

Protecció de dades personals i xarxes socials: obligacions per als mitjans de comunicació

ARTEMI RALLO

*Catedràtic de dret constitucional de la Universitat Jaume I
i exdirector de l'Agència Espanyola de Protecció de Dades
(2007-2011)*

rallo@dpu.uji.es

RICARD MARTINEZ

*Professor de dret constitucional de la Universitat de València.
Excoordinador de l'Àrea d'Estudis de l'Agència Espanyola de
Protecció de Dades (2007-2011)*

martiner@uv.es

Resum

Les xarxes socials presenten un nou escenari per a la participació ciutadana i per definir un nou model de relació entre ciutadans i mitjans de comunicació, però per operar en aquest mitjà és fonamental tenir en compte les normes vigents en matèria de protecció de dades. Aquest article explora tant els principis bàsics que regeixen aquesta matèria per als mitjans de comunicació i per a les persones usuàries dels espais en xarxes socials, com els conflictes que poden derivar d'un exercici inadequat de la llibertat d'expressió.

Paraules clau

Xarxes socials, privacitat, protecció de dades personals, llibertat d'expressió, dret a la informació.

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. Els mitjans a les xarxes socials

Les xarxes socials¹ constitueixen, probablement, la novetat més gran del darrer decenni per als mitjans de comunicació, ja que els proveeixen d'una interactivitat insospitada fins fa molt poc temps. Tradicionalment era la ràdio el mitjà que amb regularitat podia obrir els micròfons en temps real per als oients. Això depenia, però, de la disponibilitat de temps a la graella i de la naturalesa del programa. Avui, qualsevol mitjà de comunicació que es preï ha desembarcat en una xarxa social, ja sigui com a corporació, ja sigui mitjançant el recurs d'obrir els seus programes més significats a la interacció amb la persona usuària.

Per aquest procediment, les possibilitats de donar protagonisme al seguidor o seguidora es multipliquen i van des de la conversa en temps real a la provocació. La interacció a la xarxa social permet així integrar la persona usuària en la dinàmica del programa, fidelitzar-la, polsar l'estat d'opinió en temps real i, atesa la capillaritat d'aquests mitjans, multiplicar l'impacte de cada emissió.

Al fenomen de les xarxes socials cal afegir-hi l'impacte de l'anomenada *blocosfera*, que, de fet, va ser prèvia en el temps.² Ha nascut un periodisme ciutadà d'opinió –no sempre rigorós– i els mitjans tradicionals s'han afanyat a incorporar als seus espais a internet un espai de blocs, ja sigui conduïts pels seus professionals, ja sigui obert als ciutadans.

En aquest context es plantegen, almenys, dos interrogants des d'un punt de vista jurídic. Quins requisits normatius s'imposen a les empreses de comunicació que decideixen desembarcar en una xarxa social –aquí ens ocuparem essencialment del dret fonamental a la protecció de dades. I, en segon lloc, com s'articularen els conflictes relacionats amb la publicació d'informació o d'opinió pels mateixos usuaris.

2. Protecció de dades a les xarxes socials

Per aplicar les normes sobre protecció de dades personals és fonamental entendre clarament el context. Com va apuntar

Castells,³ l'evolució de la xarxa afavoreix que es generin comunitats, tant mitjançant el trasllat de grups socials preexistents al món virtual, com mitjançant la creació de grups d'interès d'àmbit global. A més, un bon nombre dels serveis que s'hi vinculen s'orienten a l'oci i a fomentar aspectes directament relacionats amb la vida personal o privada, com ara compartir fotografies, escoltar música o compartir vídeo, o expressar opinió mitjançant píndoles breus de 140 caràcters.⁴

A això s'hi ha d'unir un conjunt d'elements de caràcter tècnic, la influència futura dels quals és, avui, imprevisible. En primer lloc, la ubicuitat és una de les característiques més destacades als serveis d'internet. El telèfon mòbil⁵ es converteix en un complet gestor i organitzador amb funcions que van des de l'agenda personal a la gestió domòtica en l'anomenada "internet de les coses"⁶ passant per l'adopció de decisions basades en serveis de valor afegit, com ara la geolocalització. El telèfon és ara un espai d'oci i de joc compartit, una eina d'accés a xarxes socials o un proveïdor d'accés a serveis de televisió digital interactiva.⁷

D'altra banda, també des del punt de vista tecnològic, l'univers web deixa de ser un lloc passiu per convertir-se en un espai social molt dinàmic. La persona usuària pot expressar la seva opinió, obtenir opinions de terceres persones, mostrar-se a si mateixa. És un entorn complex en què les aplicacions no són sempre del proveïdor principal⁸ i els usuaris poden ser alhora *betatesters* i desenvolupadors.

