000 applications have 10,000 or more monthly active users, and more than 100 applications have more than 1 million monthly active users."
>
> 149. When users add an application, they must consent to allow the third-party application developer to have access to their personal information, as well as that of their friends. Moreover, as CIPPIC has correctly pointed out, unless users completely opt out of all applications and block specific applications, they are not given the option of refusing to share their names, networks, or lists of friends when friends add applications. [...]
>
> 1) Facebook had inadequate safeguards to effectively restrict these outside developers from accessing users' profile information, along with information about their online friends.
>
> 2) Facebook was not obtaining users' meaningful consent to the disclosure of their personal information to application developers when either they or their friends add applications."

Denham, E. R*eport of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act. July 16, 2009*. Office of the Privacy Commissioner of Canada. PIPEDA Case Summary #2009-008.

<http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm> (Disp. 16/04/2010), págs. 38 y 94.

9. Véase <http://www.maestrosdelweb.com/editorial/web2/>

10. Véase Alamillo Domingo, I. "La identidad electrónica en la red". En: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. págs. 37-53.

11. Véase Schwartz, P.M. "Internet privacy and the State". *Connecticut Law Review*, vol. 32, 2000, págs. 815-859

12. De hecho esta es la apuesta más reciente de Google con su red social Google +:

> "La primera de las herramientas o servicios incluidos es Circles, una herramienta que permite crear círculos de personas a través de los cuales sus miembros pueden debatir, publicar y compartir todo tipo de información únicamente con grupos definidos de contactos como la familia, amigos de la escuela, compañeros de trabajo, compañeros de equipo, colegas, etc.". <http://www.puromarketing.com/16/10334/google-project-nueva-social-google-llega.html>

13. Frente a quienes vienen afirmando la imposibilidad de acotar jurídicamente el fenómeno de internet, y sin dejar de ser conscientes de la necesidad de actuaciones concretas del legislador, cabe considerar que en el contexto de las tecnologías de la información y de las comunicaciones sea necesario modular o adaptar el ordenamiento, ya que, en el ámbito de internet, la normatividad no se proyecta sobre los instrumentos, sino sobre su uso y sobre su diseño. Véase Trías Sagnier, J. "Informática y privacidad. ¿Se pueden poner puertas al campo?" *Cuenta y razón*, núm. 63, 1992, págs. 98-101.

14. En esta línea, en los últimos años se ha profundizado en las metodologías del Privacy Impact Assessment y del Privacy by Design, cuyo planteamiento es coincidente con lo que aquí se viene señalando: los proveedores y programadores deben

tener en cuenta en su diseño, de modo apriorístico, métodos que garanticen el respeto del derecho a la vida privada de los usuarios.

Como ha señalado Lessig, el programador tiene la capacidad de definir reglas de funcionamiento del entorno que actúan de modo materialmente normativo y, por lo tanto, la posibilidad de definir modos de funcionamiento que garanticen el cumplimiento de los principios que el ordenamiento jurídico incorpora. Lessig, L. *El código y otras leyes del ciberespacio*. Madrid: Taurus, 2001 y Lessig, L. *Code version 2.0.* Basic Books. Nueva York: Perseus Books Group, 2006. Disponible en <http://pdf.codev2.cc/Lessig-Codev2.pdf>

En esta materia, los documentos son cada vez más abundantes, si bien la metodología de referencia es la de la Information Commissioner's Office británica.

- ICO. Privacy Impact Assessment (PIA) handbook (Version 2). 2009. <http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html> (disp. 22/03/2010).
- Homeland Security (EE.UU.) Privacy Impact Assessment EINSTEIN Program. <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf> (disp. 22/03/2010).
- Treasury Board of Canada Secretariat. Privacy Impact Assessment - Policies and Publications. <http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist-eng.asp> (disp. 22/03/2010).
- Privacy by Design http://www.privacybydesign.ca/

Por último, véase Warren, Adam. "Privacy Impact Assessments: the UK experience". *31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Madrid, 4-6 de noviembre de 2009*. <http://www.privacyconference2009.org/program/Presentaciones/common/pdfs/adam_warren_speech_en.pdf>

