InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

# Am I in Facebook?

Sobre la responsabilidad civil de las redes sociales *on-line* por la lesión de los derechos de la personalidad, en particular por usos no consentidos de la imagen de un sujeto

Ana Soler Presas

Facultad de Derecho
Universidad Pontificia Comillas (ICAI-ICADE)

BARCELONA, JULIO 2011

## *Abstract*[*]

*Las redes sociales on-line son las protagonistas indiscutibles de la web 2.0. El auge de su negocio se debe, entre otras razones, al limbo legal que disfrutan y que les ha permitido desplazar riesgos propios al usuario de estos servicios. El presente trabajo define cuál es el alcance de la responsabilidad contractual de estos servicios en casos de daño a la imagen o intimidad de sus usuarios, y enfatiza la eficacia que el cumplimiento de estos deberes contractuales puede tener en la protección de los intereses de privacidad e imagen de terceros.*

*Online social networks are undoubtedly the main character in web 2.0., partly because of the uncertainty about their legal regime, which enables them to outsource relevant costs. This paper defines the scope of their contractual duty relating the privacy and image of the users of such services and emphasizes the role that the performance of these duties would play in the protection of non-users privacy and image's interests.*


*Title:* Am I in Facebook?

*Palabras clave:* redes sociales electrónicas, intimidad, derecho a la propia imagen, responsabilidad civil
*Keywords:* Social Network Sites, Privacy, Right to One's Own Image, Damages

## *Sumario*



---

[*] El presente trabajo se ha podido realizar gracias al detallado trabajo de campo de Guillermo Beltrán Rodríguez, alumno de excelencia del programa E-3 de la Universidad Pontificia Comillas- Icade. He intentado pulirlo atendiendo a la crítica, siempre constructiva, de los profesores Fernando Pantaleón Prieto y Jesús Alfaro Águila-Real, a quienes debo gratitud eterna. El resultado, pese a todo defectuoso, es obra mía.

Esta propuesta se realiza en el marco del Proyecto de Investigación (DER 2009-12356) "Cómo repensar la responsabilidad extracontractual objetiva" financiado por el Ministerio de Ciencia e Innovación.

*Para Santi, un sol.*

## *1. Introducción*

El título del trabajo que presento no es más que una variación sobre el lema impreso en una tarjeta postal que llamó mi atención en la primavera de 2010. La tarjeta, con otro diseño de texto, decía: "I'm NOT in Facebook". La afirmación, rotunda, denotaba la rebeldía de su creador frente a la presión que muchos de nosotros sentimos ante el uso, ya masivo, de los servicios de redes sociales *on-line*.

Estuve tentada de comprarla, para exhibirla en mi despacho; pero dudé: ¿puedo (puede alguien) afirmar que no está en Facebook, Tuenti, o cualquier otra red social electrónica?[1] Obviamente, no; y el interrogante siguiente va de suyo ¿tengo derecho a saberlo y a decidir, en su caso, si mis fotos o información privada se muestran y en qué contexto? Intentar responderlo es el objeto del presente trabajo, y para ello partiremos de la definición del llamado servicio de red social, y explicaremos su diferencia estructural respecto de los servicios de acceso, enlace y almacenamiento propios de la web 1.0. [apartado 2]. Estudiaremos cómo afrontan las redes más difundidas (Facebook/Tuenti) la protección de la privacidad, de sus usuarios y de los que no lo somos [apartado 3], así como el significado que tiene este concepto para los adeptos al servicio [apartado 4]. Continuaremos analizando en qué casos los servicios de red social podrían ser responsables civiles por los daños derivados de la intromisión en la intimidad de un sujeto, típicamente cometida por algún otro usuario de la red; y cómo sería la citada responsabilidad: si objetiva, por el mero hecho de facilitar y lucrarse con el medio empleado para infligir la afrenta; o subjetiva, por la omisión de las medidas razonables de prevención y/o mitigación de este tipo de conductas [apartado 5]. Y concluiremos el trabajo desarrollando cómo puede protegerse la imagen de los usuarios del servicio y de terceros en este contexto [apartado 6].

## *2. Concepto de servicio de red social on-line*

La definición de *Social Network Site* (SNS)[2] más extendida es la aportada por boyd:

---

[1] Centramos el estudio en Facebook y Tuenti por ser, de largo (más de 8 millones de usuarios cada una), las más populares en nuestro país. Y distinguiremos poco el análisis entre ellos porque, aunque son servicios diferentes (Facebook está abierto a todo el que cuente con una cuenta de correo electrónico, también a empresas e instituciones; Tuenti prefiere el sistema "por invitación" de otro usuario y no permite perfiles de personas jurídicas) los problemas de privacidad que generan a sus usuarios y a terceros son prácticamente idénticos. Las invitaciones, por cierto, pueden obtenerse fácilmente en internet. Las condiciones de uso y políticas de privacidad de ambos servicios se consultaron por última vez el 23.5.2011.

[2] Utilizamos el acrónimo del término *Social Network Site* porque es el comúnmente usado por las bases de datos y bibliotecas electrónicas para referirse al servicio.

"Los servicios de redes sociales *on-line* son servicios web que permiten a los individuos (1) construir un perfil público o semipúblico partiendo de un modelo de formulario determinado (2) articular una lista de usuarios con los que se va a compartir conexión y (3) visualizar y navegar a través de esa lista de conexiones y de otras establecidas por otros usuarios del sistema" [3].

La definición destaca los tres elementos esenciales del servicio: permite al usuario presentar y construir su identidad virtual; relacionarse con otros afines en algún aspecto; y reproducir, consolidar y/o extender su red social *off-line* creando una comunidad virtual.

Bien observado, es el producto nuclear de la web 2.0, de la internet interactiva en la que el usuario no (sólo) busca información, sino fundamentalmente ofrece contenidos.

Tienen un valor social indudable, especialmente para los jóvenes, pues les permite "construir" su personalidad[4], profundizar en las relaciones sociales ya adquiridas y ampliar los límites de su red social conectando con otros que tengan intereses similares[5].

Esta conceptualización destaca ya las diferencias entre las SNS y los pioneros proveedores de servicios de internet (en adelante, ISP)[6]: su negocio era la mera intermediación, la provisión de la tecnología precisa para que la comunicación fluyera. Eran ajenos a unos contenidos (buscados, enlazados, descargados) que no les aportaban nada y que sólo ante la presión de la autoridad de

---

[3] "Social network sites are web-based services that allow individuals to:

(1) construct a public or semi-public profile within a bounded system

(2) articulate a list of other users with whom they share a connection and

(3) view and travers their list of connections and those made by others within the system."

boyd & ELLISON (2007), http:/jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. La primera se cita en minúscula porque así lo desea ella. Puede seguírsela en su blog: http://www.zephoria.org/thoughts/.

[4] Los adolescentes en el entorno digital están ocupados "writing their selves into being", dice la gurú en la materia boyd (2006) http://www.firstmonday.org/issues/issue11_12/boyd/index.html.

[5] Aunque les permite más cosas, es importante destacar que estos servicios se usan fundamentalmente para conectar y relacionarse con el círculo de amigos preexistente. Si aquí repitiéramos la pregunta con la que los sociólogos americanos comenzaron sus estudios sobre el uso de estas tecnologías (¿por qué usan los jóvenes las redes sociales *on-line*?) la respuesta sería la misma:"cuz there's where my friends are!" Hagan la prueba y consúlten GRIMMELMANN (2009, p. 1157). Para los que no se conformen con test caseros, hay estudios empíricos que demuestran esta interrelación en Facebook: véase ZHAO, GRASMUCK & MARTIN (2008, pp. 1816-1836); DEBATIN *et al*. (2009, pp. 83-108); HULL, LIPFORD & LATULIPE (2010, pp. 6-11). Para Tuenti es la razón de ser del servicio, al que se accede "por invitación" de un amigo.

[6] De nuevo utilizamos el acrónimo del término inglés *Internet Service Provider*.

policía, accedieron a conservar[7].

El negocio de las SNS es muy diferente. No cobran por la tecnología que ofrecen para la interconexión entre usuarios. Tampoco por las aplicaciones, propias o ajenas, que facilitan para que la comunicación sea más rica. Su negocio está en los datos, propios o de terceros, que los usuarios facilitan; en el uso lucrativo que pueden obtener de ellos. Para que su extracción, análisis, segmentación y uso productivo sea posible, obligan a una presentación o vertido estandarizado[8], se asegura de que sean reales;[9] y anima a compartir cuanta más información, de uno mismo y de los demás, mejor. Y los guarda, claro, aunque el titular de los mismos quiera darse de baja en el servicio[10].

Luego su negocio depende del volumen de datos que contenga la red, por lo que necesita predisponer al usuario para que vuelque contenidos.

En este empeño es esencial crear la ilusión de que se expresa un entorno privado, de confianza, íntimo. Así, el uso de datos reales y la foto en el interfaz generan la sensación de interacción

---

[7] Su excepcional posicionamiento para la persecución del crimen organizado lo explican con detalle NIETO MARTÍN y MAROTO CALATAYUD (2010, pp. 208 y ss.).

[8] Convirtiéndose así en enormes bases de datos, cada vez más eficientes en tanto que mejor organizada esté la información. Esta estandarización explica, también, que Facebook haya desbancado a MySpace.

[9] De otra forma no interesarían. Y, aunque no sería precisa esta insistencia en la necesidad de aportar datos reales, pues la misma razón por la que nos damos de alta en el servicio (conectar con nuestros amigos) incentiva que los aportemos para que puedan localizarnos, obstaculizan cualquier tentativa de simulación, amenazando con la cancelación del perfil si es descubierta y exigiendo direcciones de *email* asociadas a instituciones (educativas, laborales o de cualquier otro tipo) para integrarte en sus subredes.

i.e., en Tuenti: *El acceso al Servicio implica necesariamente que debes facilitar a TUENTI una serie de datos de carácter personal y, por tanto, consentir nuestra Política de Privacidad y Protección de Datos. Queda prohibido el suministro de datos falsos, por tanto, debes identificarte siempre con tu nombre real y con datos correctos. Si TUENTI detecta datos falsos o incorrectos en los perfiles podrá cancelarlo, de acuerdo con lo previsto en estas Condiciones de uso.*

[10] Porque a lo sumo da de baja su perfil, pero los datos que estén indexados en buscadores ahí quedan, como los que guarden del mismo los contactos del ex-usuario y los operadores de las aplicaciones que se haya descargado. Política de privacidad de Facebook: Limitaciones sobre la eliminación. *Incluso después de eliminar información de tu perfil o eliminar tu cuenta, pueden permanecer copias de dicha información visibles en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de la privacidad, o haya sido copiada o almacenada por otros usuarios. Sin embargo, tu nombre dejará de estar asociado con dicha información en Facebook. (Por ejemplo, si publicas algo en el perfil de otro usuario y después eliminas tu cuenta, dicha publicación podría permanecer, pero atribuirse a un "Usuario de Facebook anónimo.") Asimismo, podemos conservar cierta información para evitar el robo de identidades y otras conductas inadecuadas, incluso si se ha solicitado la eliminación. Si has facilitado a aplicaciones o sitios web de terceros acceso a tu información, éstos pueden conservar tu información hasta el límite permitido por sus condiciones de servicio o políticas de privacidad. Sin embargo, después de desconectarte de ellos, ya no podrán acceder a la información a través de nuestra plataforma.*

personal y directa con sus amigos; las relaciones se estructuran para estimular una comunicación permanente entre ellos[11]; y se sugiere que esta interacción está blindada: empleando términos de grafismo inequívoco ("muro") o indicando que las intromisiones serán excepcionales e imputables a terceros[12].

Crean, en definitiva, un contexto propicio para que se revelen datos que, de otra forma, no se volcarían[13]; y que inevitablemente llegarán a una audiencia mucho mayor que la percibida por el usuario[14].

Pero será cuando el usuario tome conciencia de esta extralimitación cuando se perfile el daño que, muy probablemente, será más grave que el que pueda generarse en abierto en internet, porque aquí la información llega al entorno social que le importa: a aquellos a los que pretendía mantener al margen de esos contenidos porque ante ellos se presenta y comporta de forma diferente.[15]

## *3. ¿Cómo afrontan estos servicios la protección de la privacidad de los usuarios?*

No puede olvidarse que las SNS nacieron en EEUU, luego es el sistema norteamericano de protección de la privacidad el que tienen presente al definir su negocio; el que tratan de preservar, por razones obvias, al extender su negocio fuera de EEUU; y el que copian, finalmente,

---

[11] Con invitaciones para sumarse a grupos o iniciativas, para ser "amigo", con el etiquetado de cualquier cosa con "me gusta", además de facilitando aplicaciones como el *Newsfeed* o *Beacon* de Facebook, que luego explicaremos.

[12] Por ejemplo: Riesgos inherentes a compartir información. Aunque te permitimos definir opciones de privacidad que limiten el acceso a tu información, ten en cuenta que ninguna medida de seguridad es perfecta ni impenetrable. No podemos controlar las acciones de otros usuarios con los que compartas información. No podemos garantizar que sólo vean tu información personas autorizadas. No podemos garantizar que la información que compartas en Facebook no pase a estar disponible públicamente. No somos responsables de que ningún tercero burle cualquier configuración de la privacidad o medidas de seguridad en Facebook. Puedes reducir estos riesgos utilizando hábitos de seguridad de sentido común como elegir una contraseña segura, utilizar contraseñas diferentes para servicios diferentes y emplear software antivirus actualizado.

[13] GRIMMELMANN (2009, pp. 1160-1164) explica muy bien la dinámica de esta sugestión.

[14] Aunque sólo fuera porque el número medio de contactos iniciales, establecidos al darse de alta en la red, ronda los 130, que distan mucho de ser el número de relaciones con las que después interactúa. Pero están ahí, aunque no se recuerden o borrarles sea embarazoso. Sobre estos datos, véase HULL, RICHTER LIPFORD & LATULIPE (2010, pp. 11-12).

[15] La información privada o descontextualizada volcada en abierto (en blogs u otros servicios preexistentes en la web) también puede ser lesiva, claro, pero para ello es preciso que alguien de la pista o clave para encontrarla, y que otro interesado la rastree. En la SNS no hace falta. Al lector interesado le sugiero consultar aquí la polémica entre ROSEN (2000) y POST (2001).

sus competidores.

Pues bien, en este sistema, el norteamericano, la noción de "privacidad" apenas admite matices. Entronca con la libertad que el ordenamiento jurídico reconoce al individuo para decidir, en primera instancia, qué información personal hace pública; pero, una vez publicada, le niega el derecho a controlar su difusión. Entiende que con la libre comunicación de esa información pierdes toda expectativa de privacidad sobre los datos asistiéndote, si acaso, una pretensión para controlar el uso lucrativo que se pueda hacer de ellos[16].