Per tant, el Web 2.0 va molt més enllà. No es tracta únicament d'un conjunt de recursos més avançats o menys de programari. Comporta el naixement d'un univers social propi de la societat xarxa, poblat de comunitats que poden anar del que és més proper –el grup immediat d'amics–, a qualsevol tipus d'agrupació horitzontal –grups professionals o socials–, vertical –espais de treball en grup– fins i tot "informal", sense límits d'espai o de temps. Probablement, per això s'afirma que el Web 2.0 "es una actitud y no precisamente una tecnología".⁹

2.1 La identitat és l'element nuclear

A la societat de la informació la moneda de canvi és la informació personal.¹⁰ Com tothom sap, en navegar l'internauta deixa un rastre econòmicament rendible. Gràcies a les rutines de funcionament d'internet, el rastreig de les IP, la informació bàsica sobre les aplicacions instal·lades al nostre ordinador, les *cookies* o els *logs* de navegació, es generen perfils d'usuari aprofitables per tal d'establir perfils genèrics de navegació amb un valor de mercat determinat.¹¹

Seguir el rastre d'una navegació, fins i tot sense identificar de manera concreta l'internauta, aporta informació extraordinàriament valuosa si es contextualitza. La persona usuària, de manera inconscient, revela preferències de tota mena, indica quins assumptes li interessen, quins gràfics l'atrauen o quina publicació prefereix. Aquestes empremtes electròniques aprofiten per facilitar la navegació i fer-la més ràpida, per presentar la publicitat d'una determinada manera i fer estudis de mercat, o per oferir al client que s'ha identificat serveis personalitzats adaptats a la seva navegació per internet.

Si des del punt de vista del seu funcionament bàsic i "tradicional", internet presentava un repte per a la protecció de la vida privada, revesteix més complexitat a les xarxes socials, on ja no n'hi ha prou amb els perfils genèrics d'una persona usuària ni amb les identitats fictícies. Per ser eficaç en una xarxa social, per aconseguir-ne els objectius, l'individu s'identifica. I en aquest context la identitat té un valor extraordinari, perquè gràcies a ella la informació, el missatge o la publicitat es personalitzen. Es té la capacitat d'establir o d'identificar cercles de confiança¹² i, gràcies a això, la *viralitat* dels missatges multiplica l'eficiència i l'eficàcia dels tractaments.

En cap cas s'ha de posar en dubte la contribució de les xarxes socials al debat públic; els exemples recents de democratització en països del nord d'Àfrica en constitueixen una prova evident. Això no vol dir que l'actuació dels proveïdors i dels mateixos usuaris no estigui sotmesa a regles.¹³

Per això, la primera qüestió que ens hem de plantejar és si hi ha principis aplicables a internet, i en particular a les xarxes socials. I la resposta és afirmativa. Per tant, la qüestió en els aspectes nuclears no rau tant a determinar si existeixen o no principis bàsics aplicables, que evidentment n'existeixen, sinó si realment es tenen en compte des del disseny inicial de les aplicacions.¹⁴

2.2 L'aplicació de normes sobre protecció de dades personals

Els tractaments d'informació personal constitueixen l'element nuclear de les xarxes socials. I això és així tant des de la perspectiva dels proveïdors de serveis, el negoci dels quals es basa precisament en els beneficis que produeix l'explotació d'aquesta informació, com des de la dels usuaris, que exposen la seva informació i s'exposen amb ella personalment i professionalment. Per això, el dret per excel·lència en aquest context no podria ser altre que el dret a la protecció de dades.

2.2.1 L'estàndard Lindqvist

Sense cap mena de dubte, el cas Bodil Lindqvist constitueix una referència de primer ordre quan es tracta d'establir criteri per aplicar les normes sobre protecció de dades a les xarxes socials.¹⁵ En aquest sentit, es pot dir que el Tribunal de Justícia ha definit amb claredat els criteris a seguir davant un tractament de dades personals en una pàgina web.

És important tenir en compte que la conducta consistent a publicar una foto, un vídeo o un text escrit en una xarxa social no difereix en termes materials en absolut del cas Lindqvist: és exactament la mateixa situació. Simplement, la tecnologia ha avançat i permet fer-ho sense coneixements tècnics previs i en un entorn cooperatiu. A Lindqvist, el Tribunal de Justícia va concloure que es donaven les condicions per aplicar la Directiva 95/46/CE, és a dir:

1. Que existia tractament

"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”.

Per a això, va al·ludir a les categories de tractament que –cal subratllar-ho– inclouen la comunicació per transmissió i la difusió, conceptes incardinables en el de cessió.

“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 resultava aplicable l'excepció de vida privada¹⁶

“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 conflicte entre el dret a la protecció de dades i la llibertat d'expressió o el dret a la informació n'ha de resoldre l'autoritat o el jutge nacional competent

“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”.

Per tant, si apliquem literalment les conclusions d'aquest cas a una opinió al “mur” d'una xarxa social és evident que, sota certes condicions, hi ha d'haver un tractament subjecte a la Directiva. I el mateix succeirà si s'hi etiqueta una fotografia o s'hi publica un vídeo que concerneixi persones identificades o identificables.