15. Como se recordará, la Sra. Lindqvist era una catequista sueca que, a finales de 1998, creó con su ordenador personal varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que pudiera resultarles útil. Dichas páginas contenían información sobre la Sra. Lindqvist y dieciocho de sus compañeros de la parroquia, incluido su nombre de pila, acompañado, en ocasiones, del nombre completo. Además, la Sra. Lindqvist describía en un tono ligeramente humorístico las funciones que desempeñaban sus compañeros, así como sus aficiones. En varios casos se mencionaba la situación familiar, el número de teléfono e información adicional. Asimismo, señaló que una de sus compañeras se había lesionado un pie y que se encontraba en situación de baja parcial por enfermedad. Tras ser sancionada y recurrir, el tribunal sueco consultó al Tribunal de Justicia sobre las condiciones de aplicación de la Directiva 95/46/CE.

Sentencia del Tribunal de Justicia de 6 de noviembre de 2003 en el asunto C-101/01. Petición de decisión prejudicial planteada por el Göta Hovrätt. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:007:0003:0004:ES:PDF>

16. Las normas de protección de datos personales no se aplican, como señala el artículo 4 RLOPD a los tratamientos "realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares".

17. Grupo de trabajo del artículo 29. *Dictamen 5/2009 sobre las redes sociales en línea.* (01189/09/ES WP 163). (Disp. 31/03/2010)

18. Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. <http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm>

19. El Grupo ha señalado que existen tratamientos que no podrían realizarse sin recurrir al uso del propio ordenador del usuario, generalmente mediante la explotación de *cookies*, con lo que se estarían utilizando medios en territorio europeo. Véase WP148, Dictamen 1/2008 sobre asuntos relativos a la protección de datos vinculados a las herramientas de búsqueda.

20. Agencia Española de Protección de Datos. INTECO. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Madrid, 2009.

21. A ellos se orientan dos recomendaciones específicas:

- "Tener especial cuidado al publicar contenidos audiovisuales y gráficos en sus perfiles, especialmente si se van a alojar imágenes relativas a terceras personas.
- No etiquete contenidos audiovisuales con la identidad real de sus protagonistas ni ofrezca datos de terceros en su espacio sin su consentimiento."

Y un recordatorio:

- "Cuando publica una foto o escribe en un blog puede estar incluyendo información sobre otras personas. Respete sus derechos".

<http://www.inteco.es/file/aiYG6hA575_aXKiMJlkT_g>

22. "Los medios que la informática e Internet ponen a nuestra disposición nos permiten realizar muchas actividades en Internet. Gracias a ellos podemos editar audio y vídeo y compartirlos con el mundo entero, publicar nuestras fotografías y compartirlas, organizar actividades virtuales, convocar citas y encuentros masivos, o ejercer el periodismo ciudadano. […]

- No publicar informaciones que no respondan a los requisitos de veracidad, interés público y respeto a la dignidad de las personas, y en particular a la juventud y la infancia.
- No difundir rumores o informaciones no contrastadas.
- Rectificar o retirar la información cuando de modo justificado lo solicite un afectado.
- Nunca publicar información que ponga en riesgo a la familia y en particular a los niños, ni nuestras amistades, vecinos, etc.

- Tener especial cuidado respecto a la publicación de información relativa a los lugares en que el usuario o un tercero se encuentra en todo momento. Podría poner en peligro a los usuarios, dado que permite a los posibles infractores conocer en todo momento donde se encuentra, qué está haciendo y hacia dónde se dirige el usuario, lo que puede suponer un grave riesgo para su integridad.
- No grabar ni publicar imágenes, videos o cualquier otro tipo de registro sin el consentimiento de los afectados.
- No tratar datos personales de terceros, especialmente cuando se divulguen a terceros, sin conocimiento y consentimiento de los afectados.
- Cumplir cuando proceda con las obligaciones de la Ley Orgánica de Protección de Datos.
- Informar sobre los deberes de los usuarios en los procedimientos de alta y registro.
- Elaborar y publicar códigos éticos que garanticen unas mínimas reglas de actuación de los usuarios o de las comunidades en las redes sociales".