En este contexto al servicio sólo puede exigírsele transparencia respecto de los usos que se les vaya a dar a los datos y una tecnología adecuada para que el usuario pueda decidir, conscientemente, quién ve qué contenidos. La carga de la protección de la privacidad pesa, pues, sobre el usuario de las redes.

Anticipamos al lector que, en ambas tareas, la actuación hasta la fecha de las SNS más conocidas dista mucho de ser satisfactoria[17], pero lo que ahora tratamos de resaltar es que, desde esta perspectiva, si fueran ambas –información y tecnología de control– razonablemente aceptables, cualquier uso lesivo de los datos privados o de la imagen de un sujeto sólo podría imputársele a quien los hizo públicos: a su titular o a un tercero.

Para el negocio de las redes sociales *on-line* no puede haber mejor sistema. Pueden facilitar tecnología para que el usuario establezca *grosso modo* la publicidad que quiere dar a su perfil o contenidos[18]; y añadir los oportunos *disclaimers* que, con la sutileza de reconocer al usuario la

---

[16] Sobre este concepto véase WESTIN (1967), aunque aquí interesan más MARTIN (1998, pp. 801 y ss.); o, para el objeto de nuestro estudio, SÁNCHEZ ABRIL (2007, pp. 73-88).

[17] Porque la información es insuficiente y confusa, máxime la relativa al acceso a los datos, propios y de tus contactos, y del uso que les dan quienes están detrás de las aplicaciones; porque los controles de privacidad se borran periódicamente con la excusa de "reiniciar" el sistema; porque cambian las políticas de privacidad y de uso de los datos sin informar previa y convenientemente a los usuarios, e induciendo su consentimiento a las nuevas reglas por la mera continuación en el uso del servicio; y porque las medidas tecnológicas son, como luego veremos, inadecuadas.

Así, por ejemplo, véase la siguiente cláusula:

"TUENTI se reserva el derecho a su elección exclusiva, de revisar las presentes Condiciones de uso en cualquier momento por razones legales, por motivos técnicos o por cambios en la prestación del Servicio o en la normativa, así como modificaciones que pudieran derivarse de códigos tipo aplicables o, en su caso, por decisiones corporativas estratégicas. Cuando esto ocurra te avisaremos de ello a través del sitio web y si, una vez te hemos informado de ello, continúas utilizando el Servicio, entenderemos que has aceptado las modificaciones introducidas. Si no estuvieras de acuerdo con las modificaciones efectuadas, podrás darte de baja en el servicio siguiendo el procedimiento habilitado para ello".

[18] En la Declaración de Derechos y Responsabilidades de Facebook:

propiedad de los contenidos que suba a la red, dejar claro que es a él al que compete recabar los permisos necesarios y que, consecuentemente, sólo él responde si no los tiene[19].

---

"Privacidad. Tu privacidad es muy importante para nosotros. Hemos diseñado nuestra Política de privacidad para ayudarte a comprender cómo puedes usar Facebook para compartir información con otras personas y cómo recopilamos y usamos tu información. Te animamos a que leas nuestra Política de privacidad y a que la utilices para poder tomar decisiones fundamentadas."

En Tuenti:
"Niveles de privacidad. TUENTI pone a tu disposición niveles de privacidad para garantizar la seguridad de tus datos. De esta manera, serás tú quién, bajo tu exclusiva responsabilidad decidas, por tu cuenta y riesgo, quién tiene acceso a tu información personal.

Como Usuario de TUENTI podrás controlar en todo momento la privacidad de tu perfil y sus diferentes elementos; tus fotos, tu tablón, la recepción de mensajes y/o la visibilidad de tus números de teléfono. A continuación te señalamos cómo controlar tu privacidad en diferentes niveles atendiendo al tipo de contenido y en función de tres categorías. Tú eres el único responsable del nivel de privacidad que elijas."

[19] En las Condiciones de Uso de Tuenti:

"Contenidos de los perfiles de los usuarios

Al publicar contenidos en tu perfil -fotos, archivos, textos, vídeos, sonidos, dibujos, logos o cualquier otro material- conservas todos tus derechos sobre los mismos y otorgas a TUENTI una licencia limitada para reproducir y comunicar públicamente los mismos, para agregarles información y para transformarlos con el objeto de adaptarlos a las necesidades técnicas del Servicio. Esta autorización es mundial, no exclusiva (lo que significa que puedes otorgar otra licencia sobre tu contenido a cualquier persona o entidad, además de a TUENTI), por todo el tiempo que tengas vigente tu perfil y con la única y exclusiva finalidad de que TUENTI pueda prestarte el servicio en los términos explicados en estas Condiciones de uso.

La anterior licencia quedará resuelta una vez que elimines tu contenido del Servicio o des de baja tu perfil. A partir de ese momento, TUENTI interrumpirá la comunicación de tu contenido a la mayor brevedad posible.

En relación con el contenido que publiques en el Servicio, garantizas:

Que eres el propietario o titular de los derechos que te permiten conceder a TUENTI la licencia para su publicación y que, en su caso, has obtenido de terceros el consentimiento necesario para ello.

Que no vulnera leyes aplicables tales como las relativas al derecho a la intimidad, a la imagen y/o al honor, derechos de propiedad intelectual o industrial o similares ni ningún derecho de un tercero, ya sea una persona o una entidad.

Que en caso de publiques datos de carácter personal de alguno de tus amigos o de otra persona, les has informado y obtenido previamente su consentimiento para la publicación de dichos datos.

Por ello, responderás frente a TUENTI de la veracidad de lo afirmado, manteniendo indemne a TUENTI ante cualquier demanda o reclamación presentada por un tercero en relación a las anteriores afirmaciones y en relación a cualquier derecho legítimo sobre el contenido que hayas publicado en el Servicio."

Y tiene el indudable atractivo de no ser paternalista y generar un reto (*you take control*) tan difícil de declinar –especialmente por lo más jóvenes- como imposible de alcanzar.

## *4. ¿Cómo afrontan la privacidad propia y ajena los usuarios de la red?*

Como acabamos de ver, la red social está diseñada para incentivar que el usuario vuelque información personal de sí mismo y de sus relaciones. Y lo hace de forma masiva y, según constatan los estudios empíricos, sin aprovechar exhaustivamente las herramientas de control que el servicio pone a su disposición[20].

Son muchos los académicos que han tratado de explicar este comportamiento, tildado de

---

Y en la Declaración de Derechos y Responsabilidades de Facebook:

"Compartir el contenido y la información. Eres el propietario de todo el contenido y la información que publicas en Facebook.

Luego, Si alguien interpone una demanda contra nosotros relacionada con tus acciones, tu contenido o tu información en Facebook, te encargarás de indemnizarnos y nos librarás de la responsabilidad por todos los posibles daños, pérdidas y gastos de cualquier tipo (incluidos los costes y tasas legales razonables) relacionados con dicha demanda.

Intentamos mantener facebook en funcionamiento, sin errores y seguro, pero lo utilizas bajo tu propia responsabilidad. Proporcionamos facebook "tal cual" sin garantía alguna expresa o implícita, incluidas, de manera enunciativa pero no limitativa, las garantías de comerciabilidad, adecuación a un fin particular y no contravención. No garantizamos que facebook sea seguro. Facebook no se responsabiliza de las acciones, el contenido, la información o los datos de terceros y por la presente nos dispensas a nosotros, nuestros directivos, empleados y agentes de cualquier demanda o daños, conocidos o desconocidos, derivados de o de algún modo relacionados con cualquier demanda que tengas interpuesta contra tales terceros. Si eres residente de california, no se te aplica el código civil de california §154, según el cual: "una renuncia general no incluye las demandas que el acreedor desconoce o no sospecha que existen en su favor en el momento de ejecución de la renuncia, la cual, si fuera conocida por él, deberá haber afectado materialmente a su relación con el deudor". No seremos responsables de ninguna pérdida de beneficios, así como de otros daños resultantes, especiales, indirectos o incidentales derivados de o relacionados con esta declaración de facebook, incluso en el caso de que se haya avisado de la posibilidad de que se produzcan dichos daños. Nuestra responsabilidad conjunta derivada de la presente declaración o de facebook no podrá sobrepasar la cantidad mayor de cien dólares (100 $) o la cantidad que nos hayas pagado en los últimos doce meses. Las leyes aplicables podrían no permitir la limitación o exclusión de responsabilidad por daños incidentales o consecuenciales, por lo que la exclusión de limitación anterior podría no ser aplicable en tu caso. En tales casos, la responsabilidad de facebook se limitará al grado máximo permitido por la ley aplicable."

[20] Aunque cada vez se usan más, siguen siendo mayoría los que no limitan la publicidad de sus perfiles. Véase KRISHNAMURTHY & WILLIS (2008, pp. 37-42). Consúltense también los datos del Observatorio Nacional de las telecomunicaciones y de la Sociedad de la Información, (observatorio.red.es).

paradójico[21]. Algunos, afortunadamente los menos, entienden que, dado que el usuario de estas redes es en su mayoría adolescente, los rasgos propios de esta edad (impulsividad, inconsciencia, apatía) no hacen más que potenciarse[22]. Otros se conforman con una explicación sociológica, como es que la urgencia de socialización hace que se menosprecien los riesgos y que se prescinda de toda protección[23].

Pero si hay algo cierto es que estos adolescentes son *nativos digitales*,[24] luego expertos en tecnología web. Y cada vez la usan más para protegerse. Un estudio exhaustivo demuestra que el 69% de los bachilleres de la muestra habían cambiado la política de privacidad que Facebook establece por defecto (abierto a toda la red) por otra más restrictiva, siendo la opción del 50% permitir el acceso exclusivamente a sus amigos[25]. Y otros, curiosamente, demuestran que los jóvenes usan más las opciones de privacidad que los adultos[26].

Atendida esta experiencia son ya mayoría los que apuntan otro tipo de argumentos para explicar esta paradoja, como son a) que no se ha desarrollado u ofertado la tecnología idónea para proteger la privacidad de los usuarios en este contexto (fácil, intuitiva y que no restrinja las posibilidades que la red *on-line* ofrece); y b) que el usuario no es quien está mejor posicionado a estos efectos, puesto que no puede controlar los contenidos que otros vuelcan[27].

a) Así, respecto a la cuestión tecnológica, observamos que los servicios estudiados ofrecen "opciones de privacidad" demasiado lineales, pues obligan a catalogar a todo un universo de contactos en tres únicas categorías: *amigo*, *no amigo* o *amigo de mis amigos*. Y no es fácil en un principio, y menos aún a medida que se usa la plataforma y entran en juego las aplicaciones, categorizar tus contactos conforme a estas tres únicas opciones y decidir cuál de los tres grupos, forzosamente heterogéneos, accede a qué contenidos[28].

---

[21] Debe consultarse el trabajo de HOLAND (2010).

[22] La crítica es antigua. LEVIN y SÁNCHEZ citan como precursor de esta corriente de opinion nada menos que a Hesíodo (800 ac) "I see no hope for the future of our people if they are dependant on the frivolous youth of today, for certainly all youth are reckless beyond words."

[23] Luego, coherentemente, toda mejora tecnológica sería irrelevante pues, a su juicio, los usuarios no la aprovecharían. GRIMMELMANN (2009, pp. 1140, 1178-9, 1180-4). Le sigue VILASAU SOLANA (2010, pp. 80-81).

[24] Como felizmente les bautizó PALFREY, véase PALFREY & GASSER (1998).

[25] DEBATIN et al. (2009, pp. 83 y ss.).

[26] Véanse los citados por MARWICK, MURGIA-DIAZ & PALFREY (2010, p. 30).

[27] Por todos, LEVIN & SÁNCHEZ ABRIL (2009, p. 1047).

[28] De nuevo aquí, HULL, RICHTER LIPFORD & LATULIPE (2010, p. 11). Es cierto que últimamente las plataformas permiten seleccionar individualmente quién ve algunos contenidos, pero el sistema es (¿aún?) tedioso y poco operativo.

En la práctica, la única opción estriba entre restringir el acceso a los amigos preexistentes, renunciando así a uno de los mayores atractivos de la red virtual –la posibilidad de explorar la frontera de tu red social, recuperando el contacto con viejos conocidos y contactando con desconocidos afines en algún aspecto–; o capitalizar esta utilidad prescindiendo de toda protección. Es lógico pues que quien decide darse de alta en este tipo de servicios prefiera esta última alternativa[29].

El sistema puede obviamente mejorarse, permitiendo que sea el usuario quien defina sus propias categorías de contactos para así reflejar virtualmente su verdadera red social. Y que disgregue, de forma fácil, intuitiva, según cuál sea la audiencia la visibilidad o acceso a según qué datos.

Pero los servicios de red social más extendidos carecen del suficiente incentivo para hacerlo porque, como ya apuntamos, su negocio depende del volumen de la red (cuantos más usuarios, mejor) y del tráfico de información (cuantos más datos, mejor). Luego no cabe esperar que, voluntariamente, implanten cortafuegos en la red que restrinjan el flujo de información[30].

Y así planteadas las "políticas de privacidad" sirven más como reclamo para incentivar que el usuario vuelque información que como eficaces herramientas de protección.[31]

b) La segunda razón apuntada, la imposibilidad de control por parte del usuario del uso que un tercero haga de sus datos, es aún más relevante, pues denota que cualquier innovación tecnológica será insuficiente para proteger adecuadamente a los usuarios de los ataques de sus pares. Y éstos son los más frecuentes en la red, y en los que consecuentemente nos centraremos, aunque se adviertan también intromisiones ilegítimas del propio servicio o de los terceros a los que aquél da acceso a los datos del usuario.

¿Son daños colaterales que los participantes en la red juzgan como "gajes del oficio"?

Hay quienes sostuvieron que sí, que a los usuarios de estas redes no les importa este tipo de "invasiones", que no tienen sentido de privacidad alguno. Pero ya no se mantiene. Cada vez más estudios evidencian que se sienten ultrajados cuando alguien no perteneciente al círculo o audiencia pretendida entra en sus perfiles (padres, profesores, empleadores, autoridades); o cuando sus datos o contenidos se vuelcan o usan para fines no queridos o se difunden más allá

[29] Véase GELMAN (2009, pp. 1315 y ss.).

[30] Coinciden aquí LEVIN & SÁNCHEZ (2009, p. 1047), concluyendo que aunque carecen de incentivos para mejorar la tecnología de control, tienen los medios y la demanda necesaria para hacerlo.

[31] HOLAND, (2010, p. 2).

del ámbito buscado[32].

Aunque a los *inmigrantes digitales* nos extrañe, no renuncian a su privacidad por el hecho de contar intimidades en la red. Entienden que hablan con su círculo de amigos y se sienten agredidos cuando alguien que no pertenece al mismo accede a esa información o vuelca información personal sobre ellos[33].

Tienen pues su propio concepto de privacidad, muy ligado al contexto en el que vuelcan información íntima[34]. Y quieren poder expresarse, comunicarse, edificar una identidad libremente ante una determinada audiencia y poder mostrarse de forma diferente ante otras[35].