A la pràctica, com veurem tot seguit, l'excepció de *vida priva-*

da únicament és aplicable quan l'espai a la xarxa social es configuri de tal manera que només sigui visible a un grup d'amics i s'autoritzi expressament. Si no, es donaria plenament el cas Lindqvist.

2.2.2 L'opinió del Grup de treball de l'article 29

En el Dictamen 5/2009 sobre les xarxes socials en línia,¹⁷ el Grup de treball estableix les condicions d'aplicació de la Directiva 95/46/CE¹⁸ partint de la consideració que, en sentit jurídic, les xarxes socials són serveis de la societat de la informació. És evident que per al funcionament d'aquest tipus de serveis cal tractar dades personals primer en el registre i per a la configuració del perfil de la persona usuària. D'altra banda, i ja que l'objectiu final d'una xarxa social és interactuar amb altres usuaris, cada un d'ells aporta informació en forma de descripcions, opinions, fotografies etc., i la xarxa social els proveeix d'eines –llistes de usuaris, missatgeria privada, correu electrònic, etc.– que la faciliten i per als quals es requereix desenvolupar algun tipus de tractament.

Des d'aquest punt de vista, no hi ha dubtes respecte de l'aplicabilitat de la Directiva. Per aquest motiu, el Grup de treball centra els seus esforços a esmicolar cadascun dels elements d'aquests tractaments. En aquesta línia, hi ha un aspecte que no ofereix dubtes: les disposicions de la Directiva relativa a la protecció de dades s'apliquen en la majoria dels casos als proveïdors de serveis de xarxa social, encara que la seva seu es trobi fora de l'EEE.¹⁹ No obstant això, la complexitat d'aquest tipus de serveis obliga a fixar criteris que identifiquin altres possibles responsables. Ho seran els proveïdors externs d'aplicacions quan tractin dades i també podrien ser-ho els mateixos usuaris sota certes condicions:

- Quan la xarxa social s'utilitza com una plataforma de col·laboració per a una associació o una empresa.
- En segon lloc, segons el Grup, quan l'accés a la informació del perfil va més enllà dels contactes escollits, en particular, quan tots els membres que pertanyen al servei de xarxa social poden accedir a un perfil o quan les dades són indexables pels motors de cerca, l'accés sobrepassa l'àmbit personal o domèstic. De la mateixa manera, si una persona usuària decideix, amb perfecte coneixement de causa, ampliar l'accés més enllà dels “amics” escollits, assumeix les responsabilitats d'un responsable del tractament de dades. A la pràctica, s'aplica aleshores el mateix règim jurídic que quan una persona utilitza altres plataformes tecnològiques per publicar dades personals a internet.
- A l'últim, es planteja no aplicar l'excepció domèstica quan es tractin dades de terceres persones sense el seu coneixement i/o consentiment, particularment quan es tracti de dades protegides especialment.

Finalment, el Grup de Treball recorda que hi pot haver casos en què l'exempció domèstica no s'apliqui, però hi prevalguin drets com la llibertat d'expressió, el dret a la informació o les llibertats de creació artística o literària. De la mateixa manera,

tampoc no exclou l'aplicació de les disposicions generals del dret civil o penal nacional.

2.2.3 Aportacions de l'Agència Espanyola de Protecció de Dades

L'autoritat espanyola ha desenvolupat diverses accions en aquest àmbit promocionant i participant en estudis,²⁰ emetent informes o actuant en aplicació del règim sancionador. Cal destacar els documents que d'alguna manera contribueixen a definir una posició de la institució en aquesta matèria. En aquest sentit, cal llegir atentament les *Recomendaciones a usuarios de internet 2009*. Aquest document apunta un canvi d'òptica interessant. En edicions anteriors es concebia la persona usuària com un subjecte passiu, les dades de la qual eren objecte de tractament. No obstant això, les recomanacions que contenen els punts X i XI del document apunten un nou enfocament. En primer lloc, es parteix de la base que un ús normal dels recursos del Web 2.0 pot determinar tractaments de dades i d'imatges de persones que no els han consentit i recomana posar-hi una cura especial.²¹

D'altra banda, el document considera també els internautes que conscientment utilitzen els recursos del Web 2.0 amb finalitats informatives i, referent a això, les *Recomendaciones* de l'epígraf dotzè són molt concretes i apunten clarament en la línia de conscienciar la persona usuària sobre les condicions d'exercici del dret a la informació a internet.²²

A més d'aquesta activitat promocional, l'Agència ha adoptat decisions amb transcendència jurídica per tal com els seus informes i resolucions serveixen per orientar l'actuació dels prescriptors. Així, s'ha emès un informe sobre aquesta matèria, el 615/2008,²³ relatiu a una cosa tan comuna com l'actuació d'uns particulars que comparteixen, utilitzant per a això les seves pàgines web, fotos dels seus fills realitzant activitats extraescolars.

