Recibido: 08-01-2013 / Revisado: 08-02-2013
Aceptado: 23-03-2013 / Publicado: 01-09-2013

DOI: http://dx.doi.org/10.3916/C41-2013-20

● Lucía Tello
Madrid (España)

Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook

Intimacy and «Extimacy» in Social Networks. Ethical Boundaries of Facebook

RESUMEN

El presente trabajo analiza cómo ciertas herramientas de Facebook, modelo de las nuevas tecnologías de la información, han derivado en la vulneración de algunos planteamientos éticos vigentes hasta el momento. Este paradigma comunicativo que encuentra su máxima expresión en las redes sociales y la tecnología 2.0, implica un replanteamiento de los principios de la ética informativa relativos a la salvaguarda de la intimidad, la protección de la vida privada y el resguardo de la propia imagen. Esta investigación estudia cómo estas áreas no solo se ven afectadas por los cambios tecnológicos y la propia naturaleza de la fuente informativa, sino por la confianza y desconocimiento de los usuarios, quienes dan primacía a la comunicación por encima de la intimidad. Este fenómeno denominado «extimidad» por Jacques Lacan, se traduce como la intimidad hecha pública a través de las nuevas redes de comunicación o intimidad expuesta. En nuestro análisis expondremos los resortes a través de los cuales se quebranta nuestra privacidad en Facebook, especialmente por medio de la captación de pautas de comportamiento, el empleo de datos derivados de los perfiles, los cambios en la política de privacidad y el reconocimiento facial, avalando su transgresión con documentación derivada de investigaciones realizadas por organismos internacionales. En resumen, analizar la vulneración de la intimidad en las redes sociales y entender qué medidas pueden implementarse para defender nuestros derechos son el objetivo de esta comunicación.

ABSTRACT

The current paper aims to analyze how certain Facebook settings, model of new Information and Communication Technologies (ICT), have turned into an infringement of some existing privacy Ethical principles. This totally changed and modern paradigm has its clearest expression in recent Web 2.0, and omnipotent Communication Technology, and implies the reconsideration of each Ethical Principles, especially those related to Intimacy and Image Protection. Our research explains not just how these areas are affected by technological changes but also the way these imperative ethical principles are violated because users ignorance and confidence. This carefree attitude and the increasing communicative relevance have given networking precedence over Intimacy protection. The result of this action has been denominated «Extimacy» according to the author Jacques Lacan, a concept which can be translated as public Intimacy through networking activities, namely, exposed Intimacy. The goal we aim to achieve is to illustrate the different ways our Privacy can be damaged by some Facebook measures (as Privacy Policies Change, collecting tendencies of consumption, the use of private data and revealing users confidence). Likewise, these arguments will be endorsed by international researches focused on Facebook privacy violations, which we are going to expose to understand how citizens can carry out different actions to defend our Intimacy and Image Rights.

PALABRAS CLAVE / KEYWORDS

Internet, ética, Facebook, intimidad, extimidad, vulneración, redes sociales.
Internet, ethics, Facebook, intimacy, extimacy, social networking.

❖ Dra. Lucía Tello-Díaz es Doctora Honorífica del Departamento de Periodismo III de la Facultad de Ciencias de la Información de la Universidad Complutense de Madrid (España) (lucytel1959@hotmail.com).

1. Introducción y estado de la cuestión

En la era de las nuevas tecnologías los límites de la intimidad y la vida privada se han visto diluidos. Principios éticos asumidos por la sociedad como inalienables se han visto sometidos a nuevas maneras de vulneración, de suerte que la mayor parte de los estados no poseen fórmulas legales para combatirlas o erradicarlas. Tal es el caso de la intimidad y la vida privada de las personas, cuyos contornos se han distorsionado al verse sus marcos de actuación convencionales superados por la nueva realidad comunicativa: «como hipnotizados, los beneficios percibidos de las redes sociales tienen más peso que los riesgos de la información personal revelada» (Debatin, Lovejoy & al. 2009: 100). La generalidad de los usuarios desconoce que sus datos personales, las elecciones que realiza en los distintos buscadores, los productos que compra o los enlaces que visita son almacenados y empleados para fines de variada naturaleza sin su consentimiento ni conocimiento. Tal como ilustraremos, específicamente invasivas serán las técnicas empleadas para monitorizar la información obtenida en la red social Facebook, cuya arquitectura favorece la pérdida de control de la intimidad a través de la captación de pautas de comportamiento, el empleo de datos derivados de los perfiles, los cambios en la política de privacidad sin consentimiento y el reconocimiento facial. Estos aspectos insólitos hasta el momento han provocado que países como Irlanda, Estados Unidos, Canadá y Alemania hayan elaborado informes para valorar el grado de intromisión de la compañía norteamericana en la vida privada de los ciudadanos, quienes no tienen conocimiento de adónde van a parar sus datos ni cuál es el objeto que persiguen quienes hacen acopio de ellos. Como mostraremos, estos datos son claves no solo por ser personales, sino porque proporcionan información de los individuos que éstos creen inadvertida, y porque los destinatarios de tales datos son desconocidos por los propios individuos. Pese a que las redes sociales favorecen la interacción promoviendo «el mantenimiento y creación de capital social» (Ellison, Steinfield, & al. 2007: 1.161), lo cierto es que las contraprestaciones de su uso en materia de intimidad, desbordan los preceptos éticos imperantes hasta la actualidad.