Bien pensado, no es nada nuevo. Todos nos comportamos así en el mundo real. Lo difícil es proteger esta "privacidad contextualizada" desde la óptica del sistema norteamericano. Desde su

---

[32] Pueden consultarse los trabajos de campo de LEVIN & SÁNCHEZ ABRIL (2009, pp. 1001-1051). Para explicar este sentimiento de ultraje suele relatarse lo que ocurrió con el lanzamiento del *News Feed* de Facebook. Se trata de una aplicación que Facebook presentó en 2006 como un avance decisivo para mantener a todos los contactos permanentemente informados de lo que hacían los demás. En lugar de tener que visitar uno por uno los muros de tus contactos para ver qué novedades tienen, la aplicación presenta, en un sólo pantallazo actualizado al instante, todos y cada uno de los cambios. Pero, lejos de ser bien recibida, la aplicación generó un agrio rechazo por los usuarios pues evidenciaba que estaban permanente monitorizados por Facebook y entre si, además de insoportablemente bombardeados por información trivial de sus contactos. Este rechazo obligó a Facebook a modificar la aplicación permitiendo que sea el usuario quien decida qué quiere saber y de quién.

[33] Un amplio elenco de usuarios de Facebook concluye que "It's fine for close friends to look at one's profile. It's also fine for more distant aquaintances to look at your profile, but there needs to be a social reason. People with no social connection to you could look at your profile but shouldn't. It's not your responsability to fence them out!" La comenta GRIMMELMANN (2009, p. 1167).

[34] Sobre este concepto de *privacidad contextual* se ha escrito mucho. La idea original es de NISSEBAUM (2004, pp. 119 y ss.), que explica que toda comunicación está regida por unas normas de corrección y de distribución propias y peculiares del contexto en que se produce (familiar, sanitario, laboral, etc). En cada uno de ellos, lo que es correcto preguntar o contar, y lo que puedes después transmitir a terceros, es muy distinto, y este matiz esencial se pierde cuando pretende definirse qué es privado atendiendo únicamente a aquello que has mantenido en secreto, y negándoselo a cualquier información que, en un contexto determinado, hayas revelado. Un buen ejemplo que explica cómo puede invadirse la privacidad de un sujeto aunque la información que del mismo se difunde sea pública lo proporciona el "volcado" de las transcripciones de los juicios en internet. La información recogida en la transcripción es pública, también los datos personales, luego el interesado en la misma siempre ha podido acceder a ella. Pero le ha costado esfuerzo, y éste, a su vez, acredita su interés y restringe la difusión de los datos personales. Al subir las transcripciones a internet se ha alterado la norma de distribución implícita en este contexto al hacer accesible en un sólo click la información contenida en la transcripción y diseminándola más allá del círculo de personas realmente interesadas. La misma lógica explica porqué la aplicación antes comentada de Facebook (*Newsfeed*) indignó a los usuarios. Véase HULL, RICHTER LIPFORD & LATULIPE (2010).

[35] En palabras de WEST, LEWIS & CURRIE (2009, pp. 615-627), "young people conceptualize the Internet as a private space where they can share secrets and talk to their friends. Rather than viewing a distinct division between privat/public young people view social contexts as multiple and overlapping".

perspectiva, y simplificando el análisis, una vez que, voluntariamente, has revelado el dato o que te muestras en sitios públicos, la información o la imagen es pública[36].

La web 2.0., facilitando el acceso y la difusión global de los datos e imagen de los individuos sólo ha potenciado los riesgos de daños irreparables ya presentes en su anterior versión y puesto de manifiesto que el sistema de protección americano no es adecuado[37].

Asistimos pues a un alud de propuestas doctrinales que, en definitiva, buscan que el sistema reconozca el derecho de los individuos a construir su personalidad, permitiéndole mutar según cuál sea su interlocutor y a mantener dentro de un ámbito determinado las confidencias que revelan[38].

Buscan, en definitiva, aproximarse al sistema normativo europeo.

Los Derechos Europeos reconocen el *derecho a la vida privada* como una cuestión de dignidad del individuo[39]. La intimidad y la propia imagen, amén del honor, son derechos fundamentales respecto de los que toda intromisión se juzga, a priori, ilícita y constitutiva, per se, de un daño[40].

Somos los individuos, por tanto, quienes definimos, expresa o implícitamente, cuál es nuestra esfera privada y qué difusión le damos a la información relativa a la misma. Así, las revelaciones hechas en un determinado contexto no legitiman su difusión a otros o la imagen captada en

---

[36] A lo que ya avanzamos añadiremos ahora que los Tribunales han consolidado la idea de que no existe una *reasonable expectation of privacy* en lugares públicos.

[37] Porque es evidente que no se puede controlar la difusión de tu imagen o de tu información personal en un entorno donde mini cámaras pueden captar tu imagen y diseminarla sin tu consentimiento y blogueros pueden difamar a los individuos sin filtro editorial alguno ni oportunidad de rebatirles.

Ya en el contexto de las redes sociales, las digitales presentan caracteres que no tienen las físicas, como son que la información quede grabada para la posteridad, pueda rastrearse posteriormente y permita trazar todo un expediente digital del individuo con información descontextualizada. Véase boyd (2008, p. 40).

[38] Además de los ya citados LEVIN & SÁNCHEZ ABRIL, ROSEN (2000) o SOLOVE (2007). También hay críticos, no tanto con el concepto de privacidad defendido anteriormente cuanto con las medidas de protección un tanto naïf propuestas por algunos. Así, SCHWARTZ (2009, pp. 1407 y ss.); o POST (2001, pp. 2087 y ss.); pero sus alternativas no lo son menos, pues pasan por confiar en que las buenas prácticas terminarán reinando entre los internautas (?), o que el exceso de información en la red mitiga el impacto del daño. Así, LESSIG (2001, p. 2070).

[39] Sintetizando la doctrina del Tribunal Constitucional, particularmente la contenida en la sentencia 292/2000, dice GRIMALT SERVERA (2007, p. 36), que el art. 18. 1. CE no garantiza una intimidad determinada, sino el derecho a poseerla, una suerte de *derecho a una vida privada* que excluyo del resto.

[40] Art. 18 CE; LO 1/1982 de 5 de mayo.

lugares públicos sólo podrá reproducirse si la ampara su carácter "noticiable" (*newsworthiness*) [41].

Luego la defensa de nuestra privacidad mediante una pretensión indemnizatoria dirigida contra quien, en contra de nuestra voluntad, difunde nuestras intimidades o imágenes por la red es sin duda viable; y será aún más fácil de fundamentar cuando el afectado sea un foráneo a la red social *on-line*, pues su autoexclusión evidencia que no es éste el medio en el que, de haber querido publicar y/o difundir esa información, lo habría hecho.

Pero lo cierto es que, en cualquiera de los dos casos, la protección que ofrecen las pretensiones indemnizatorias dirigidas contra el infractor directo no resulta eficaz.

A los riesgos inherentes a toda pretensión de este tipo (localización del infractor y solvencia)[42], se suman aquí el hecho de que el mero ejercicio de la acción incrementa el daño, al aumentar la difusión de unos datos que el actor pretendía mantener confinados; y que el mismo remedio no es una respuesta adecuada cuando el daño es en sí irreparable y, por tanto, imposible de cuantificar[43].

Busquemos pues otro posible responsable que pueda colaborar eficazmente en la contención del daño.

## *5. La responsabilidad de los servicios de red social on-line por los contenidos ajenos que violen la privacidad de sus usuarios y de terceros.*

Antes de seguir avanzando quizá convenga aclarar que todos los prestadores de servicios de internet han desempeñado una función de filtrado de contenidos, por más que les pese a algunos. Es falso, por tanto, que internet sea un foro libre en el que los individuos puedan expresarse sin limitación alguna. Y no parece tampoco que deba serlo, no ya por razones ontológicas -porque los límites a cualquier derecho, también el de expresión, han de ser los mismos, sea donde fuere que se ejerciten, que también; sino fundamentalmente por motivos prácticos. Para que la red sea útil, para que los individuos accedan a los materiales que les interesan y no les colapsen los que desprecian, es imprescindible que haya filtros. La labor de filtrado de los servicios de

[41] Sobre este tema volveremos infra, apartado 6. Pero conviene avanzar que las imágenes que típicamente circulan por las redes sociales carecen de valor "noticiable" o interés público alguno, circunstancia que nos ahorra la difícil tarea de delimitar el ámbito de protección que merece el derecho a la propia imagen frente a la libertad de información o prensa. Sobre este tema, compartiendo de pleno la tesis sostenida por los autores, véase SALVADOR CODERCH, RUBÍ PUIG y RAMÍREZ SILVA (2011).

[42] No será en cambio un obstáculo su identificación porque, a diferencia de los servicios abiertos de internet, en las redes sociales los datos del usuario infractor son reales.

[43] Así, LIPTON (2010, pp. 25-27).

intermediación, tantas veces calificada peyorativamente como "censura", hace pues posible que el individuo se exprese permitiéndole formar una opinión propia[44].

La segunda cuestión, ya largamente debatida, es si dichos intermediarios deben también filtrar los contenidos ilícitos que circulan por la red, y en particular los que aquí interesan: los difamatorios y los vulneradores de la intimidad de los sujetos.

> Las objeciones a semejante atribución de responsabilidad a los intermediarios de las comunicaciones en internet (los ISP originarios) son por todos conocidas. Pueden sintetizarse en que la responsabilidad del intermediario por la ilicitud de los contenidos ajenos abocaría a un filtrado excesivo de los mismos, pues es tecnológicamente más fácil (y barato) para el ISP bloquear todo contenido sospechoso, incluyendo muchos que no sean ilícitos, que discriminar entre los mismos. Y que este exceso de censura mermaría gravemente el derecho de los ciudadanos a expresarse libremente, máxime teniendo en cuenta que, tal y como estaba estructurado su negocio, el ISP no obtenía una ventaja económica clara del (mayor) flujo de la comunicación, luego carecía de incentivo para intentar siquiera una criba razonable de contenidos[45].
>
> Si las reproducimos aquí es para que el lector juzgue si la situación de las SNS es la misma.

Y, de ser afirmativa la respuesta, la tercera cuestión será determinar el criterio o régimen de responsabilidad idóneo, que no resulte en exceso censurador pero que proteja razonablemente la privacidad y reputación de los individuos.

Vuelve a ser de nuevo importante, por la normativa aplicable a las matrices de las SNS más exitosas, estudiar el sistema normativo norteamericano:

Y allí, la responsabilidad de los ISP por contenidos provistos por terceros se excluye, legal y jurisprudencialmente, cuando dicho contenido atente contra la reputación o la privacidad. Adelanto la conclusión porque, por sorprendente e injustificada que parezca, está consolidada.

Pero merece ser explicada.

> El § 581 del *Restatement 2nd on Torts* (1977) recoge las reglas de la tradición del *common law* sobre la responsabilidad de los intermediarios por los daños a la reputación que ocasionen los contenidos ajenos que distribuyen, distinguiendo, lógicamente según el intermediario ejerza funciones de editor (luego controla el contenido de lo difundido) o de mero distribuidor (que carece de esa posibilidad de control).

---

[44] Concluye YOO (2010), que "La imagen de Internet como una experiencia sin intermediarios en la que se pueda hablar directamente a una audiencia sin pasar ningún tipo de filtro es más un mito que una realidad. La cuestión no es, por tanto, si debe haber intermediarios, sino quién debe asumir este rol (p. 707). La Primera Enmienda sólo excluye al Gobierno como filtro, pero no le impone obligación alguna de eliminar otros posibles filtros privados (p. 694) Es más, los Tribunales norteamericanos han reconocido que la labor editorial de los medios privados ha contribuido notablemente en la promoción de la libertad de expresión (p. 700)".

[45] Véase KREINMER (2006, pp. 11 y ss. y p. 85).

En este último caso, el intermediario sólo responde "si conoce o tiene motivos para reconocer" el carácter ilícito de la información[46].

Ambas condiciones (editor/distribuidor) son perfectamente aplicables a los intermediarios on-line según la función que de facto desempeñen. Y así lo entendieron los Tribunales[47]:

En Cubby *v*. Compuserve, Inc.[48] la demandada fue absuelta de responsabilidad pues se entendió que en su condición de mera distribuidora de información provista por terceros, ni conoció ni tuvo razón para conocer el carácter difamatorio de la información difundida.

En Stratton Oakmont Inc. *v*. Prodigy Services Co.,[49] en cambio, condenaron a la demandada basándose en su condición de editora de contenidos, pues así se presentaba el servicio en el mercado: un servicio dirigido a las familias, con contenidos controlados por un software que detectaba el lenguaje ofensivo y por un moderador del foro que retiraría los contenidos que considerase intimidatorios, de mal gusto o perjudiciales para la juventud. La demandada alegó que, pese a todo, era muy difícil controlar los contenidos, pues el volumen de los mensajes era enorme. Pero fracasó, también porque la responsabilidad del editor es, en el *common law*, objetiva.

El revuelo ante semejante condena no se hizo esperar. Si pese a la adopción de medidas de prevención razonables el intermediario responde porque se escapen a su control contenidos difamatorios, más vale no esforzarse en absoluto en tratar de evitar la difusión de la difamación. Esta "ceguera voluntaria" le permitirá aducir su condición de mero distribuidor y eludir una posible condena civil.

Corregir este indeseable resultado mediante el establecimiento de un sistema que incentivara al intermediario para efectuar labores de criba fue el motivo declarado por el legislador para promulgar la sección 230 de la *Communications Decency Act*, (1996) (47 U.S.C. § 230), correspondientemente titulada "Protection for Private Blocking and Screening of Offensive Material".[50]

La idea, pues, era garantizar al "buen samaritano" que emprendiese tareas de monitorización de contenidos para prevenir difamaciones en la red que no se vería expuesto a reclamaciones de daños, fundamentalmente contractuales.

---

[46] § 581: "Transmission of Defamation Published by Third Person" (...) one who only delivers or transmits defamatory matter published by a third person is subject to liability if, but only if, he knows or has reason to know of its defamatory character".

[47] Nos limitamos a resumir la evolución. El desarrollo minucioso de la misma puede consultarse en PEGUERA POCH (2007, pp. 9-40).

[48] 776 F. Supp. 135 (S.D.N.Y. oct. 29, 1991).

[49] WL 323710 N.Y. Supp. Ct. (may 24, 1995).

[50] Esta sección no resultó afectada por el juicio de inconstitucionalidad de (otras secciones) de la ley efectuado por el Tribunal Supremo en Reno *v*. American Civil Liberties Union [117 S.Ct. 2329 (jun. 26, 1997)], por lo que se encuentra compilada en el incorporada en el 47 U.S.C. § 512 (c) (3) 1999). Comenta la sentencia antes mencionada FAYOS GARDO (1997, pp. 231-243).