L'informe analitza, en primer lloc, si s'hi donen les condicions d'aplicació de l'excepció domèstica. En relació amb aquest aspecte, apunta dues conclusions. La primera, amb referència del cas Bodil Lindqvist, és que no s'hi aplica aquesta excepció perquè no ens trobem en l'àmbit de la vida privada o familiar dels particulars quan la publicació de la informació es projecta més enllà de l'àmbit domèstic, cosa que amb les imatges a internet es constata per tal com "no existe una limitación de acceso a las mismas". Un segon criteri, coherent amb el del Dictamen 5/2009 esmentat més amunt, a l'hora de considerar quins indicis apunten l'existència d'un tractament sotmès a la Directiva, conclou que "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.

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 conclusió, la configuració de l'espai web és molt rellevant a l'efecte de determinar l'aplicabilitat de la legislació sobre protecció de dades.

A l'últim, cal que ens referim a diferents resolucions dictades en el marc de procediments sancionadors i/o tuteles de drets que afecten serveis propis del Web 2.0. En primer lloc, s'han plantejat supòsits d'emissió d'imatges en portals que serveixen arxius de vídeo. En aquest àmbit, l'Agència Espanyola de Protecció de Dades s'ha servit de la doctrina de l'article 29 del Dictamen 4/2004, d'11 de febrer, del Grup de treball relatiu al tractament de dades personals mitjançant vigilància per video-càmera, i ha conclòs que "los datos constituidos por imagen y sonido son personales". El caràcter identificable d'aquestes dades "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 d'aquesta premissa es conclou 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

Aquest plantejament s'ha matisat i s'ha adaptat a la realitat d'internet tot apostant per prioritzar l'exercici de drets de cancel·lació com a mètode per resoldre conflictes i reservant l'aparell sancionador per als supòsits més greus.²⁵

2.3 Recomanacions d'actuació

A la vista dels plantejaments de tribunals i d'autoritats de protecció de dades personals, una primera conclusió sembla evident: un mitjà de comunicació que obri un espai a Facebook està obligat a complir alguns principis normatius bàsics en aquesta matèria.

Estudiats sis dels principals mitjans de comunicació,²⁶ i llevat d'error dels autors, resulta que només un d'aquests mitjans –la cadena SER– disposa d'algun tipus de regles²⁷ per als seus usuaris:

“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, cínete 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 dades personals, 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”.

Com es pot apreciar, es tracta de polítiques d'ús pròpies d'un fòrum i només una al·ludeix vagament a la protecció de dades personals.

No obstant això, si consultem l'espai de l'Agència Espanyola de Protecció de Dades²⁹ generat amb motiu de la celebració d'una conferència internacional, podem llegir-hi la informació següent:

“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 què respon aquesta diferència significativa? És evident que, en el moment en què una empresa actua en una xarxa social està obligada a complir amb les previsions del dret vigent.³⁰

Es poden diferenciar diversos escenaris, encara que el més comú consisteix a registrar un usuari o usuària en els espais més utilitzats, és a dir, Facebook, Tuenti, Twitter i, eventualment, YouTube. En aquest cas es tracta d'una situació híbrida, ja que, per una banda, s'actua com un usuari o usuària més de la xarxa social i, per l'altra, s'assumeixen responsabilitats jurídiques per l'actuació que es desenvolupa. Així, quan s'obre un espai en una xarxa social, l'organització actuarà com el que l'Agència Espanyola de Protecció de Dades i la jurisprudència han definit com a *responsable* d'un tractament:

“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

Com a conseqüència de la sentència esmentada, l'article 5 del Reial Decret 1720/2007, de 21 de desembre, pel qual s'aprova el Reglament de desenvolupament de la Llei Orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal (RLOPD), ha definit aquesta figura com:

“q. Responsable del fitxer o del tractament: persona física o jurídica, de naturalesa pública o privada, o òrgan administratiu, que sol o conjuntament amb altres decideixi sobre

la finalitat, contingut i ús del tractament, encara que no ho realitzi materialment.

També poden ser responsables del fitxer o del tractament els ens sense personalitat jurídica que actuen en el tràfic com a subjectes diferenciats.”

Per tant, es dona aquí la circumstància definida en la sentència i en el precepte. Es tracta d'un tractament en què la persona usuària que obre el seu compte no té cap control sobre el fitxer titularitat de la xarxa social. Per això, les obligacions que es deriven per a l'organització en matèria de compliment de la LOPD resulten limitades i, per exemple, no hi ha deure d'inscriure un fitxer ni de formalitzar un contracte d'accés a dades per compte de terceres persones.