23. <http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdfs/2008-0615_Inaplicaci-oo-n-LOPD-a-actividad-de-particulares-que-comparten-fotos-de-sus-hijos-a-trav-ee-s-de-Internet.pdf>

24. Véase PS/00479/2008, disponible en: <http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2008/common/pdfs/PS-00479-2008_Resolucion-de-fecha-30-12-2008_Art-ii-culo-6.1-LOPD.pdf>.

25. "Es cierto que la realidad de Internet requiere realizar una interpretación del principio de consentimiento que evite una aplicación estricta que la paralizaría o la convertiría en una red profusa en vulneraciones de datos personales de millones de personas accesibles fácilmente usando un mero buscador y de los que no cabe aportar el consentimiento previo.

De ahí que no sea conveniente realizar una interpretación maximalista del requerimiento de consentimiento sino que debe considerarse el principio según el cual cuando el ordenamiento jurídico ofrece varias soluciones sea más adecuado el agotamiento de otras fórmulas alternativas en el caso de que sea posible, razón por la que el uso del derecho de cancelación de datos tendente al cese del tratamiento de datos personales deba priorizarse. Se trataría de un procedimiento que posibilita la corrección con celeridad del dato incluido con objeto reparador con carácter previo a una tutela por incumplimiento o a la incoación, en su caso, de un procedimiento sancionador, que reviste naturaleza punitiva si no se hiciera desaparecer.

Esta premisa no debe obstar para que en determinados supuestos – datos especialmente sensibles o derechos afectados de especial gravedad así como vulneración del secreto profesional – quepa utilizar el procedimiento sancionador al objeto de sancionar una conducta especialmente grave no amparable en las reglas de Internet como ocurre en el caso denunciado".

Véase PS/00508/2008.

26. Cadena SER, Cadena COPE, Onda Cero, Televisión Española, Telecinco y laSexta.

27. <http://es-es.facebook.com/cadenaser?sk=app_214923178538944>

28. El subrayado es de los autores.

29. <http://es-es.facebook.com/AEPD?sk=info>

30. Véase Vilasau Solana, M. "Privacidad, redes sociales y el factor humano". En: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. págs. 66-71.

31. Véase la Sentencia de 5 de junio de 2004, de la Sala Tercera de lo Contencioso-Administrativo del Tribunal Supremo, sobre diferenciación entre el responsable del fichero y el responsable del tratamiento que confirma la Sentencia de 16 de octubre de 2003, de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, dictada en el recurso número 1539/2001. Disponible en <http://bit.ly/oDvST6>.

32. La publicidad comportamental se basa en la observación continuada del comportamiento de los individuos. Busca estudiar las características de dicho comportamiento a través de sus acciones (visitas repetidas a un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los intereses inferidos de su comportamiento. La publicidad comportamental implica normalmente la recogida de direcciones IP y el tratamiento de identificadores únicos (mediante las *cookies*). La utilización de dichos dispositivos permite aislar a los usuarios, aun desconociéndose sus nombres verdaderos. Además, la información recogida se refiere a características o comportamiento de una persona y se utiliza para influir a dicha persona concreta. Este perfil se acentúa cuando se tiene en cuenta la posibilidad de que los perfiles se vinculen en todo momento con información directamente identificable proporcionada por los usuarios, como la información aportada en el registro.

Debe tenerse en cuenta que se define aquí una posibilidad tecnológicamente disponible. Corresponderá a editores, anunciantes y proveedores de servicios de publicidad la decisión de utilizar estas técnicas.

Véase Grupo de Trabajo del Artículo 29. *Dictamen 2/2010 sobre publicidad comportamental en línea*. 00909/10/ES GT 171, disponible en *http://bit.ly/dsAN9F*, y Peguera Poch, M. "Publicidad online basada en comportamiento y protección de la privacidad". En: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. págs. 354-380.

33. Véase, Arenas Ramiro, M. "El consentimiento en las redes sociales on line". En: Rallo Lombarte, A.; Martínez Martínez, R. (coord.). *Derecho y redes sociales*. op. cit. págs. 117-144.

34. Cosa distinta sería el uso indebido de datos personales por parte de los usuarios de redes sociales en sus propios muros, que podría determinar en algunos casos responsabilidades en materia de protección de datos personales. Por ejemplo, mediante la publicación de imágenes o comentarios con datos personales en un entorno privado de red social sin el consentimiento de las personas afectadas.