Pero el texto resultante, mejor, la interpretación y alcance que los tribunales le han dado, lograron el resultado opuesto: cualquier intermediario de internet, desarrolle o no labores de monitorización de contenidos, conozca o no el carácter ilícito por difamatorio o invasivo de la intimidad de terceros del contenido difundido, está inmunizado frente a las posibles reclamaciones de daños del tercero.

El texto reza así:

230 (c) (1) "No provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider"

230 (c) (2) "Additionally, no provider or user of an interactive computer service shall be held liable on account of:

any action voluntary taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessive violent, harassing, or otherwise objectionable, whether or not such material constitutionally protected;

or any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

La Sección (f) (2) define "interactive computer service" como "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the internet and such systems operated or services offered by libraries or educational institutions" [51].

El término "Publisher" bien podía entenderse limitado al editor, dejando a salvo la posible responsabilidad del intermediario como mero distribuidor; pero desgraciadamente no ha sido ésta la interpretación preferida por los que han aplicado esta norma.

En el principal caso posterior a la promulgación de la norma, y hasta la fecha no contestado, Zeran *v*. AOL[52], entendió el tribunal que la sección 230 c (1) inmuniza a los ISP tanto en su condición de editores como de meros distribuidores y, por tanto, aunque la demandada había sido requerida por el

---

[51] Una definición tan amplia cobija, claro, a las SNS, por lo que algún tribunal ya ha aplicado esta sección a MySpace. Me refiero a Julie Doe *v*. MySpace.com, 474 F Supp. 2nd 847 (W.D. Tex 2007).

En el supuesto contemplado, una niña de 14 años creó su perfil en MySpace afirmando ser mayor de edad, incluyó su teléfono y quedó con un chico de 19 años que abusó sexualmente de ella. Una vez arrestado y condenado, la familia de la niña demandó a MySpace por no poner impedimento alguno para que los menores puedan darse de alta en el servicio y quedar expuestos a depredadores *on-line*. La demanda, por tanto, no basa la responsabilidad del servicio en la omisión de una razonable labor de filtrado de contenidos, sino en la falta de establecimiento de controles efectivos para evitar que los menores accedan al servicio. Con todo, el juez de distrito aplicó el § 230 porque entendió que si se imputaba responsabilidad a MySpace por la omisión de medidas de control, sean del tipo que sean, se frenaría la libertad de expresión en contra de lo perseguido por la citada norma. Sobre este caso, véase SÁNCHEZ ABRIL (2007, nota 53).

[52] Zeran *v*. America Online Inc. 258 F. Supp. 1124 (E. D. Va, mar. 21, 1997).

demandante para que retirase un mensaje difamatorio, pese a que tardó en retirarlo y no impidió que reapareciera acto seguido, la exoneró de responsabilidad[53].

Recientemente se ha intentado otra vía para imputar a los ISP eludiendo la aplicación de la controvertida norma. La vía es la contractual, arguyendo la doctrina de la *promissory estoppel*. En el caso, Barnes *v*. Yahoo Inc[54], el ex novio despechado de la demandante había suplantado su personalidad creando perfiles falsos en un sitio web de Yahoo en los que la presentaba como promiscua, los ilustraba con imágenes de ambos desnudos y aportaba datos de contacto reales. Barnes requirió a la demandada que los retirase, siguiendo para ello el protocolo establecido en las condiciones de uso de la página, pero no obtuvo respuesta. Llevó el caso a la prensa y un día antes de que emitieran el reportaje la Directora de Comunicación de Yahoo telefoneó a la demandante, le requirió el envío por fax de los *mails* que previamente había remitido denunciando los hechos y le aseguró que se encargaría personalmente de eliminar los perfiles no autorizados. La demandante alegó que confió en su promesa. Pero transcurrieron dos meses más sin que hicieran nada, y planteó la demanda. Poco después, los perfiles falsos desaparecieron.

La cuestión a resolver por la Corte de Apelación del noveno circuito era si la sección 230 c (1) de la ley precluía la acción fundada en las reglas contractuales, y la respuesta fue negativa. Pero no se pronunció (porque no fue requerido para ello) sobre si los hechos sustentaban semejante demanda, esto es, si la promesa telefónica bastaba para generar una vinculación contractual[55]; ni sobre si Yahoo podría defenderse ante dicha demanda *ex* sección 230 c (2).

De momento, por tanto, los Tribunales han blindado a todo ISP de responsabilidad. A los que actúen como "buenos samaritanos" y a los que no hacen nada. Consecuentemente, denuncian los autores, una horda de sitios web han florecido animando a volcar cotilleos, rumores y difamaciones[56].

Lo sorprendente es que si el contenido infringe derechos de *copyright* ahí sí, el intermediario, en tanto que tal (esto es, mientras no cree, seleccione o modifique el contenido), responde "si supo o tuvo razones para conocer" el carácter ilícito del contenido que distribuye.

La única razón que explica este doble resero es que al haber mucho dinero en juego, la presión del *lobby* de titulares de derechos de propiedad intelectual fue difícil de contrarrestar por el *lobby* de las tecnológicas, que en materia de difamación o privacidad no encontraron una oposición

---

[53] Las sentencias de instancia posteriores que han procurado desmarcarse de semejante doctrina han fracasado en la Corte superior. Véanse los casos en PEGUERA POCH (2007, p. 24).

[54] 570 F. 3d 1096 (9th Cir. 2009).

[55] Aunque sí aclaró que el mero hecho de contar con un protocolo de monitorización de contenidos o incluso el hecho de intentar ayudar a una persona determinada no basta para generar responsabilidad contractual; que es preciso que la promesa sea tan clara y definida que pueda servir como oferta contractual (*id*. p. 5334).

[56] SOLOVE (2007, p. 159).

organizada[57].

Así, el sistema finalmente consensuado y sancionado en la *Digital Millennium Copyright Act* (1998), § 512 U.S.C., se presenta habitualmente como idóneo para equilibrar los intereses de los titulares del *copyright*, que querían otro, de responsabilidad objetiva del ISP por distribución o almacenamiento de material protegido; y de los ISP y usuarios de internet, que preferían obviamente la inmunidad de la CDA.

Lograron defenderse frente a una posible responsabilidad objetiva arguyendo la imposibilidad técnica de controlar el inmenso volumen de contenidos ajenos que circulan por su servidor pero, principalmente, amenazando con repercutir el coste del correspondiente mecanismo de filtrado y del inevitable seguro a los usuarios, concentrando así el mercado y encareciendo internet. También, que valorar si el material infringe derechos de propiedad intelectual es complejo, y no parece ser el intermediario quien deba decidir al respecto.

La responsabilidad del intermediario en la difusión de material protegido por el *copyright* es, pues, finalmente subjetiva. Responde si supo o pudo razonablemente saber de la infracción y no hizo nada para bloquear o retirar el material.

Para definir el perímetro de este deber de cuidado detalla la DMCA los procedimientos de aviso-retirada de materiales protegidos.

Así, en lugar de establecer la ley una obligación genérica de supervisión, obliga al ISP a actuar con prontitud en cuanto *conozca* o tenga *indicios claros* de un uso ilícito de materiales protegidos.

La principal vía de conocimiento es la notificación del titular del derecho afectado, que la ley regula con cuidado para evitar notificaciones abusivas y para salvaguardar los derechos del que subió el contenido. Para que proceda, la notificación tiene que identificar al denunciante e ir firmada, contener todos los datos precisos para su localización e identificar la infracción (obra, páginas, tipo de ilicitud etc.) e incluir la declaración del notificante de estar obrando de buena fe.[58]

Recibida esta notificación formal, el servidor debe bloquear el contenido y notificarlo inmediatamente al supuesto infractor, dándole así la oportunidad de defenderse. Si lo hace, esta contra-notificación será también trasladada de inmediato al denunciante, advirtiéndole que el material será desbloqueado si en el plazo de 10 a, como máximo, 14 días no presenta un requerimiento judicial para la retirada del mismo (*restraining order*) [59].

Es, sin duda, un buen sistema, pues reduce la litigiosidad, compromete al mejor posicionado para hacerlo en la persecución de usos ilícitos y evita un filtrado excesivo de contenidos (la temida *overdeterrance*) que, de instaurarse una posible responsabilidad vicaria de corte objetivo probablemente

[57] Porque que en casos de contenidos difamatorios/intromisivos cualquier tipo de control afectaría a la libertad de expresión, cosa que no sucede si el control es razonable y el contenido está protegido por el *copyright* no se lo cree nadie ¿no?

[58] Se le apercibe además de sanciones pecuniarias en caso de utilización fraudulenta del sistema.

[59] El sistema lo sintetiza muy bien XALABARDER (2002, pp. 131-135).

se produciría[60].

Luego los remedios para el injuriado en la red quedan, en el sistema norteamericano, muy seriamente limitados[61].

También los del que vea invadida su intimidad por contenidos proporcionados por otro[62].

Muchos autores defienden la promoción de un código de buenas prácticas entre los usuarios, entre las que se encuentra no acceder a información no dirigida a ellos o no difundir la información accedida más allá del límite pretendido por su titular[63]; y también entre los servicios, que comenzaría con la adopción de sistemas efectivos de *notice-take down* similares a los de la DMCA[64].

Pero sin duda la mejor solución sería derogar la sección 230 de la CDA y volver al régimen tradicional de responsabilidad del editor o distribuidor, según sea el caso.

Esta es, por cierto, la opción del sistema normativo del Reino Unido.

> Su *Defamation Act*, de 1996, sanciona la responsabilidad del editor por los daños que causen los contenidos difamatorios que difunde cuando, precisamente por la función que desempeña, pudo y, por tanto, debió filtrarlos. La posibilidad de defenderse alegando que no pudo razonablemente controlarse el

---

[60] Véase la crítica favorable del sistema de TAPALE, que cita en su apoyo también a la escuela de Chicago, en (2003, p. 22 y nota 140).

Otros no se muestran tan satisfechos, principalmente porque consideran que se presta al fraude, al permitir denuncias poco argumentadas y decisiones automáticas del servidor. Pero eso no significa que sistema sea malo, sino que controles de ley no se aplican como deberían.

[61] Alguno sugiere perseguir al servicio vía *torts,* basando su responsabilidad en la *contributory liability.* [THIERER (2009, p. 2)]. Pero los tribunales ya se han pronunciado al respecto exigiendo para su aplicación una clara inducción al ilícito por parte del que, de ser así, dejaría de ser un intermediario. "Mere knowledge of potential or actual infringing uses would not be enough to subject a distributor to liability", enfatizó POSNER en *In re Aimster* (Copyright Litg. núm. 01-6-8933, 2002 US Distr. LEXIS 21453 N.D. Ill. oct 30, 2002), entendiendo que esa inducción había quedado demostrada en autos, pues la red (p2p) operada por el demandado promovía activamente y facilitaba el software preciso para compartir material protegido entre los usuarios.

[62] Porque, como hemos visto, la separación sin matices entre lo público/lo privado precluye la acción al que revele los datos o se muestre en público pero, sobre todo, por la limitadísima eficacia de un remedio como el extracontractual frente al infractor directo ante la lesión de la intimidad o privacidad de un sujeto.

[63] Llegando incluso a sostener que entre ellos existen deberes de confidencialidad [GELMAN (2009, pp. 1139-40)] que, de infringirse, sirven de base para demandar al usuario-infractor de manera más eficaz que los tradicionales *torts against privacy* [véase MCCLURG (2006, pp. 887-940); SOLOVE (2007, p. 176, 192)].

[64] SOLOVE (2007, pp. 154-159; 191).

contenido publicado sólo está al alcance de los distribuidores, no de los editores; y, a diferencia del *common law*, es una excepción, esto es, se presume que también los distribuidores pudieron filtrar el contenido, pesando pues sobre ellos un *reasonable standard of care* que deben probar haber satisfecho[65].
El equilibrio alcanzado por la norma es notable pues no obstante fundamentar la responsabilidad en el conocimiento del carácter ilícito del contenido, impone un deber de cuidado razonable que obligará, según los casos y contenidos, a estar más o menos alerta, evitando así la exoneración en casos de "ceguera voluntaria".

Responden pues por los contenidos ajenos que sepan positivamente que son ilícitos (en sí o por el uso que se les esté dando); y por aquellos cuya ilicitud desconozcan si se juzga *reckless* o *willful* la falta de monitorización o prevención de la misma[66].

Cuáles son las medidas de prevención que puedan exigírseles se determinará igual que cualquier otro estándar de cuidado: deberá atenderse a la disponibilidad y accesibilidad de una tecnología de monitorización adecuada para detectar la infracción, a su coste, y a la gravedad y probabilidad del daño potencial[67].

Pues bien, hasta la fecha, y probablemente porque la SNS líder es Facebook y está domiciliada en EEUU, todas las redes sociales *on-line* consideran estar cubiertas frente a un posible de riesgo de incurrir en responsabilidad por la ilicitud de los contenidos subidos por los usuarios porque, afirman, su labor es de *mera intermediación*[68] y ofrecen a sus usuarios un sistema de denuncia de infracciones[69].

---

[65] Los *bloggers*, por tanto, sólo podrán ampararse en la defensa del *innocent disseminator* en tanto que demuestren que adoptaron las medidas de cuidado razonables para evitar que el comentario difamador se difundiera por todo el mundo. Sobre el tema, véase TUMBRIDGE (2009, pp. 505-507). La comparación entre la británica *Defamation Act* y la norteamenricana *Communications Decency Act* la sintetiza bien DETURBIDE (2000).

[66] Sobre la praxis de los tribunales británicos admitiendo la *innocent disseminator defense*, con la consecuente aproximación de un *tort* como el de *Defamation*, de responsabilidad estricta, al *tort of Negligence*, véase DESCHEEMAEKER (2009, pp. 603-641). Esta misma evolución, de una responsabilidad sancionada como objetiva a otra, subjetiva, que admite como defensa del informador su indagación exhaustiva de la verdad, se observa en nuestro Tribunal Constitucional, a juicio de SALVADOR (1990, pp. 247-8). La concreción de este deber de cuidado por el Tribunal Supremo la expone en las pp. 278-282.

[67] TAPALE (2003, p. 24). Volvemos pues a LEARNED HAND en U.S. *v*. Carroll Towing Co., [159 F. 2d 169 (2d Cir. 1947)].

[68] Así, Tuenti afirma:

"En relación al Servicio, TUENTI actúa como mero intermediario que pone a tu disposición su espacio web, asumiendo única y exclusivamente la responsabilidad derivada de la diligencia que le pudiera ser exigible por ley. TUENTI no asumirá ninguna responsabilidad, ya sea directa o indirecta, derivada del mal uso que hagas del Servicio, del sitio web o de los contenidos allí localizados.