Cal partir de la base que en aquest tipus de supòsits l'ús es limita exclusivament a l'alta en la xarxa social i a la utilització de les eines que hi existeixen i no hi ha cap capacitat de decidir sobre l'estructura, l'ordenació o la gestió material de les dades diferent de la pròpia de la xarxa social. Per poder afirmar que s'actua com una persona usuària més s'hi haurien de donar, a més, altres condicions:

- Comportar-se com una persona usuària que interactua en el sistema de xarxa social.
- No incorporar dades personals a recursos propis.
- No contractar cap prestació de serveis per al desenvolupament o el manteniment de l'espai amb el proveïdor de la xarxa social.
- No pactar serveis addicionals amb el proveïdor, com ara l'anàlisi del comportament, el seguiment o l'elaboració de perfils de persona usuària, associats o no, a l'emissió de publicitat comportamental.³²

En aquest cas, per garantir un compliment adequat de la LOPD, el mitjà de comunicació hauria de:

- Complir amb el deure d'informació, perquè, ja que hi ha un tractament, s'han de respectar els principis i les obligacions derivats de l'article 5 de la LOPD. Per això, resulta recomanable:
 - Ubicar una informació breu en l'espai del compte que faciliti la xarxa social amb la informació bàsica sobre la identitat i la localització de la persona responsable, la finalitat que es persegueix i les formes d'exercir els drets.
 - Articular un procediment de benvinguda a nous amics amb un missatge de correu electrònic que inclogui aquesta informació.
 - Hiperenllaçar a polítiques de privacitat corporatives.

I, com assenyala el Grup de l'article 29 en el Dictamen 5/2009 esmentat més amunt, informar en particular sobre:

- La utilització de les dades amb finalitats de comercialització directa.
- La possible distribució de dades a categories específiques de terceres persones.

- L'ús de dades sensibles.
- La integració en l'entorn d'aplicacions de terceres persones que captin i/o tractin les dades dels “amics” quan aquesta integració depengui de la voluntat de la persona usuària responsable del compte.

En segon lloc, cal assenyalar que la causa que legitima el tractament de les dades personals en aquest àmbit és el consentiment de l'article 6 de la LOPD.³³ Cal entendre que aquest consentiment es manifesta quan es demana “fer-se amic de” o quan s'accepta una invitació. Cal tenir en compte que:

- El consentiment únicament afecta les dades de la persona que s'hi agrega, mai les de terceres persones relacionades amb “l'amic” el perfil del qual estigui obert.
- La possible existència d'excepcions a la regla del consentiment s'han d'examinar cas per cas i amb ple respecte a la regulació. Petició?
- Un perfil obert “no implica consentiment”. Cal recordar que, d'acord amb el que assenyala l'Agència Espanyola de Protecció de Dades en el seu Informe 0342/2008, internet, i per això les xarxes socials, no són fonts accessibles al públic.
- La incorporació de dades, com ara l'adreça de correu electrònic, als propis sistemes constitueix un tractament subjecte a la LOPD i el fet que siguin accessibles en un entorn de xarxa social no és necessàriament una causa que en legítimi el tractament.
- La garantia dels drets dels “amics” té un contingut limitat. Regeixen els drets d'accés, de rectificació, de cancel·lació i d'oposició al tractament. No obstant això:
 - El contingut del dret d'accés es definirà per les possibilitats que ofereixi la xarxa i per la capacitat d'accés a informació del perfil de cada persona usuària concreta. Per tant, pràcticament n'hi haurà prou a oferir, a qui exerceixi el dret, les captures de pantalla en què es mostri a quines dades s'accedeix.
 - El dret d'oposició, de rectificació i de cancel·lació estarà modulats. La persona responsable del tractament hauria de satisfer-lo sobre aquells aspectes de l'aplicació que es trobin sota el seu control, com ara modificar o eliminar un comentari del propi mur. La rectificació d'aspectes relatius al perfil de la persona usuària normalment s'exerceixen davant la persona proveïdora. La cancel·lació o l'oposició, quan consisteix a “deixar de ser amics”, es podria exercir per totes dues parts.
- Hi ha d'haver límits quant a l'ús de les dades. El principi de finalitat constitueix un límit infranquejable i s'ha de definir per:
 - Les condicions d'ús de la xarxa social, que podria prohibir usos concrets.
 - La informació disponible i facilitada efectivament “en fer-se amics”.
- Regeixen els principis de seguretat i de secret per a qual-

sevol persona usuària del responsable del tractament, però s'han d'adaptar a les condicions pròpies de l'entorn i afectar-
ran únicament els tractaments realitzats efectivament.

3. Opinió i informació dels usuaris d'una xarxa social

Per finalitzar amb l'examen de les qüestions relacionades amb l'ús de xarxes socials, cal examinar el que sens dubte és l'objectiu essencial d'aquests espais: afavorir que els seus usuaris manifestin la seva opinió lliurement.