35. Véase el Expediente nº: E/00871/2005. <http://bit.ly/nx7oMt>.

36. "La imagen, pues, es un dato que encuentra amparo en la Ley Orgánica 15/99 pero resulta que un examen detallado del expediente permite entender que, aunque las imágenes no sean de buena calidad, puede entenderse que el tratamiento del dato de la imagen ha sido excesivo tomando en consideración que no se encuentra amparado por el consentimiento de los afectados (no consta que conocieran la publicación de las imágenes) y tampoco se encuentra amparado por la libertad de información y, en todo caso, parece que se ha producido un empleo desmedido de la imagen como dato personal puesto que el carácter noticiable de la información se cumplía suficientemente sin necesidad de incluir imágenes directas de los enfermos. Por ello, deberá continuarse la instrucción en relación al posible empleo del dato de la imagen sin justificación". Sentencia de 9 de julio de 2009, de la Sección Primera de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional, dictada en el recurso número 325/2008.

37. Véase el Procedimiento nº: TD/00690/2009. Disponible en <http://bit.ly/n9DwdR>.

38. "C) En particular, respecto a aquellos supuestos en los que el medio autoriza la publicación de un escrito procedente de persona enteramente ajena al mismo, hemos precisado que "el deber de diligencia del Director del periódico entraña la comprobación de la identidad de la persona que figura como autor de la carta, antes de autorizar su publicación", como es práctica habitual. Agregando que si esta específica diligencia no fuera exigible, "no quedarían debidamente deslindados, respectivamente, el ejercicio de la libertad de expresión de una persona ajena al medio, que éste posibilita al publicar la carta, y el derecho que asiste al diario de informar de esa opinión a sus lectores"; y, ello supondría, asimismo, "que quedase afectado el derecho de los lectores a recibir una información veraz, que el art. 20.1 d) CE garantiza". La comprobación de la identidad de la persona que es autora del escrito permite, pues, "que ésta asuma su responsabilidad caso de que la carta sea constitutiva de delito", dado que, en otro caso, "se abriría la puerta a la creación de espacios inmunes a posibles vulneraciones del derecho al honor constitucionalmente garantizado" [STC 336/1993, fundamento jurídico 7.º,B)].

3. Ahora bien, la anterior doctrina no lleva necesariamente a estimar que la acción del medio autorizando la publicación de una "carta al Director" procedente de persona que no resulta identificada entrañe, en todo caso, la responsabilidad de aquél, y que a este fin sea suficiente la verificación de que no ha existido esa diligencia específica. Pues cuando se trata de enjuiciar una posible lesión del derecho al honor de una tercera persona por el escrito ajeno que el medio ha publicado, lo decisivo es no sólo el hecho de la publicación sino determinar, en atención al contenido de dicho escrito si se ha producido o no la vulneración de ese derecho fundamental.

En efecto, al autorizar la publicación de un escrito ajeno cuyo autor se ha identificado previamente será éste quien asuma la responsabilidad que del mismo pueda derivarse si su contenido resulta lesivo del derecho al honor de una tercera persona. Sin embargo, la situación es muy distinta si el escrito ajeno es publicado sin que el medio conozca la identidad de su autor, pues en tal supuesto dicho escrito no constituye una acción que pueda ser separada de la de su publicación por el medio, conforme a la doctrina expuesta en la STC 159/1986. De suerte que al autorizar la publicación del escrito pese a no conocer la identidad de su autor ha de entenderse que el medio, por ese hecho, ha asumido su contenido. Lo que entraña una doble consecuencia: en primer lugar, que el ejercicio de las libertades que el art. 20.1 reconoce y garantiza habrá de ser enjuiciado, exclusivamente, en relación con el medio, dado que el redactor del escrito es desconocido. En segundo término, que al medio le corresponderá o no la eventual responsabilidad que pueda derivarse del escrito si su contenido ha sobrepasado el ámbito constitucionalmente protegido de la libertad de información y, en su caso, de la libertad de expresión, lesionando el honor de terceras personas o, por el contrario, lo ha respetado". STC 3/1997.

39. Véase Agencia Española de Protección de Datos. INTECO. *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Madrid, 2009, pág 92.