TUENTI hará todo lo razonablemente posible para vigilar la legalidad de los contenidos, imágenes, opiniones y demás información que se comuniquen a través del Servicio y del sitio web. Sin embargo, al no ser posible el control absoluto de aquellos, tú serás el único responsable de la información, imágenes, opiniones, alusiones o contenidos de cualquier tipo que comuniques, alojes, transmitas, pongas a disposición o exhibas a través del sitio web; y, en concreto, serás el único responsable del mantenimiento de tu perfil, y de la información, imágenes,

opiniones, alusiones o contenidos de cualquier tipo que comuniques, alojes, transmitas, pongas a disposición o exhibas en tu perfil."

El *disclaimer* de Facebook lo reproducimos en la nota 20.

[69] Los sistemas se enuncian en las condiciones de uso de Facebook:

"Protección de los derechos de otras personas. Respetamos los derechos de otras personas y esperamos que tú hagas lo mismo.

No publicarás contenido ni realizarás ninguna acción en Facebook que infrinja o viole los derechos de otros o que viole la ley de algún modo.

Podemos retirar cualquier contenido o información que publiques en Facebook si consideramos que viola esta Declaración.

Te proporcionaremos las herramientas necesarias para ayudarte a proteger tus derechos de propiedad intelectual. Para obtener más información, visita nuestra página Cómo informar de presuntas infracciones de los derechos de propiedad intelectual.

Si retiramos tu contenido debido a una infracción de los derechos de autor de otra persona y consideras que ha sido un error, tendrás la posibilidad de .

Si infringes repetidamente los derechos de propiedad intelectual de otra persona, desactivaremos tu cuenta si es oportuno.

No utilizarás nuestros copyrights o marcas registradas (incluidos Facebook, los logotipos de Facebook y F, FB, Face, Poke, Wall y 32665) ni ninguna marca que se parezca a las nuestras sin nuestro permiso por escrito.

Si recopilas información de usuarios: deberás obtener su consentimiento previo, dejar claro que eres tú (y no Facebook) quien recopila la información y publicar una política de privacidad que explique qué datos recopilas y cómo los usarás."

Y en las de Tuenti:

"NOTIFICACIÓN DE INFRACCIÓN DE DERECHOS. En TUENTI velamos por la protección de los derechos de sus titulares por lo que, si cualquier persona o entidad detecta que sus contenidos han sido publicados en el Servicio sin su consentimiento, generando una infracción de derechos de propiedad intelectual o industrial y/o de derecho al honor, intimidad o a la imagen o de cualquier otro derecho, podrá comunicarlo a TUENTI, enviando un email a soporte@tuenti.com o bien mediante correo postal a la dirección que consta al final de estas Condiciones de Uso y Política de Privacidad Y Protección de Datos Personales (con el asunto en el caso del email o la referencia expresa en correo postal "Infracción de Derechos") y acompañando la siguiente información:

Identificación del contenido o datos personales o derecho protegido que ha sido vulnerado.

Identificación del citado contenido de forma suficiente para que en TUENTI podamos ubicarlo dentro del Servicio.

Identificación suficiente para que TUENTI pueda contactar con el reclamante: correo electrónico y teléfono.

Y merece la pena detenerse a estudiar si esto es así, para lo que comenzaremos desarrollando dos evidencias ya adelantadas:

La primera, que el sistema normativo europeo no es como el norteamericano; y la segunda, que el negocio de las redes sociales *on-line* es muy distinto del de los ISP, luego las soluciones legales dictadas en atención a estos últimos pueden no ser adecuadas para solucionar los problemas que plantean.

1) El sistema europeo de responsabilidad de los intermediarios de internet.

La Directiva comercio electrónico de 8 de junio de 2000/31/CE (en adelante DCE) y su implementación en nuestro sistema, la ley 34/2002 de 11 de julio de servicios de la sociedad de la información y de comercio electrónico (en adelante LSSI), a diferencia del sistema norteamericano, optaron por una regulación horizontal de la responsabilidad del intermediario por la difusión de cualquier contenido ilícito ajeno. No distinguen, por tanto, entre materiales protegidos por el derecho de autor y materiales difamatorios o vulneradores de la intimidad de otros[70]; ni la responsabilidad civil de la penal o administrativa[71].

Pero el régimen de responsabilidad que establece es prácticamente idéntico al de la DMCA: es un régimen subjetivo en cuya virtud el ISP responde, en tanto que intermediario, si supo o tuvo razones para saber que el archivo ajeno al que da acceso, aloja, almacena temporalmente o enlaza[72] es ilícito y no reacciona con prontitud para bloquear su acceso o retirarlo.

---

Copia de su D.N.I, pasaporte o documento oficial similar que permita su identificación.

Una declaración firmada en la que el reclamante manifieste que la información anterior es veraz y que afirme ser el legítimo titular (o bien que está autorizado a actuar en su nombre) de los derechos presuntamente vulnerados."

Ambos sistemas han sido analizados por los expertos de la UE para acreditar si cumplen con los Principios del Joint Statement on Key Principles of Social Networking Sites, (2009) [pueden consultarse en http://ec.europa.eu/information_society/activities/social_networking/docs] y ambos se consideran insuficientes y poco claros. Los test de implementación de los principios por parte de Facebook y de Tuenti son de febrero de 2010.

[70] Aunque gran parte del contenido regulador esté pensado para infracciones del *copyright,* i.e. no sabotear dispositivos tecnológicos de protección, no alterar recuentos de visitas mediante enlaces etc.

[71] Obviamente porque, como inmediatamente contaremos, excluyen la imputación civil si se satisface un estandar de cuidado. Excluida la responsabilidad civil, tanto más la sancionadora, penal o administrativa. Si la responsabilidad civil fuera objetiva, la norma tendría que diferenciar necesariamente el régimen sancionador.

[72] En art. 17 LSSI. La DCE no regula la actividad de los buscadores.

Aunque hay matices diferenciadores importantes. Así, mientras que la DMCA impone, como presupuesto para la aplicación de los denominados *safe harbors* o prácticas seguras, un deber general de colaboración y delimita la cooperación precisada al ISP, especialmente en caso de alojamiento de datos (*hosting*), regulando con detalle el procedimiento de notificación-retirada; la DCE/LSSI obvian la exigencia genérica de colaboración y no regulan un mecanismo de denuncia-réplica-retirada. Confían, dicen los comentaristas, en la autorregulación del sector.

Y es más, pese a que la DCE (art. 14) sienta como base de la imputación civil[73] (que no penal) el conocimiento efectivo o fuertemente indiciario de comportamiento ilícito, y la falta de reacción tempestiva; nuestro art. 16 LSSI limita la imputación a los casos de "conocimiento efectivo", sin ofrecer un criterio claro sobre cuándo adquiere el ISP dicho conocimiento. Veámoslo:

> Art.16 LSSI: "Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.
>
> 1.- Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario siempre que:
>
> a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
>
> b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.
>
> Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse".

Cuáles son esos "otros medios de conocimiento efectivo" sigue abierto a discusión. Algunos, alegando seguridad jurídica, son partidarios de una interpretación restrictiva que deje prácticamente sin contenido tan vaga mención[74].

Pero entiendo preferible una interpretación amplia que nos aproxime a la DCE y que permita la

---

[73] Para la imputación penal es indispensable el conocimiento efectivo. Sobre el tema, MORALES GARCÍA (2002, pp. 190-191).

[74] Particularmente contundente "sólo cuando hay notificación oficial surge la responsabilidad" parece GARROTE FERNÁNDEZ-DÍEZ (2004, p. 91), pero cita en su apoyo (nota 148) a quien dice lo contrario, como es PEGUERA POCH, y posteriormente afirma que bastaría una notificación fehaciente por los titulares del derecho (pp. 97-98). La cita doctrinal, completa hasta la fecha, puede consultarse en PEGUERA POCH (2007, p. 302).

imputación en casos de indicios claros de infracción[75].

Y así lo entiende finalmente también el Tribunal Supremo, que concluye en la sentencia de la Sala 1ª, de 9.12.2009 (RJ 2010\131, MP José Ramón Ferrándiz Gabriel) que "el conjunto de circunstancias pueden servir para acreditar la concurrencia de un conocimiento efectivo".

> Ese "conjunto de circunstancias" que menciona el Tribunal no podía pasar desapercibido:
>
> La demandada, la Asociación de Internautas, prestaba servicios web a sus asociados a través de la dirección www.internautas.org; entre otros, el alojamiento de datos. En dicha dirección web enlazaron otras con los dominios "putasgae.org"; "antisgae.org"; y "antisgae.internautas.org"; donde se podía leer de los demandantes (representantes legales de la SGAE), que eran una "banda de desocupados"; "matones a sueldo", "sanguijuelas sgaeras", o "putos chorizos", entre otras lindezas. La demandada perdió en ambas instancias y recurrió en casación apoyándose en el art. 20 CE y en la inexistencia de una resolución judicial *ex* art. 16 LSSI que le urgiera a cerrar las webs en discordia. Y el recurso, claro, fue desestimado[76].

No concurrían, en cambio, parecidas circunstancias en el caso resuelto por la STS, 1ª, de 18.5.2010 (RJ 2010\2319, MP: José Ramón Ferrándiz Gabriel), por lo que coherentemente absuelve el Tribunal al demandado que "no conocía ni podía razonablemente conocer, directa ni indirectamente, del carácter ilícito de la queja"; pero sobretodo que "en cuanto es informado del hecho por el demandante retira el comentario sin tacha de negligencia."

> Se trataba de un caso de suplantación de personalidad, en el que un anónimo, haciéndose pasar por el demandante, abogado de la Mutua, comenta en el portal "quejasonline.com" que "está harto de engañar a la gente retrasando los expedientes para no pagar" (...) y que la Mutua "tiene pinta de irse al garete."

Y en la reciente STS, 1ª, de 10.2.2011 (RJ 2011\313, MP: Juan Antonio Xiol Ríos) se condena al responsable del sitio web por su ceguera voluntaria, pues obstaculizó su localización para impedir así que se le comunicase oportunamente una infracción evidente.

> El sitio en cuestión, "alasbarricadas.com" contenía el "foro anarquista para el debate y contacto directo entre compañer@s" y, en él, un apartado dedicado a "El Rey del Pollo Frito. Zapatones", donde se podían leer insultos ultrajantes sobre el demandante. La domiciliación del sitio, en contra de lo requerido por el art. 10 LSSI, no estaba actualizada, siendo por tanto imposible la comunicación temprana que interrumpiera la difusión de los contenidos vejatorios, que prosiguió hasta la notificación

---

[75] De acuerdo, por tanto, con PEGUERA POCH (2002, p. 49), quien concluye que "sea como fuere, el juez deberá apreciar si el prestador tuvo o no conocimiento efectivo de la ilicitud y no hay obstáculo para que admita como prueba todo medio admitido en derecho, como la confesión o la presunción cuando la ilicitud es patente." En su monografía (2007, pp. 314-315), desarrolla el estado judicial de la cuestión, hasta esa fecha empatado (dos resoluciones a favor de la tesis restrictiva y dos en contra); pero hoy claramente superado por la interpretación no restrictiva contenida en las sentencias del Supremo que inmediatamente comentamos.

[76] Comenta la sentencia BERCOVITZ (2010, p. 2232).

de la demanda.

Tiene razón pues RUBÍ PUIG cuando concluye que para el Tribunal Supremo la mera comunicación del perjudicado (y, ahora, las circunstancias del caso) parecen suficientes para determinar la concurrencia de un conocimiento efectivo por el ISP; y en defender que se corrija normativamente este mensaje exigiendo un mínimo de diligencia a la hora de redactar dicha comunicación, evitando así una inseguridad nada deseable[77].

Pero lo cierto es que mientras la norma siga diciendo lo que dice no cabe reproche alguno a la interpretación que está dándole el Tribunal Supremo. Es a ellos, a los jueces, a quienes compete ponderar las circunstancias del caso y entender, si procede, que la notificación del demandante era suficiente para que el servicio adquiriera "conocimiento efectivo" de la ilicitud. Y está en manos del intermediario sustentar que su actuación posterior (ignorando la denuncia, arbitrando un proceso de bloqueo/réplica tipo el de la DMCA o, directamente, bloqueando el material) fue razonable, pues es en esta reacción, en la omisión del exigible deber de cuidado, en la que la norma basa la imputación[78].

Entiendo que la responsabilidad de la que se ocupan ambos textos, Directiva y Ley española, es la extracontractual en que pueda incurrir el servicio como consecuencia de la difusión de un contenido ilícito proporcionado por otro.

La responsabilidad contractual del proveedor de acceso/alojamiento frente a su cliente al que preste un mal servicio queda incólume[79].

Y que es una responsabilidad extracontractual subjetiva, fundada en la omisión del deber de cuidado que para cada una de las cuatro actividades contempladas (acceso, alojamiento, conservación temporal y enlace) establecen las normas.

También, que no basta con esa prueba de negligencia para que el servicio responda. Esta negligencia debe ser, además, la causa eficiente del daño, descartándose la responsabilidad del servicio cuando los hechos demuestren que de haberse satisfecho el estándar de cuidado normativo el daño se habría producido igualmente.

> Creo que esta conclusión la comparten todos los autores consultados, a los que la pésima técnica legislativa consistente en expresar negativamente algo que puede definirse positivamente, como es que

---

[77] RUBÍ PUIG (2010, pp. 16-18). Entiende, en cambio BERCOVITZ (2010, p. 1614), que no es preciso desarrollo normativo alguno, pues compete al Tribunal determinar cuáles son esos "otros medios".

[78] Lo explica muy bien el penalista MORALES GARCÍA (2002, p. 203).

[79] Así también PEGUERA POCH (2002, p. 38); PAZ ARES (2000, p. 95). En contra, CLEMENTE MEORO y CAVANILLAS MÚGICA (2003 y p. 82).

> el intermediario responde por culpa, les ha llevado a discutir si los supuestos en los que el intermediario no responde (por cumplir con el estándar de diligencia exigido) son de *exclusión*[80] o de *exención*[81] de responsabilidad. Discusión, insisto, sin resultado práctico relevante, porque los dos exponentes más notables de ambas tesis concluyen que, para que el ISP responda, además de la omisión del deber de cuidado deben concurrir los demás elementos de la pretensión indemnizatoria: daño (en nuestro caso presunto) e imputación objetiva.

¿Y las acciones de cesación? La Directiva (art. 18.1) las permite sin restricciones, pero deja libertad a los estados miembros para que establezcan la regulación que estimen conveniente. El silencio de nuestra LSSI al respecto se ha interpretado, a mi juicio correctamente, como una mera remisión al sistema general[82]. Y, pese a que la jurisprudencia inicial fue vacilante en este punto,[83] e indujo a proponer que para asegurar el éxito de la solicitud debía notificarse previamente al ISP la infracción, para amparar, después, en su inactividad la solicitud de cese o remoción[84]; actualmente admite la procedencia de las acciones de cesación conforme criterios que le son propios (idoneidad de la medida, coste etc.).

2) ¿Es aplicable el régimen de la DCE y de la LSSI a los servicios de redes sociales *on-line*?

Todos entienden que sí[85], aunque hay razones sólidas para dudarlo.