2. Material y métodos

La metodología que emplearemos será el análisis de contenido de los informes elaborados por organismos internacionales a colación de la vulneración de los principios éticos de intimidad y vida privada en Facebook, así como los artículos científicos y en prensa relativos a la misma temática. Nos valdremos de los informes publicados por los estados que se han anticipado en la regulación de la intromisión en la intimidad a través de las redes sociales, tales como el Alto Comisionado alemán, la Comisión de Privacidad de Canadá, la Federal Trade Commission de los Estados Unidos y la Comisión de Protección de Datos de Irlanda, los cuales nos otorgarán las líneas de actuación básicas para delinear los contornos de los abusos de Facebook en materia de privacidad. Para ello emplearemos una metodología cualitativa deductiva, obrando de lo general a lo particular, analizando las categorías relativas a los términos clave «intimidad», «privacidad» y «propia imagen» y realizando un análisis de contenido de los aspectos concretos que cada país ha priorizado con respecto a esta temática. Por tanto, analizaremos una muestra limitada pero representativa de la documentación realizada sobre la privacidad en Facebook. El motivo que nos ha empujado a estudiar estos países concretos viene precipitado por el hecho de que son los únicos que han publicado estudios relativos a la intimidad en las redes sociales, entendiendo que en el futuro la senda abierta por estos países se ampliará con nuevas investigaciones. Finalmente, emplearemos como material de apoyo estudios previos realizados en relación con nuestra temática en ARPN Journal of Systems and Software, Cyberpsychology, Behavior, and Social Networking, Journal of Computer-Mediated Communication e igualmente en Harvard Business Review para entender el alcance ético y la importancia de las redes sociales.

3. Análisis y estudio: el contexto de las redes sociales y la comunicación global

Las actividades humanas son sociales, de ello deriva que desde hace siglos se haya desarrollado un conglomerado de redes que proveen circuitos de interacción interpersonal, desde el establecimiento del correo a la generalización de la imprenta. Esta interconexión no es una realidad de nuestra sociedad actual, ya que el comercio, la búsqueda de materias primas y el contacto con otros individuos forma parte de nuestra naturaleza, aunque las tecnologías de que disponemos hoy en día hayan dotado al concepto de intercomunicación de un sentido global:

Está surgiendo un nuevo tipo de relaciones entre las personas que no conoce fronteras. La globalización está transformando nuestras vidas. Esta es la característica que mejor define la sociedad en la que vivimos, la que le imprime un rasgo más distintivo (Javaloy & Espelt, 2007: 642).

Gracias a Internet la comunicación global es posible, «de manera global cada vez estamos más amplia-

mente interconectados» (Ehrlich & Ehrlich, 2013: 1). La conexión de individuos y la transferencia de datos son ahora tanto cuantitativa como cualitativamente superiores. Desde que Tim O´Reilly definiera el modelo de comunicación on-line en «What is the Web 2.0. Patterns and Business Models for the Next Generation of Software» se ha sobrepasado el concepto de mero vínculo: «Como la forma de las sinapsis en la mente […] la Red de las conexiones crece orgánicamente como resultado de la actividad colectiva de todos los usuarios de la web» (O´Reilly, 2007: 22). Así la conectividad es ahora más real que nunca: «Ha habido un correspondiente arrebato de interés en la ciencia de las redes. Los investigadores están estudiando las redes de personas, compañías, juntas directivas, ordenadores, instituciones financieras –cualquier sistema que conste de muchos componentes conectados– para buscar principios comunes» (Morse, 2003: 1).