En principi, i atesa la naturalesa de l'entorn, és a dir, un espai d'un mitjà de comunicació vinculat a l'exercici ciutadà dels drets de l'article 20 de la Constitució espanyola, es donen condicions per excloure l'aplicació de les normes sobre protecció de dades personals.³⁴ En aquest sentit, habitualment, l'Agència Espanyola de Protecció de Dades ha reconegut la prevalença dels drets de l'article 20 de la CE.³⁵ No obstant això, cal assenyalar que, almenys en un cas, l'Audiència Nacional ha considerat prevalent el dret a la protecció de dades, quan va considerar que la informació publicada no requeria de l'acompanyament de la imatge d'una de les víctimes de l'11-M i hi va aplicar un judici de proporcionalitat.³⁶

Quan qui tracta dades personals és una persona usuària al seu propi mur, l'Agència acostuma a reconduir la qüestió al procediment de tutela de drets de l'article 18 de la LOPD i ordena la cancel·lació de les dades a la persona responsable de la xarxa social.³⁷

Tots els criteris exposats permeten aproximar-nos a la naturalesa jurídica de les opinions abocades al mur d'un mitjà de comunicació basada en dues categories de judici. En primer lloc, un judici sobre el contingut permetrà determinar si la persona usuària hi exerceix el seu dret a informar o a expressar la seva opinió i s'hi donen les condicions de prevalença d'aquest dret respecte dels drets de terceres persones. És a dir, que la informació es basi en fets certs, o percebuts com a tals, i tinguin rellevància pública per conformar l'opinió pública.

El segon criteri d'aproximació es basa en la determinació de la responsabilitat de la persona titular del mur. Aquí el punt de vista de l'Agència s'emmarca en la línia que defineix la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, i que apunta el Dictamen 5/ 2009, de considerar la persona titular d'una xarxa social com a proveïdora de serveis de la societat de la informació.

Es dona aquí una diferència substancial amb la responsabilitat de la persona editora, per exemple, en les tradicionals cartes al director. La STC 3/1997 sintetitza de manera molt precisa el criteri del tribunal, que, partint del fet de l'existència d'un examen previ de les cartes que publica, requereix d'alguna manera l'aplicació d'un doble filtre sobre la identitat de la persona remitent i sobre la rellevància del contingut quan la identificació no sigui fiable. Per això, considera la persona editora responsable d'aquests continguts.³⁸

En resum, i utilitzant un raonament analògic elemental, en aquells espais d'internet en què els continguts són directament desenvolupats per la persona titular i s'hi deixa un espai a la participació, la responsabilitat se centraria a verificar la identitat del lector o lectora que publica la seva opinió. Aquesta doctrina seria inaplicable en el context d'una xarxa social, ja que la seva manera de funcionar impedeix avui dia qualsevol identificació i, a més, la celeritat a l'hora de publicar comentaris i el nombre d'aquests comentaris en fa impossible el control, si no és a posteriori.

Per això, com assenyala el Dictamen 5/2009, en aquest cas es tracta de la prestació d'un servei de la societat de la informació subjecte al que disposa la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic (LSSI). Per tant, quan sigui aplicable la legislació espanyola, la responsabilitat de la persona proveïdora, pel que fa a aquest document, s'ha de regir pels articles 16 i 17 de la LSSI. Per tant, cal la concurrència de dos elements perquè existeixi responsabilitat:

- Coneixement efectiu. Es produirà quan es notifiqui la reclamació per mitjà de l'espai de denúncies de la xarxa social o quan una autoritat, com l'AEPD, requereixi algun tipus d'actuació.
- Absència de diligència en la retirada de la informació.

En qualsevol cas, es tracta d'una realitat complexa que trasllada una certa responsabilitat ètica als mitjans. Com que s'ha produït una democratització mitjançant l'extensió de la possibilitat d'exercir la llibertat d'opinió a qualsevol ciutadà, i ja que els mateixos mitjans faciliten aquests espais a les xarxes socials, seria molt aconsellable que promoguessin la formació dels usuaris mitjançant codis ètics o regles d'ús.³⁹

Això és particularment necessari en un context d'absència d'una normativitat específica. Ni la Llei orgànica 1/1982, de 5 de maig, de protecció civil del dret a l'honor, a la intimitat personal i familiar i a la pròpia imatge, ni la Llei orgànica 2/1984, de 26 de març, reguladora del dret de rectificació, ofereixen solucions adequades per resoldre aquests problemes. Bona prova d'això és que cada cop més sovint el ciutadà o ciutadana exerceix el dret de cancel·lació de l'article 16 de la LOPD en aquest tipus de supòsits.

Els conflictes en aquesta matèria superen de molt les xarxes socials i s'estenen al periodisme ciutadà i als blocs, i a l'anomenat *dret a l'oblit*. La Directiva 95/46/CE facultava els estats membres per desenvolupar aquesta matèria en l'àmbit dels mitjans de comunicació. Potser ha arribat el moment d'afirmar que aquest desenvolupament resulta indispensable.