Tanto la DCE como sus normas de implementación están claramente dirigidas a controlar la compilación y uso inadecuado por parte de los gobiernos o empresas de *e-commerce* de los datos, en formato de texto, de los individuos[86]. No se plantean los problemas derivados de los posibles daños ocasionados por los particulares ni de los formatos de imagen.

---

[80] PEGUERA POCH (2007, pp. 322 y ss.); también en (2002, pp. 35-37).

[81] GARROTE FERNÁNDEZ-DÍEZ (2004, pp. 79 y ss.), para decir a continuación que obviamente tienen que darse además los (otros) elementos de la responsabilidad civil (nota 88). También CLEMENTE MEORO y CAVANILLAS MÚGICA (2003, p. 78).

[82] PEGUERA POCH (2007, p. 234); MASSAGUER (2003, p. 36); GARROTE FERNÁNDEZ-DÍEZ (2004, p. 67); BUSTO LAGO (2002).

[83] El juzgado mercantil de Madrid núm. 2, en su Auto de 10.11.2004, entendió que el ISP que adecúe su actividad al estándar de la norma está protegido no sólo frente acciones indemnizatorias, también frente acciones de cesación o remoción, que sólo pueden solicitarse si se fundamentan en la infracción del deber marco de colaboración del art. 11 LSSI.

[84] Así, GÓMEZ MARTÍNEZ (2004, p. 184).

[85] Sin excepción, todos los autores españoles que han escrito sobre redes sociales y citados en este texto.

[86] Destaca este último aspecto LIPTON (2010, pp. 6-13).

En materia de responsabilidad civil, tratan únicamente de delinear la responsabilidad del único intermediario entonces relevante: las empresas de telecomunicaciones que permitían el funcionamiento de internet.

Y escogen el sistema de responsabilidad subjetiva antes descrito. Pero las razones que justificaron el régimen finalmente implantado atendían, como no podía ser de otra forma, al concreto negocio de los ISP: a la necesidad de proteger un negocio entonces incipiente[87]; a la imposibilidad técnica de controlar el flujo de la información; y a la ausencia de interés en los datos que difundían.

Razones que no concurren ya en la web 2.0. donde, además, el riego de daños a la privacidad del individuo aumenta exponencialmente al entrar en juego sus pares.

Y si todas estas razones fuesen suficientes para entender que las normas antes mencionadas no son aplicables a los servicios de red social *on-line*, quedarían éstos expuestos a una posible deriva objetivadora de su responsabilidad por parte de los tribunales, que les convirtiera en garantes de la privacidad de los afectados.

No es éste, en absoluto, un resultado que estime conveniente.

La actividad de estos servicios no genera un riesgo de daños tan extremo que justifique la imposición de un régimen de responsabilidad objetiva cuyo coste, sin duda, amenazaría la pervivencia de un negocio de indiscutible valor social[88].

Entiendo, por tanto, que los servicios electrónicos de redes sociales deben regirse por el sistema general de responsabilidad del Código Civil, que fundamenta la obligación indemnizatoria en la omisión del deber de cuidado que razonablemente les sea exigible en la evitación o contención del daño. Deber de cuidado que, lógicamente, será más vago o concreto según quién sea el potencial perjudicado.

Luego el tercero, que ve cómo un usuario de la red le difama, difunde una información íntima o cuelga su foto sin permiso sólo debería poder exigir responsabilidad al servicio, *ex* LSSI, como

---

87 PEGUERA POCH (2002, pp. 25-33) insiste en este aspecto: "En todo momento histórico marcado por la innovación (...) el sistema de responsabilidad civil o Derecho de daños emerge con protagonismo especial al establecer una serie de reglas clave para el desarrollo y puesta en marcha de nuevas actividades que aparecen como fuentes potenciales de daños. Son las reglas que determinan qué niveles y tipos de riesgos serán tolerables y quién o de qué manera deberá soportar el daño"; y continúa (en p. 35) advirtiendo que el legislador debería tener en cuenta cuáles son los incentivos que se desprenden del régimen que quiera adoptar; y pensarse hasta qué punto una carga excesiva en términos de responsabilidad civil podría poner en peligro la consolidación de los ISP. También GARROTE FERNÁNDEZ-DÍEZ (2004, nota 103).

88 Sobre el despropósito que supondría una generalización de un sistema de responsabilidad objetiva véase PANTALEÓN PRIETO (2000, pp. 437-465).

prefieren los autores, o directamente *ex* art. 1902 CC, *si lo supo* o *lo pudo saber* y *no impidió* la difusión del ilícito. Pero nada más. Frente a un extraño, el deber de cuidado del servicio es muy genérico, luego nuestro tercero afectado carece del poder suficiente para exigirle que cambie el *modus operandi* del servicio, que adecúe su interfaz o que filtre, ni genérica ni aleatoriamente, los contenidos[89].

Sí puede exigírselo, en cambio, otro usuario de la red social. Y es que frente a él asume un deber de cuidado contractual, mucho más exigente.

Que la relación que une a la SNS con el usuario es contractual me parece indiscutible[90].

Que no es gratuito, quizá merezca algún receso, aunque solo sea por la vehemencia con que defienden este carácter los responsables de los servicios de red social[91].

Dicen que el servicio es gratuito porque el usuario no "paga" al darse de alta y crearse un perfil; ni por relacionarse con sus contactos, pero claro que paga. No con dinero, pero sí con sus datos, que vuelca masivamente en la confianza de encontrarse en ese entorno privado sugerido por el servicio y conforme al orden y criterios establecidos por este para que pueda rentabilizar esta *commodity* en el mercado. Y lo hace[92].

Luego la contraprestación al servicio es, precisamente, la privacidad del usuario. Privacidad que el servicio está obligado a proteger de manera principal y no meramente accesoria ex art. 1258 CC. No es, por tanto, un deber del que pueda descargarse a través de condiciones generales de contratación, como son todas las que típicamente regulan la "política de privacidad" del sitio.

> Porque son cláusulas que no suelen leerse; que, de hacerlo, no siempre explican bien cómo controlar tus

---

[89] El art. 15 DCE excluye expresamente la posibilidad de que los Estados impongan a los prestadores de servicios de intermediación deberes generales de monitorización; aunque sí podrían, dicen, imponerles deberes concretos de supervisión de, por ejemplo, materiales alojados en el servidor. Así, CLEMENTE MEORO y CAVANILLAS MÚGICA (2003, p. 71).

[90] Aunque no quepa hablar más que de *adhesión* a la mayor parte de la reglamentación contractual y la terminología empleada por los servicios –*condiciones de uso*, *declaración de derechos y responsabilidades*– eludan el término técnico: *cláusulas*.

[91] Véase MARTOS DÍAZ (2010, p. 147), asesora jurídica de Tuenti. También el séptimo Principio de Facebook: Servicio fundamental: Las personas deben ser capaces de utilizar Facebook de forma gratuita para establecer una presencia, conectarse con otros y compartir información con ellos. Toda persona tiene que poder utilizar el servicio de Facebook, independientemente de su nivel de participación o contribución.

[92] En el número de diciembre de 2010, que declara al creador de Facebook "personaje del año" 2010, la revista Time estima los ingresos del negocio en el ejercicio corriente en 1.500 millones de €; y apunta que de confirmarse el rumor de su salida a bolsa antes de 2012, el valor de cotización rondaría los 32.000 millones de €. El 86% de Tuenti, por otra parte, fue adquirido por Telefónica en verano de 2010 por una cifra aproximada de 75 millones €.

> datos en todo contexto; y que, de no estar de acuerdo con ellas, por entender que no protegen suficientemente, no puedes evitarlas ni siquiera dándote de alta en otro servicio, pues como hemos visto todos ofrecen básicamente las mismas[93].

Los servicios de redes sociales deben pues internalizar un coste, el de protección, que es inherente a su negocio. Su sistemático desplazamiento al impotente usuario evidencia, dicen los economistas, un notable fallo del mercado de datos personales[94].

Y para que la protección sea eficaz no bastan, claro, las políticas de privacidad corrientes. Es preciso un cambio en la arquitectura del sitio y en el interfaz para que pueda aprovecharse el valor social añadido que proporcionan estas redes *on-line* sin detrimento de la privacidad del usuario, esto es, que permitan al usuario disgregar fácil y eficazmente audiencias.

Esta tecnología está ya operativa:

> Recientemente se ha puesto en funcionamiento un prototipo de red social con medidas de seguridad adaptadas a la expectativa de privacidad del usuario[95].
>
> El sistema permite establecer distintas colecciones o grupos dentro de una misma agenda de contactos, sin restricciones ni etiquetas preestablecidas, luego conforme a los términos preferidos por el usuario. Los grupos y su etiqueta sólo son visibles para el usuario, que puede en todo momento cambiarlos o agregar/suprimir contactos.
>
> En todo momento, y gracias a un interfaz sencillo, se informa al usuario de cuál es su audiencia, para que sobrevenidamente pueda cambiar el acceso a cada contenido que desglosa.
>
> Y por defecto, puesto que está demostrado que es el grupo de amigos íntimos al que todo usuario se dirige principalmente, el acceso a los datos estará restringido a ellos; pero puede aprovecharse la facilidad que el medio digital ofrece para conectar con otras personas afines permitiendo que determinados contenidos que no se estimen comprometedores estén en abierto o accesibles a una audiencia más amplia.

No es la que ofrecen, quiero pensar que todavía, Facebook o Tuenti, aunque es justo reconocer

---

93 Permítame el lector que en este punto me remita a la doctrina ya clásica sobre las condiciones generales de contratación y el significado de "adherirse", ALFARO ÁGUILA-REAL (1991). Que lo son, desde luego, todas las que afectan a la política de privacidad, pues respecto de ellas "consent recedes further into background because of behavioral market distorsions and intense societal pressure to mantain network connection and visibility". HOLAND (2010, p. 17).

94 "Even sophisticated individuals concerned about privacy and aware of risks are unlikely to act as a rational economic agent", HOLAND (2010, pp. 6-10). Cita el caso Columbia Pictures Industries *v*. Bunnell , U.S. Dist. LEXIS 46364, 36-37 (D. Cal 2007), donde se fundamentó la responsabilidad del servicio en el incumplimiento de un *contractual duty*.

95 Véase http://www.clique.primelife.eu; y el estudio de su *alma mater*, LEENES (2010, pp. 48-65).

que ha habido avances y que esta última protege mejor que la primera la privacidad del usuario.

> En tanto que, al menos de momento, no permiten a los buscadores indexar los perfiles y que, afirman, aplican por defecto la máxima privacidad a los menores de 18 años. También porque tienen un procedimiento para la verificación de la edad de los usuarios que, dicen, evita la presencia de menores de 14 años en la red.
>
> Pero debe matizarse esta contundencia.
>
> Así, en materia de protección/exclusión de menores, el sistema, no por casualidad, opta por la reacción en lugar de la prevención. En vez de requerir para darse de alta la acreditación de ese mínimo de 14 años exigido reglamentariamente (art. 13 del RLOPD de 21 de diciembre de 2007) [96], que en nuestro país sería relativamente fácil pues contamos con un documento público de identificación, en muchos casos electrónico, prefieren esperar a que el menor sea denunciado por sus pares para entonces, ahora sí, exigirle que envíe copia de DNI bajo amenaza de expulsión. Últimamente parece que han complementado este inoperativo sistema de verificación con otro de rastreo de perfiles sospechosos[97]; pero, y como apunte meramente anecdótico, hemos constatado que del grupo de 60 alumnos de 1º de la E.S.O. (12 años) del colegio de mis hijos, 40 son usuarios de Tuenti.
>
> Y en materia de *default rules*, donde Tuenti asegura aplicar la más restrictiva (sólo mis amigos) cuando se trate de menores de 18 años, de nuevo acreditamos que, de 60 alumnos de 14 años (3º de la E.S.O.), 29 han sido encontrados en Tuenti por un adulto extraño a ese círculo.

¿Y los contenidos difamatorios?

Como acabamos de exponer, el deber contractual de cuidado protege la privacidad del usuario frente a usos no consentidos, imponiendo una suerte de deber de confidencialidad al servicio; pero no llega al punto de proteger frente a informaciones falsas y difamatorias que sobre uno de los usuarios de la red vuelque otro.

Es más, si filtrara comentarios ofensivos que algún usuario vertiera en sus comunicaciones con sus amigos podría este, con razón, alegar que esta suerte de censura viola el derecho al secreto en las comunicaciones.

Pero entiendo que el análisis cambia si los vierte en abierto a toda la red social, porque entonces pesa más el deber de protección del usuario ofendido, que impone al servicio la obligación de informarle para que pueda defenderse a través de un eficaz mecanismo de resolución de conflictos que, en este caso, cumpliría una función de reintegración del derecho lesionado[98].

---

[96] Texto normativo de dudosa competencia para determinar la edad de referencia, como critica PANIZA FULLANA (2009, p. 63).

[97] MARTOS (2010, pp. 157-159). No está de más recordar aquí que hace ya tiempo que están operativos sistemas que con un simple algoritmo detectan, por lista de contactos, la edad del usuario.

[98] Que el servicio puede detectar el lenguaje claramente ofensivo y que se reserva el derecho a filtrar estos

Como colofón, y gracias a una suerte de "efecto rebote", este deber contractual de protección del usuario protege también a los terceros de difamaciones o exposiciones no queridas en la red.

Porque establecidos los mecanismos privados de resolución de conflictos por invasión de la privacidad o difamación, podrán aprovecharlos en tanto que conozcan la publicación de su información personal o que les están difamando en la red, conocimiento al que accederán bien porque les alerte un usuario de la misma, bien porque la red tenga la posibilidad de identificarles y contactarles, ya que si pudiendo hacerlo no lo hacen incumplirían, ahora sí, su deber legal de actuar con prontitud cuando tengan constancia de una posible actuación ilícita.

La protección del derecho a la propia imagen del usuario o de un tercero es como inmediatamente veremos, mucho más sencilla.

## *6. En particular, las fotos.*

Dice GRIMMELMANN que el engorroso ritual del "desetiquetado" de imágenes no existiría si no hubiera habido otro, previo, de etiquetado en contra de la voluntad del retratado[99].

Entiende, pues, que el comportamiento a corregir es este último: el de etiquetar una foto sin el

---

contenidos puede deducirse de sus propias condiciones de uso:

"Protección de los derechos de otras personas. Respetamos los derechos de otras personas y esperamos que tú hagas lo mismo.

No publicarás contenido ni realizarás ninguna acción en Facebook que infrinja o viole los derechos de otros o que viole la ley de algún modo.

Podemos retirar cualquier contenido o información que publiques en Facebook si consideramos que viola esta Declaración."