El auge de la interconexión en la era de la Web 2.0 implica un continuo feed-back entre emisores y receptores, aunque también supone la perversión del concepto de intimidad por parte de los usuarios, quienes valoran por encima de su salvaguarda, su publicidad: «Ha cambiado la forma en que nos construimos como sujetos, la forma en que nos definimos. Lo introspectivo está debilitado. Cada vez nos definimos más a través de lo que podemos mostrar y que los otros ven. La intimidad es tan importante para definir lo que somos que hay que mostrarla. Eso confirma que existimos» (Pérez-Lanzac & Rincón, 2009).

Esta debilitación del ámbito introspectivo ya fue enunciada por Jacques Lacan en 1958 bajo el término de «extimidad», un concepto que entronca con la manifestación pública en la era de las redes sociales, del contenido otrora íntimo:

El término «extimidad» rompe el binario interior-exterior y designa un centro exterior a lo simbólico, lo que conlleva la producción de un hiato en el seno de la identidad consigo mismo, vacío que la identificación no llegará a colmar. Lo «éxtimo» podría definirse como ese objeto extraño que habita en ese Otro que es el sujeto para sí mismo y que eventualmente puede localizarse afuera en el otro (Extimidad. El curso de orientación lacaniana, 2012).

Esta «extimidad» y el auge de la transferencia de datos personales han derivado en que las redes sociales generen una ingente cantidad de información personal, a la postre útil para quienes basan su profesión en la recopilación de datos de los usuarios. En este sentido:

> La generalidad de los usuarios desconoce que sus datos personales, las elecciones que realiza en los distintos buscadores, los productos que compra o los enlaces que visita son almacenados y empleados para fines de variada naturaleza sin su consentimiento ni conocimiento. Tal como ilustraremos, específicamente invasivas serán las técnicas empleadas para monitorizar la información obtenida en la red social Facebook, cuya arquitectura favorece la pérdida de control de la intimidad a través de la captación de pautas de comportamiento, el empleo de datos derivados de los perfiles, los cambios en la política de privacidad sin consentimiento y el reconocimiento facial.

Internet se ha convertido en la Biblia de los publicitarios, que rastrean a los potenciales consumidores por las comunidades on-line más relevantes, en función del producto que se quiera promocionar, identificando a los líderes de opinión, observando las interacciones de los usuarios (social media monitoring). Frente a la búsqueda del target de los tradicionales estudios de mercado, Internet ofrece de manera creciente una información más precisa sobre las características y las preferencias de esos nuevos nichos de espectadores (Lacalle, 2011:100).

Estos datos además de informar acerca de preferencias de los usuarios, revelan parte de su intimidad. La información de los usuarios no solo permite «articular y hacer visible su red de amistades» (Kanai, Bahrami, & al., 2012), ni establecer «conexiones con otras

personas que de cualquier otra manera no podrían ser hechas» (Boyd & Ellison, 2007: 210), sino que «provee de un gran poder predictivo» (Jones, Settle & al., 2013) acerca de tendencias y actitudes. Incluso cuando los «individuos prefieren mantener en la intimidad algunos detalles como sus preferencias políticas o su orientación sexual» (Horvát, Hanselmann & Hamprecht, 2012), la información revelada por sus contactos puede desvelar lo que el usuario elige mantener en secreto. Aunque se considere que el mayor riesgo de las redes radica en que «pueden facilitar comportamientos asociados con intrusiones relacionales obsesivas» (Marshall, 2012: 521), otra amenaza inadvertida para los usuarios se halla en la misma formulación de las redes y en la recopilación de datos que éstas realizan.

Es preocupante la erosión de la intimidad en numerosos frentes durante los últimos años. La culpa es de tres grandes fuerzas: está la tecnología en sí, que permite seguir la pista de una vida entera y de cualquier persona con una precisión instantánea ante la que a un general de la Stasi se le haría la boca agua. Luego está la búsqueda de beneficios, que hace que las empresas hagan un seguimiento cada vez más detallado de los gustos y costumbres de sus clientes, para personalizar la publicidad. Y por último están los gobiernos, que encuentran maneras de hacerse con muchos de esos datos, además de reunir montañas de ellos en sus propios servidores.