Notes

1. Aquest article és, en gran mesura, deutor d'una monografia prèvia. RALLO LOMBARTE, A.; MARTÍNEZ MARTÍNEZ, R. (coord.). *Derecho y redes sociales*. Cizur Menor (Navarra): Civitas, 2010.
2. CEREZO, J.M. *La blogosfera hispana: pioneros de la cultura digital* [En línia]. Biblioteca de la Fundación France Telecom España, 2006. <http://fundacionorange.es/areas/25_publicaciones/publi_253_9.asp> (Disp. 19/03/2010).
3. Molt gràficament, Castells assenyalava:
 "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, p. 139. Per entendre la capacitat de les xarxes per definir espais de comunitat, resulta particularment interessant el capítol dedicat a aquest treball a les comunitats virtuals (p. 137-158).
4. Vegeu <<http://twitter.com/>>
5. Vegeu MARTÍNEZ MARTÍNEZ, R. "¿Interrogantes jurídicos ante los smartphone?". *Actualidad Jurídica Aranzadi*, núm. 822, p. 13.
6. Vegeu <<http://www.theinternetofthings.eu/>>
7. Quan de la mà de la televisió digital terrestre es produeixi una veritable interactivitat es multiplicaran els tractaments de dades personals mitjançant aquest canal. MARTÍNEZ MARTÍNEZ, R. "Los contenidos audiovisuales en la multidifusión digital. Nuevos retos para la protección de datos personales". A: FRANCÉS I DOMENECH, M. (coord.). *Hacia un nuevo modelo televisivo. Contenidos para la televisión digital*. Barcelona: Gedisa, 2009, p. 83-95.
8. Resulten particularment rellevants en aquest sentit les troballes de l'autoritat canadense de protecció de dades en les indagacions realitzades respecte de 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. *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIP-PIC) 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), p. 38 i 94.
9. Vegeu <<http://www.maestrosdelweb.com/editorial/web2/>>
 10. Vegeu ALAMILLO DOMINGO, I. "La identidad electrónica en la red". A: RALLO LOMBARTE, A.; MARTÍNEZ MARTÍNEZ, R. (coord.). *Derecho y redes sociales*. op. cit. p. 37-53.
 11. Vegeu SCHWARTZ, P.M. "Internet privacy and the State". *Connecticut Law Review*, vol. 32, 2000, p. 815-859.
 12. De fet, aquesta és l'aposta més recent de Google amb la seva xarxa 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. Davant els que afirmen la impossibilitat de delimitar jurídicament el fenomen d'internet, i sense deixar de ser conscients de la necessitat d'actuacions concretes del legislador, cal considerar que en el context de les tecnologies de la informació i de les comunicacions sigui necessari modular-ne o adaptar-ne l'ordenament, ja que, en l'àmbit d'internet, la normativitat no es projecta sobre els instruments, sinó sobre el seu ús i sobre el seu disseny. Vegeu TRIAS SAGNIER, J. "Informática y privacidad. ¿Se pueden poner puertas al campo?" *Cuenta y razón*, núm. 63, 1992, p. 98-101.
 14. En aquesta línia, en els darrers anys s'ha aprofundit en les metodologies del *Privacy Impact Assessment* i del *Privacy by Design*, el plantejament dels quals és coincident amb el que s'assenyala aquí: els proveïdors i els programadors han de tenir en compte en el seu disseny, de manera apriorística, mètodes que garanteixin el respecte del dret a la vida privada dels usuaris.
 Com ha assenyalat Lessig, el programador té la capacitat

de definir regles de funcionament de l'entorn que actuen de manera materialment normativa i, per tant, la possibilitat de definir modes de funcionament que garanteixin el compliment dels principis que l'ordenament jurídic incorpora. LESSIG, L. *El codi i altres lleis del ciberespai*. Madrid: Taurus, 2001 i LESSIG, L. *Code versió 2.0*. Basic Books. Nova York: Perseus Books Group, 2006. Disponible a:

<<http://pdf.codev2.cc/Lessig-Codev2.pdf>>

En aquesta matèria, els documents són cada vegada més abundants, si bé la metodologia de referència és la de la Information Commissioner's Office britànica.

- 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 (EUA) *Privacy Impact Assessment EINSTEIN Program*. <http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_einstein.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/>.

A l'últim, vegeu 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. Com es recordarà, la senyora Lindqvist era una catequista sueca que, al final del 1998, va crear amb el seu ordinador personal diverses pàgines web amb la finalitat que els feligresos de la parròquia que es preparaven per a la confirmació poguessin obtenir fàcilment la informació que pogués resultar útil. Aquestes pàgines contenien informació sobre la senyora Lindqvist i divuit dels seus companys de la parròquia, incloent-hi el nom de pila, acompanyat, de vegades, del nom complet. A més, la senyora Lindqvist descrivia en un to lleugerament humorístic les funcions que exercien els seus companys, així com les seves aficions. En diversos casos se n'esmentava la situació familiar, el número de telèfon i informació addicional. Així mateix, va assenyalar que una de les seves companyes s'havia lesionat un peu i que es trobava en situació de baixa parcial per malaltia. Després de ser sancionada i de recórrer, el tribunal suec va consultar al Tribunal de Justícia sobre les condicions d'aplicació de la Directiva 95/46/CE.