Y en Tuenti:

"Podremos limitar el acceso al Servicio de opiniones, informaciones, comentarios, imágenes o dibujos que como usuario de TUENTI nos hagas llegar, pudiendo instalar, si así lo entendiéramos oportuno, filtros a tales efectos. Lo anterior no supone, en modo alguno, la obligación de TUENTI de controlar los contenidos que puedan difundirse a través del Servicio, sino la voluntad de evitar, en la medida de lo posible, que a través de TUENTI puedan difundirse en la Red contenidos u opiniones que puedan ser considerados difamatorios, racistas, sexistas, xenófobos, discriminatorios, pornográficos, violentos o que, de cualquier modo contraríen la moral, el orden público o las buenas costumbres, o resulten claramente ilícitos o ilegales."

[99] "The remarkable thing about the untagging ritual is that it would be completely unnecessary if there weren't a corresponding tagging ritual" GRIMMELMANN (2009, pp. 1171-3).

correspondiente permiso de los que en ella figuran, y no el hecho de publicarla, aunque sea sin etiqueta, sin dicho consentimiento.

Y es en cierta medida lógico que así piense, pues su sistema jurídico, recordémoslo, no considera ilícito captar imágenes de terceros cuando están en un lugar público ni diseminar otras ya "publicadas" [100]. Y presume que las imágenes volcadas en la red son públicas[101].

> La única conducta que en este sistema puede generar una pretensión en cabeza del retratado es el uso comercial de su imagen, motivo por el cual las empresas se cuidan mucho de contar con los consentimientos oportunos antes de "subir" fotos de sus eventos en las que pueda reconocerse a los figurantes[102].

Pero no es ese nuestro sistema, ni el común en Europa. Nuestros sistemas normativos reconocen, dentro de unos límites, nuestro derecho a decidir cómo y quién capta nuestra imagen y dónde y cómo se difunde[103].

Luego la presunción es la contraria a la vigente en el sistema norteamericano: puede constituir una intromisión la captación de la imagen de otro en un lugar público; y permitir la captación no equivale a autorizar su publicación. Más aún cuando esa imagen publicite facetas íntimas del representado.

Los sistemas normativos europeos han optado, por tanto, por un sistema que prima la prevención de la lesión. Ofrecen así tres únicas alternativas para que el uso de imágenes en las que un tercero puede ser identificado sea lícito en internet:

---

[100] *Restatement 2nd of Torts* § 652 (c).

[101] Por lo que concluyen los autores que "a particular irony with photos is that often the photographer, who is not in the picture, is the only person with rights to prevent its republication, and the person of who the photo was taken has no mechanism in law to asset any interest." LAUREN GELMAN (2009, p. 1331); también SÁNCHEZ ABRIL (2007, p. 81). De ahí el esfuerzo académico para desarrollar un nuevo *tort* que proteja a los ciudadanos frente a prácticas de monitorización contínua en lugares públicos, como por ejemplo la de la aplicación de Google *Street View*. Véase BLACKMANN (2008, pp. 313 y ss).

[102] La conciencia de ser los titulares del derecho a explotar comercialmente la propia identidad explica la reacción, mucho más que airada, de los usuarios de Facebook ante el lanzamiento de otra de sus aplicaciones, esta vez *Beacon*. Consistía en utilizar el conocimiento que la plataforma tiene sobre las compras realizadas por los usuarios para informar a sus contactos sobre sus adquisiciones, foto incluida.

[103] STC, de 2.7.2001 (RTC 156\2001; MP: Carles Viver Pi-Sunyer). Únicamente excluye del ámbito constitucional (que no del de la LO 1/82) el aspecto patrimonial del derecho a la propia imagen (STC, de 26.3.2001 [RTC 81\2001, MP: Carles Viver Pi-Sunyer)]. Sobre las mismas, GRIMALT SERVERA (2007, p. 37). En sus sentencias, el Tribunal Supremo defiende el derecho de autodeterminación del retratado, esto es, el derecho a decidir si su imagen se plasma, cómo y si se divulga. IGARTUA ARREGUI (1990, p. 320).

a) La primera, que la difusión de la imagen del tercero se ampare en la excepción del carácter "noticiable" de la imagen o del evento que se documenta, siendo la imagen del sujeto en este caso accesoria (art. 8.2. LO 1/82) [104].

b) La segunda, que esa difusión pueda cobijarse en la excepción de "uso doméstico" del art. 2.2 a) de la LOPD[105].

c) Y, la tercera, que la difusión haya sido consentida por el sujeto retratado (art. 2.2. LO 1/82).

La primera opción es la típicamente empleada por los medios de comunicación, que filtran las imágenes que publican para que sólo aparezcan las que entienden que responden a ese "carácter noticiable" y asumen el correspondiente riesgo de equivocarse y tener que responder en casos de extralimitación. Quizá sea también el paraguas en que deban cobijarse servicios como *Flickr*, donde se comparten fotos de carácter documental o artístico, más que meros recuerdos de eventos privados.

En la segunda sólo pueden cobijarse los intercambios de fotos por mensajería privada, por medio del correo electrónico o servicios como *Google Buzz*; pero no los típicos en una red social al uso, ni siquiera cuando el usuario configura el acceso a las mismas de la forma más restrictiva posible (sólo mis amigos), pues basta con que uno de los contactos esté en abierto para que la difusión deje de ser "privada", sin que pudiéramos imputarle a este último su difusión.

La tercera, contar con el consentimiento previo del retratado, es pues la única que sensatamente pueden aprovechar los servicios electrónicos de red social, a quienes no parece razonable que les pueda interesar asumir la labor de criba propia de los medios de comunicación –y su correspondiente riesgo de responsabilidad–.

Pero ponerla en práctica requiere, justo al contrario de lo que defiende GRIMMELMAN, que la foto se etiquete, pues solo así puede comprobarse si el titular de la imagen ha consentido su publicación por quien pretende colgarla en la red[106].

La técnica consistente en no etiquetar las imágenes, iniciada en la web 1.0., puede mitigar el efecto lesivo que la publicación de la foto tenga para la privacidad del retratado si se publica en

---

[104] GRIMALT SERVERA (2007, pp. 128 y 132). Que la protección que brinda nuestro sistema al derecho a la propia imagen es excesiva cuando se confronta con la libertad de información lo defienden convincentemente SALVADOR CODERCH, RUBÍ PUIG y RAMÍREZ SILVA (2011). Pero las redes sociales *on-line* no son, ni lo pretenden, medios de comunicación.

[105] Así, ARENAS (2010, p. 140); y, parecido, VILASAU SOLANA (2009, p. 134).

[106] Que cuentan ya con *software* para reconocer figuras humanas en imágenes es sobradamente conocido por todos.

foros abiertos, tipo *Youtube*[107], porque aquí es probable que la imagen se pierda en una montaña de videos desorganizados[108].

En las redes *on-line*, en cambio, el no etiquetar la foto no evita el impacto lesivo de la publicación, porque esa imagen en la que puede reconocerse a un sujeto, llega precisamente al círculo social (laboral, familiar, de amistad) que le puede identificar, pues típicamente se suben fotos de personas conocidas por tus contactos[109].

Y conceder al retratado el "derecho" a quitar su nombre de la imagen no soluciona nada, pues el daño ya está causado. Ni siquiera colabora en su contención, pues la imagen "desetiquetada" sigue ahí[110].
Luego es imprescindible el consentimiento del retratado antes de proceder al volcado. Y pueden articularse sistemas para que no sea costoso obtenerlo[111].

Si el retratado es (otro) usuario de la red, puede localizársele y articular un procedimiento de confirmación similar al ya utilizado para invitar a eventos o difundir noticias. Y podría también articularse un sistema algo más general de consentimiento previo, siempre que el elenco de sujetos autorizados pueda definirse por cada usuario y modificarse en cualquier momento. No es esto, ciertamente, lo que a juicio de la doctrina y jurisprudencia mayoritaria requiere la norma cuando exige que el consentimiento sea inequívoco y concreto para cada acto, persona, y publicación[112]; pero entiendo, de acuerdo con la doctrina más reciente, que la exigencia legal debe interpretarse de forma algo más laxa para que sea operativa en un foro como el de las redes sociales electrónicas[113].

---

[107] Estudios de campo evidencian que los videobloggers (*vloggers*) no se dirigen a su círculo de amigos preexistente. Véase los citados por HULL, RICHTER LIPFORD & LATULIPE (2009, nota 4).

[108] Lo que no quiere decir que la conducta sea lícita, pero sí que el impacto lesivo generalmente es menor. Con todo, el caso de *Youtube* es lo suficientemente complejo como para abordarse en este trabajo.

[109] Como bien precisa MARTÍN I CASALS (1990, p. 397); la gravedad del daño muchas veces depende más de aspectos cualitativos (ámbito próximo de difusión de la información) que de aspectos cuantitativos (alcance de la difusión).

[110] Sólo puede borrarla su "dueño" en la red, esto es, el que la publicó.

[111] De acuerdo pues con MARTÍNEZ MARTÍNEZ (2010, nota 22).

[112] Véase comentario al art. 2.2 en conexión con el 1.3 de la LO 1/82 de GRIMALT SERVERA (2007, p. 106); y de IGARTUA ARREGUI (1990, pp. 324-326).

[113] Un exceso de protección podría bloquear la funcionalidad del servicio y destruir el valor social del servicio. Sobre este difícil equilibrio, HOLAND (2010, p. 19). Parece que también defenderían esta interpretación SALVADOR, RUBÍ y RAMÍREZ (2011, p. 18).

Si el titular de la imagen es foráneo a la red, debe contactársele vía *e-mail*, como no hay inconveniente en hacer cuando se trata de capturar la lista de contactos del que se da de alta[114].
Sin el consentimiento oportuno, la foto sólo puede colgarse en la red pixelando el rostro del afectado, técnica que resultará eficaz para "salvar" las fotos de grupo cuando no se cuente con el permiso de todos los retratados.

Las fotos de eventos de empresas e instituciones deben subirse en su página web, y serán ellas las que sin duda filtrarán las imágenes para publicar únicamente las que no les comprometan por un uso comercial indebido de la imagen de terceros.

## *7. Conclusiones*

I.- Los servicios de red social on-line tienen un valor y una relevancia social indiscutibles, máxime para los jóvenes. Consecuencia lógica de esta progresiva implantación es la aparición de un número considerable de conflictos entre los usuarios de este servicio y entre ellos y los foráneos a la red, que plantean serias dudas sobre el régimen jurídico conforme al que deban resolverse.

II.- Puesto que las SNS prestan servicios de intermediación en internet, son hoy mayoría los que entienden que quedan sometidas al régimen establecido en la Directiva de Comercio Electrónico y en su norma española de implementación, la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, en particular al régimen de responsabilidad por el alojamiento de contenidos ilícitos ajenos (art. 16 LSSI).

Pero aunque literalmente sean prestadores de servicios en internet, su negocio y circunstancias son muy diferentes a las propias de los proveedores de servicios de *hosting* contemplados por el legislador al promulgar las normas citadas, luego su aplicabilidad puede discutirse.

III.- Pese a ello, el régimen de responsabilidad extracontractual de los servicios de red social *on-line* por los daños que los contenidos subidos por sus usuarios causen en la reputación, intimidad o imagen de un tercero debe ser sustancialmente idéntico al establecido en el art. 16 LSSI, que no hace más que concretar la cláusula general del art. 1902 CC para este contexto. Sólo responden pues si omiten el deber de cuidado que les es exigible en el desarrollo de su actividad, esto es, si no reaccionan con prontitud y eficacia retirando o bloqueando el contenido tan pronto como sepan o debieran razonablemente saber que es ilícito. El establecimiento de un régimen objetivo

---

[114] También lo hace Facebook para darte la oportunidad de "desetiquetar" una foto ya colgada sin tu consentimiento, pero para ello previamente tendrías que darte de alta en el servicio. No te permite, como ya avanzamos, borrarla, a menos que seas el titular del copyright sobre la misma y atiendan tu reclamación.

En Tuenti sólo se permite el etiquetado de fotos de *amigos*, luego no podría colgarse una foto de un ajeno a la red y etiquetarla con su nombre. Pero no hay obstáculo alguno para añadir un primer plano de dicho sujeto en un documento y titularlo con su nombre.

de responsabilidad no estaría, a mi juicio, justificado.

IV.- La responsabilidad contractual que el servicio asume frente al usuario no se regula, obviamente, en la Ley, pues depende de cada tipo de servicio. Y el de las redes sociales tiene un contenido sustancialmente diferente al asumido por los servicios de alojamiento de contenidos. A diferencia de éstos, las SNS no cobran por alojar los contenidos ni por la intercomunicación con los usuarios. Tampoco despliegan publicidad genérica en los perfiles y cobran por ello a las empresas. El usuario paga a las empresas de red social con sus datos e información personal que, vertida de la forma que el servicio la requiere, puede rentabilizarse mediante su cesión a terceros (empresas de marketing u otros). La monitorización de los contenidos vertidos por los usuarios y su posterior distribución constituye pues el núcleo del negocio de estas empresas.

V.- El objeto del contrato entre el usuario y el servicio de red social es, por tanto, sus datos e información, también privada. Luego el servicio está contractualmente obligado a proteger esta privacidad del usuario frente a las intromisiones de terceros ajenos a la red; pero también, y en lo que aquí interesa, frente a los ataques de sus pares.

VI.- Los servicios de red social *on-line* asumen pues el deber contractual de proporcionar a sus usuarios la tecnología precisa para que puedan comunicarse con mayor o menor privacidad, permitiéndoles de forma rápida e intuitiva disgregar sus contactos para que accedan a según qué contenidos.

VII.- Deben además detectar contenidos notoriamente ofensivos que circulen en abierto por la red, informar a los afectados y ofrecerles mecanismos eficaces de resolución de los conflictos de difamación o intromisión en la intimidad que puedan surgir entre ellos.

VIII.- Y deben, en fin, impedir la publicación de su imagen sin su previo consentimiento, para lo cual deben impedir la visualización de fotos con figuras humanas identificables cuyo rostro no esté bien etiquetado, bien pixelado. El usuario retratado puede permitir que se publique su imagen de manera concreta, como requiere el art. 2.2. LO 1/82; o de forma algo más genérica (por álbum de fotos o grupo de amigos), como demanda la operatividad del servicio, pero siempre que éste permita en cualquier momento alterar el grupo de autorizados y exigir el borrado de su imagen.

IX.- Estas medidas de precaución frente a posibles lesiones de la privacidad o imagen del usuario que el contrato impone al servicio de red social benefician, *par ricochet*, también al no usuario, pues le permitirán acceder a los mecanismos de resolución de conflictos cuando sepan que están siendo objeto de difamación o su intimidad está siendo invadida por los usuarios y, lo más importante a los efectos de este estudio, impedirán que una foto en la que sean perfectamente identificables se suba a la red sin su permiso.

X.- Sólo falta que los usuarios se animen y exijan, extra y/o judicialmente, la mejora de los servicios.