3.1. La revolución llega a las redes sociales: el nacimiento de Facebook

La dispersión de los usuarios y la constante reformulación tecnológica definen las redes on-line. Así «la Web 2.0 vuelve a dar protagonismo a la conversación social, impulsada por la metamorfosis profunda y continua de las tecnologías de la comunicación» (Ruiz & Masip, 2010: 9). En este contexto nace Facebook, la mayor red social de Internet. Aunque GeoCities o MySpace fueran espacios consolidados, Facebook (creada en 2003 por Mark Zuckerberg) se implantó revolucionando el concepto de interacción: «La proliferación de medios sociales, donde la audiencia crea, comparte y consume información de forma muy diferente a como lo venía haciendo, ha derivado, por un lado, en la desaparición de la intermediación –hoy los usuarios tienen acceso directo a las fuentes de información– y, por otro, en la generación abundante de contenido de muy diversa procedencia» (Yuste, 2010: 86).

Según el último informe «Hábitos de redes sociales en España», Facebook ha desbancado al resto de redes sociales en nuestro país (Libreros, 2011), siendo empleado por el 95% de los usuarios, (seguido por YouTube, Tuenti y Twitter), para enviar mensajes privados (60%), mensajes públicos (50%), compartir y subir fotos (37%), actualizar el perfil (32%) y hacerse fan o seguir marcas comerciales (26%) (Libreros, 2011). Serán estas cinco actividades las que muestren tendencias y establezcan parámetros de un determinado perfil.

3.2. La vulneración de la intimidad y la protección de datos en Internet

Conexión a Internet y una fuente de alimentación son los dos elementos que se necesitan para acceder a nuestra información desde cualquier parte del mundo. La facilidad que proporcionan las nuevas tecnologías para la reproductibilidad de los datos hace que éstos estén disponibles para todo aquel que desee consultarlos y emplearlos: Es preocupante la erosión de la intimidad en numerosos frentes durante los últimos años. La culpa es de tres grandes fuerzas: está la tecnología en sí, que permite seguir la pista de una vida entera y de cualquier persona con una precisión instantánea ante la que a un general de la Stasi se le haría la boca agua. Luego está la búsqueda de beneficios, que hace que las empresas hagan un seguimiento cada vez más detallado de los gustos y costumbres de sus clientes, para personalizar la publicidad. Y por último están los gobiernos, que encuentran maneras de hacerse con muchos de esos datos, además de reunir montañas de ellos en sus propios servidores (Garton, 2010).

Cuando se marca una preferencia, se muestra interés por un anuncio o se elige una aerolínea, los «rastros» de estas actividades delatan gustos y hábitos de consumo. Lo que antes era personal, ahora se torna colectivo: «La masificación de las redes sociales ha generalizado un concepto que los expertos llaman «extimidad», algo así como hacer externa la intimidad, y que tiene su origen en el auge de los «reality shows» y de la Web 2.0» (Pérez-Lanzac & Rincón, 2009). Si por intimidad entendemos la información personal que no debe ser revelada o hecha pública (Kieran, 1998: 83), o aquello que «seria y legítimamente queremos proteger de la publicación» (Olen, 1988: 61), el que sea posible rastrear nuestra presencia en Internet, nuestra «extimidad», implica la vulneración de nuestros derechos: «Renunciar a la intimidad en las compras por Internet parece benigno. Renunciar a ella en los vuelos puede parecer razonable; incluso puede aparentar no ser problemático un circuito cerrado de televisión que opera en lugares públicos. Sin embargo, cuando todo se suma nos encontramos con que no tenemos ninguna intimidad en absoluto» (Johnson, 2010: 193).

4. Formas de vulneración de la intimidad en Facebook

En las redes sociales muchos aspectos de la intimidad quedan desprotegidos, especialmente en Facebook, la plataforma con mayor acceso a gran cantidad de datos personales. Facebook recopila esta información a través de distintas opciones (settings), entre ellas las solicitadas al cumplimentar los datos del perfil o la exploración a través de su célebre opción «me gusta»: «Los «me gusta» de Facebook pueden ser usados para predecir automáticamente y con exactitud un rango de características personales altamente sensibles, incluidas: la orientación sexual, la etnicidad, las perspectivas políticas y religiosas, rasgos de la personalidad, inteligencia, felicidad, el uso de sustancias adictivas, la separación de los padres, edad y género» (Kosinskia, Stillwella & Graepelb, 2013). Aunque existen más de cincuenta y siete patrones de datos personales susceptibles de ser obtenidos por Facebook (Facebook´s Data Pool, 2012), analizaremos únicamente las medidas que han suscitado la crítica por parte de organismos competentes en distintos países, como la «captación de pautas de comportamiento», el «empleo de datos derivados de los perfiles» y los «cambios en la política de privacidad sin consentimiento y reconocimiento facial».