Sentència del Tribunal de Justícia de 6 de novembre de 2003 a l'assumpte C-101/01. Petició de decisió prejudicial plantejada pel Göta Hovrätt. <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2004:007:0003:0004:ES:PDF>>

16. Les normes de protecció de dades personals no s'apliquen, com assenyala l'article 4 del RLOPD, als tractaments "realitzats o mantinguts per persones físiques en l'exercici d'activitats exclusivament personals o domèstiques.

Només es consideren relacionats amb activitats personals o domèstiques els tractaments relatius a les activitats que s'inscriuen en el marc de la vida privada o familiar dels particulars".

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 d'octubre, relativa a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades.

<http://europa.eu/legislation_summaries/information_society/data_protection/114012_es.htm>

19. El Grup ha assenyalat que hi ha tractaments que no es podrien dur a terme sense recórrer a l'ús del propi ordinador de la persona usuària, en general mitjançant l'explotació de *cookies*, de manera que s'estarien utilitzant mitjans en territori europeu. Vegeu WP148, Dictamen 1/2008 sobre assumptes relatius a la protecció de dades vinculades a les eines de cerca.

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 les persones usuàries s'hi orienten dues recomanacions específiques:

- "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."

I un recordatori:

- "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_aXKiMJkT_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. Vegeu 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. Vegeu PS/00479/2008, disponible a 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”. Vegeu 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. Vegeu VILASAU SOLANA, M. “Privacidad, redes sociales y el factor humano”. A: RALLO LOMBARTE, A.; MARTÍNEZ MARTÍNEZ, R. (coord.). *Derecho y redes sociales*. op. cit. p. 66-71.

31. Vegeu la Sentència de 5 de juny de 2004, de la Sala Tercera Contenciosa Administrativa del Tribunal Suprem, sobre diferenciació entre el responsable del fitxer i el responsable del tractament, que confirma la Sentència de 16 d'octubre de 2003 de la Secció Primera de la Sala Contenciosa Administrativa de l'Audiència Nacional, dictada en el recurs número 1539/2001. Disponible a: <http://bit.ly/oDvST6>.

32. La publicitat comportamental es basa en l'observació continuada del comportament dels individus. Cerca estudiar les característiques d'aquest comportament per mitjà de les seves accions (visites repetides a un lloc concret, interaccions, paraules clau, producció de continguts en línia, etc.) per desenvolupar un perfil específic i proporcionar així als usuaris anuncis a mida dels interessos inferits del seu comportament. La publicitat comportamental implica normalment la recollida d'adreces IP i el tractament d'identificadors únics (mitjançant les *cookies*). La utilització d'aquests dispositius permet aïllar els usuaris, encara que se'n desconeixin els noms veritables. A més, la informació recollida es refereix a característiques o comportament d'una persona i s'utilitza per influir en aquesta persona concreta. Aquest perfil s'accentua quan es té en compte la possibilitat que els perfils es vinculin en tot moment amb informació directament identificable proporcionada pels usuaris, com ara la informació aportada en el registre.

Cal tenir en compte que aquí es defineix una possibilitat tecnològicament disponible. Correspon a editors, anunciants i proveïdors de serveis de publicitat la decisió d'utilitzar aquestes tècniques.

Vegeu GRUPO DE TRABAJO DEL ARTÍCULO 29. *Dictamen 2/2010 sobre publicidad comportamental en línea*. 00909/10/ES GT 171, disponible a <http://bit.ly/dsAN9F>, i PEGUERA POCH, M. “Publicidad online basada en comportamiento y protección de la privacidad”. A: RALLO LOMBARTE, A.; MARTÍNEZ MARTÍNEZ, R. (coord.). *Derecho y redes sociales*. op. cit. p. 354-380.

33. Vegeu, ARENAS RAMIRO, M. “El consentimiento en las redes sociales on line”. A: RALLO LOMBARTE, A.; MARTÍNEZ MARTÍNEZ, R. (coord.). *Derecho y redes sociales*. op. cit. p. 117-144.

34. Una altra cosa seria l'ús indegut de dades personals per part dels usuaris de xarxes socials en els seus propis murs, que podria determinar en alguns casos responsabilitats en matèria de protecció de dades personals. Per exemple, mitjançant la publicació d'imatges o de comentaris amb dades personals en un entorn privat de xarxa social sense el consentiment de les persones afectades.

35. Vegeu l'expedient núm. 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". Sentència de 9 de juliol de 2009, de la Secció Primera de la Sala Contenciosa Administrativa de l'Audiència Nacional, dictada en el recurs número 325/2008.

37. Vegeu el procediment núm. TD/00690/2009. Disponible a <<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 7º.,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. Vegeu 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, p. 92.