## *8. Tabla de jurisprudencia citada*

### *Sentencias del Tribunal Constitucional*

| *Fecha* | *Ref.* | *Magistrado Ponente* |
|---|---|---|
| 26.3.2001 | RTC 81 | Carles Viver Pi-Sunyer |
| 2.7.2001 | RTC 156 | Carles Viver Pi-Sunyer |
| 30.11.2000 | RTC 292 | Julio Diego González Campos |

### *Sentencias del Tribunal Supremo*

| *Fecha* | *Ref.* | *Magistrado Ponente* |
|---|---|---|
| 9.12.2009 | RJ 131 | José Ramón Ferrándiz Gabriel |
| 18.5.2010 | RJ 2319 | José Ramón Ferrándiz Gabriel |
| 10.2.2011 | RJ 313 | Juan Antonio Xiol Ríos |

### *American Case Law*

| Case | Date/ref. |
|---|---|
| Barnes *v*. Yahoo Inc. | 570 F. 3d 1096 (9th cir.)2009 |
| Doe *v*. MySpace.com | 474 F. Supp 2nd 847 WD Tex 2007 |
| In re Aimster | Distr.Lexis 21453 ND III oct, 30 2002 |
| Reno *v*. American Civil Liberties Union | 117 S. Ct. 2329 jn, 26 1997 |
| Zeran *v*. America Online Inc. | 258 F. Supp. 1124 ED Va mar 21, 1997 |
| Stratton Oakmont Inc. *v*. Prodigy Services Co. | W6 323710 NY Supp. Ct, may 24, 1995 |
| Cubby *v*. Compuserve Inc. | 776 F. Supp 135 SDNY oct 29, 1991 |

## *9. Bibliografía*

Jesús ALFARO ÁGUILA-REAL (1991), *Las condiciones generales de la contratación*, Civitas, Madrid.

Mónica ARENAS RAMIRO (2010), "El consentimiento en las redes sociales", en Artemi RALLO LOMBARTE y Ricard MARTINEZ MARTINEZ (Coords.), *Derecho y redes sociales*, Aranzadi, Pamplona, pp. 117-145.

Rodrigo BERCOVITZ RODRÍGUEZ-CANO (2010), "SENTENCIA DE 9 DE DICIEMBRE DE 2009: Responsabilidad de los prestadores de servicios de la sociedad de la información: servicios de alojamiento o de almacenamiento de datos", *Cuadernos Civitas de Jurisprudencia Civil* , núm. 84, pp. 603-1615.

Josh BLACKMANN (2008), "Omniveillance, Google, Privacy in Public and the Right to your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet", *Santa Clara Law Review*, núm. 49, pp. 313-392.

Danah Michele BOYD (2006), "Friends, Freindsters, and MySpace Top 8: Writing Community Into Being on Social Network Sites" (www.firstmonday.org/issues/issue11_12/boyd/index.html).

--- (2008), "Taken out of Context: American Teen Sociality in Networked Publics" (ecopy at www.ssrn.com/abstract= 1344756).

Danah Michele BOYD y Nicole B. ELLISON, (2007), "Social Network Sites: Definition, History and Scholarship" (www.jcmc.indiana.edu/vol13/issue1/boyd.ellison.html).

José Manuel BUSTO LAGO (2002), "La responsabilidad civil de los prestadores de servicios de intermediación en la sociedad de la información", *Actualidad Jurídica Aranzadi,* núm. 542 (www.westlaw.com/BIB 2002/1091.).

Mario E. CLEMENTE MEORO y Santiago CAVANILLAS MÚGICA (2003) *Responsabilidad civil y contratos en internet*, Comares, Granada.

Bernhard DEBATIN *et al.* (2009) "Facebook and Online Privacy: Attitudes, Behaviour, and Unintended Consequences", *Journal of Computer-Mediated Communication*, núm. 15(1), pp. 83-108.

Eric DESCHEEMAEKER (2009-4), "Protecting Reputation: Defamation and Negligence", *Oxford Journal of Legal Studies*, núm. 29, pp. 603-641.

Michael DETURBIDE (2000), "Liability of Internet Service Providers for Defamation in the Us and Britain: Same competing Interests, Different Responses", *Journal of Information, Law and Technology (JILT)*, núm. 3 (www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/deturbide/).

Antonio FAYOS GARDO (1997), "El nuevo mercado de las ideas (sobre la sentencia del Tribunal Supremo norteamericano del caso Internet), *Revista de Administración Pública*, núm. 144, pp. 231-243.

Ignacio GARROTE FERNÁNDEZ-DÍEZ (2004), "Acciones civiles contra los prestadores de servicios de intermediación en relación con la actividad de las plataformas p2p. Su regulación en la ley 34/2002 y en la Ley de Propiedad Intelectual", *Pe.i*, núm. 16, pp. 55-104.

Lauren GELMAN (2009), "Privacy, Free Speech, and Blurry-edged Social Networks", *Boston College Law Review*, núm. 50, pp. 1315-1344.

Carlos GÓMEZ MARTÍNEZ (2004), *Derecho a la intimidad y nuevas tecnologías*, Consejo General del Poder Judicial, Madrid.

Pedro GRIMALT SERVERA (2007), *La protección civil de los derechos al honor, intimidad y propia imagen,* Iustel, Madrid.

James GRIMMELMANN (2009) "Saving Facebook", *Iowa Law Review*, núm. 94, pp. 1137-1206.

Brian HOLAND (2010), "Privacy Paradox 2.0", *Wiedener Law Journal* (forthcoming) (ecopy at www.ssrn.com/abstract=1584443.).

Gordon HULL, Heather RICHTER LIPFORD & Celine LATULIPE (2010), "Contextual Gaps: Privacy Issues on Facebook" (www.ssrn.com/abstract=1427546), pp. 1-37.

Fernando IGARTUA ARREGUI (1990) "El derecho a la imagen en la jurisprudencia española", en Pablo SALVADOR CODERCH (Dir.), *El mercado de las ideas*, Centro de Estudios Constitucionales, Madrid.

Balachander KRISHNAMURTHY y Craig WILLIS (2008), "Characterizing Privacy in Online Social Networks", *Proceedings of first workshop on Online social networks*, ACM, New York, (http://portal.acm.org/citation.cfm?doid=1397735.1397744).

Seth F. KREINMER (2006), "Censorship by Proxi", *University of Pennsylvania Law Review*, núm. 155, pp. 11-101.

Ronald E. LEENES (2010), "Context is Everything - Sociality and Privacy in Online Social Network Sites", *Privacy and Identity* (ecopy at www.ssrn.com/abstract=1706295.), IFIP AICT 320, A.M. Bezzi, ed., pp. 48-65.

Lawrence LESSIG (2001), "Privacy and Attention Spam", *Georgetown Law Journal*, núm. 89, pp. 2063-2072.

Avner LEVIN y Patricia SÁNCHEZ-ABRIL (2009), "Two Notions of Privacy Online", *Vanderbilt Journal of Enterteinment and Technology Law*, núm. 11 (ecopy www.ssrn.com/abstract=1428422), pp. 1001-1051.

Jacqueline D. LIPTON (2010), "Mapping Online Privacy", *Northwestern Univiversity Law Review* (forthcoming), núm. 104 (ecopy at papers.ssrn.com/sol3/papers.cfm?abstract_id=%201443918).

Craig MARTIN (1998), "Mailing lists, Mailboxes and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem", *Houston Law Review*, núm. 35, pp. 801 y ss.

Miquel MARTÍN I CASALS (1990), "Indemnización de daños y otras medidas judiciales por intromisión ilegítima contra el derecho al honor", en Pablo SALVADOR CODERCH (Dir.), *El mercado de las ideas*, Centro de Estudios Constitucionales, Madrid, pp. 382-409.

Nuria MARTOS DÍAZ (2010), "Políticas de privacidad y verificación de la edad en Tuenti", en Artemi RALLO LOMBARTE y Ricard MARTINEZ MARTINEZ (Coords.), *Derecho y redes sociales*, Aranzadi, Pamplona, pp. 145-163.

Alice MARWICK, Diego MURGIA-DIAZ & John PALFREY, (2010) "Youth, Privacy and Reputation (Literature Review)", *Berkman Center Research Publication*, núm. 5 (ecopy at www.ssrn.com/abstract=1588163.), pp. 1-75.

Ricard MARTÍNEZ MARTÍNEZ (2010), "Protección de datos personales y redes sociales: un cambio de paradigma", en Artemi RALLO LOMBARTE y Ricard MARTINEZ MARTINEZ (Coords.), *Derecho y redes sociales*, Aranzadi, Pamplona, pp. 83-116.

José MASSAGUER (2003), "La responsabilidad de los prestadores de servicios en línea por las infracciones de los derechos de autor y de los derechos conexos en el ámbito digital. El Tratado OMPI sobre Derecho de Autor (WCT) y el Tratado OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT)", *Pe.i*, núm. 13, pp. 11-48.

Andrew Jay MCCLURG (2006), "Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality", *University of Cincinnati Law Review*, núm. 74, pp. 887-940.

Óscar MORALES GARCÍA (2002), "Criterios de atribución de responsabilidad penal a los prestadores de servicios e intermediarios de la sociedad de la información", en *Contenidos Ilícitos y Responsabilidad de los Prestadores de Servicios de Internet*, *Revista de Derecho y Proceso Penal*, monografía, núm. 8, pp. 163-210.

Adán NIETO MARTÍN y Manuel MAROTO CALATAYUD (2010), "Redes sociales en internet y data mining en la prospección e investigación de comportamientos delictivos", en Artemi RALLO LOMBARTE y Ricard MARTÍNEZ MARTÍNEZ (Coords.), *Derecho y Redes Sociales*, Aranzadi, Pamplona, pp. 207-258.

Helen NISSEBAUM (2004), "Privacy as Contextual Integrity", *Washington Law Review*, núm. 79, pp. 119-157.

Paula ORTIZ LÓPEZ (2010), "Redes sociales: funcionamiento y tratamiento de la información", en Artemi RALLO LOMBARTE y Ricard MARTINEZ MARTINEZ (Coords.), *Derecho y Redes Sociales*, Aranzadi, Pamplona, pp. 23-37.

John PALFREY y Urs GASSER (1998), *Born Digital: Understanding the First Generation of Digital Natives*, Basic Books, New York.

Antonia PANIZA FULLANA (2009), "Cuestiones jurídicas entorno a las redes sociales: Uso de datos personales para fines publicitarios y protección de datos de menores", *Revista Española de Protección de Datos*, 6, pp. 41-68.

Fernando PANTALEÓN PRIETO (2000), "Cómo repensar la responsabilidad civil extracontractual (También la de las Administraciones Públicas)", en Juan Antonio MORENO MARTÍNEZ (Coord.), *Perfiles de la Responsabilidad Civil en el nuevo Milenio*, Dykinson, Madrid, pp. 437-465.

Cándido PAZ ARES (2000) "El comercio electrónico (una breve reflexión de política legislativa) en Rafael MATEU DE ROS y Juan Manuel CENDAYA (Coords.), *Derecho de Internet*, Aranzadi, Pamplona, pp. 85-98.

Miquel PEGUERA POCH (2002), "La exclusión de responsabilidad civil por contenidos ajenos en Internet", *Contenidos Ilícitos y Responsabilidad de los Prestadores de Servicios de Internet, Revista de Derecho y Proceso Penal*, monografía núm. 8, pp. 25-64.

--- (2007) *La exclusión de responsabilidad de los intermediarios en Internet*, Comares, Granada.

Robert C. POST (2001), "Three Concepts of Privacy", *Faculty Scholarship Series*, núm. 185 (http://digitalcommons.law.yale.edu/fss_papers/185/), pp. 2087-2098.

Jeffrey ROSEN (2000), *The Unwanted Gaze: The Destruction of Privacy in America*, Random House, New York.

Antoni RUBÍ PUIG (2010) "Derecho al honor online y responsabilidad civil de ISPs, *InDret* 4/2010, (www.indret.com).

Pablo SALVADOR CODERCH (1990) *El mercado de las ideas*, Centro de Estudios Constitucionales, Madrid.

Pablo SALVADOR CODERCH, Antoni RUBÍ PUIG y Pablo RAMÍREZ SILVA (2011), "Imágenes veladas. Libertad de información, derecho a la propia imagen y autocensura de los medios", *InDret* 1/2011 (www.indret.com).

Patricia SÁNCHEZ ABRIL (2007), "A (my)Space of One's Own: On Privacy and Online Social Networks", *Northwestern Journal of Technology & Intellectual Property*, núm. 6 (ecopy at papers.ssrn.com/sol3/papers.cfm?abstract_id=1392285), pp. 73-88.

Paul M. SCHWARTZ (2009), "From Victorian Secrets to Cyberspace Shaming", *University of Chicago Law Review*, núm. 79, pp. 1407-1448.

Daniel J. SOLOVE (2007), *The Future of Reputation: Gossip, Rummor and Privacy on the Internet*, Yale.

Daniel J. SOLOVE y Chris Jay HOOFNAGLE (2006), "A Model Regime of Privacy Protection", *University of Illinois Law Review*, núm. 2, pp. 357-404.

Kim TAIPALE (2003), "Secondary Liability on the Internet: Towards a Performative Standard for Constitutive Responsibility", (www.advancedstudies.org/).

Adam THIERER (2009), "Dialogue: The Future of online Obscenity and Social Networks", (http://arstechnica.com/tech-policy/news/2009/03/a-friendly-exchange-about-the-future-of-online-liability.ars/).

James TUMBRIDGE (2009), "Defamation - The Dilemma for Bloggers and their Commenters", *European Intellectual Property Review (Eipr)*, núm. 31, pp. 505-507.

Mónica VILASAU SOLANA (2009), "¿Hasta dónde deben regularse las redes sociales?", *Revista Española de Protección de Datos*, núm. 6, pp. 105-138.

Mónica VILASAU SOLANA (2010) "Privacidad, redes sociales y factor humano", en Artemi RALLO LOMBARTE y Ricard MARTINEZ MARTINEZ (Coords.), *Derecho y Redes Sociales*, Aranzadi, Pamplona, pp. 55-83.

Anne WEST, Jane LEWIS & Peter CURRIE (2009), "Student's Faceboof "Friends": Public and Private Spheres", *Journal of Youth Studies*, núm. 12(6), pp. 615-627.

Alan F. WESTIN (1967), *Privacy and Freedom*, Atheneum Press, New York

Raquel XALABARDER (2002),"Infracciones de la propiedad intelectual y la Digital Millenium Copyright Act", *Contenidos Ilícitos y Responsabilidad de los Prestadores de Servicios de Internet*, *Revista*

*de Derecho y Proceso Penal*, monografía núm. 8 , pp. 119-142.

Christopher S. YOO (2010), "Free Speach and the Myth of the Internet as an Unintermediated Experience", *George Washington Law Review*, núm. 78, pp. 697-756.

Shamyang ZHAO, Sherri GRASMUC. & Jason MARTIN (2008) "Identity Construction on Facebook: Digital empowerment in Anchored relationships", *Computers in Human Behaviour*, 25(5), pp. 1816-18.