4.1. Captación de pautas de comportamiento

La monetización de los datos personales es uno de los aspectos más controvertidos de Facebook, ya que implica no solo la revelación de información personal, sino el provecho económico de una información sustraída sin consentimiento expreso de sus propietarios: «En agosto de 2009 se publicó un informe en el que se demostraba que Facebook había enviado a sus anunciantes los nombres, edades y profesión de todos aquellos usuarios que «clickeaban» en sus anuncios» (La historia oculta de Facebook, 2010). Esta cesión de información a empresas con intereses ajenos es, sin embargo, desconocido por la generalidad de usuarios de la red social. En palabras del propio Zuckerberg: «Tengo 4.000 correos electrónicos y sus contraseñas, fotos y números de seguridad social, la gente confía en mí» (La historia oculta de Facebook, 2010). En 2009 el control de datos de los usuarios provocó el surgimiento de críticas en defensa de la autoridad del interesado para reclamar su derecho a la intimidad. La Federal Trade Commission (FTC) de los Estados Unidos recibió un gran número de denuncias de usuarios solicitando medidas para que la empresa explicara qué información iba a ser compartida. La propia Comisión exigió que Facebook asegurase la conservación de la privacidad de sus usuarios, así como: «Cumplir sus promesas en el futuro, incluidas las de ofrecer a los consumidores información clara y prominente y la de obtener el consentimiento expreso de éstos antes de que su información sea compartida más allá de los acuerdos de privacidad que han establecido» (Facebook settles FTC Charges, 2011).

A colación de las críticas emitidas, Facebook lanzó una nueva arquitectura que permitía personalizar el nivel de seguridad. Si bien Elliot Schrage, Vicepresidente de Política Pública, mostró el interés de Facebook en otorgar mayor control al usuario, las nuevas herramientas para el control de la información adquirieron una complejidad inusitada para una red social. Para borrar los datos indeseados: «es necesario hacer click en más de cincuenta botones de privacidad, los cuales requieren elegir entre un total de más de 170 opciones» (Bilton, 2010).

4.2. Empleo de datos derivados de los perfiles

El perfil en las redes sociales es el carnet de identidad del usuario, su información es de carácter privado y en consecuencia confidencial, si no existe consentimiento por parte del interesado. Sin embargo, la confidencialidad de los datos contenidos en el perfil se ha diluido, convirtiéndose en reclamo para las empresas. El aumento de intereses creados por terceras partes ha derivado en la masificación de los mensajes publicitarios, y la personalización de éstos. En vista de ello, la Comisión de Privacidad de Canadá denunció a

Facebook por oscuridad en el tratamiento de los datos privados en 2009, advirtiendo que determinaría si su actividad infringía la legalidad. Como respuesta, la empresa resolvió modificar de nuevo su política de privacidad: «El portal ha anunciado que desde ahora las aplicaciones desarrolladas por terceras partes deberán especificar a qué datos personales acceden y solicitar permiso para difundirlos. Facebook exigirá a las aplicaciones que especifiquen las categorías de información de los usuarios a las que desean acceder y que obtengan el consentimiento de éstos antes de que se compartan esos datos» (Más intimidad en Facebook, 2009).

Si bien estas medidas fueron tomadas en 2009, Facebook ha realizado distintas acciones que infringen la normativa de protección de datos asumida por la propia empresa:

Facebook prometió que los usuarios podían restringir su información a una audiencia limitada, empleando ciertas opciones de privacidad. Pero lo cierto es que incluso cuando un usuario entra en la página central de privacidad de Facebook, y en el enlace de controlar quién puede ver su perfil e información personal limita el acceso a cierta gente –por ejemplo, «solo amigos»– la opción del usuario es inefectiva cuando llega a aplicaciones de terceras partes que emplean los amigos del usuario (Fair, 2011).

Esta realidad redunda en el hecho de que los usuarios no son informados oportunamente acerca del destino de sus datos, ni tampoco las empresas que van a hacer uso de ellos: «La gente no sabe cómo pueden ser compartidos sus datos personales. Se acaba compartiendo su información privada con personas no autorizadas por su desconocimiento […] la complejidad de los marcos de privacidad y la ausencia de control otorgado a los usuarios es igualmente responsable de la transferencia involuntaria de información» (Zainab & Mamuna, 2012: 124).

La dación de información a terceras partes hace que otras empresas pueden tener acceso a datos no relacionados con la actividad que persiguen. En lo concerniente a las aplicaciones a las que se pueden acceder a través de Facebook, ha vuelto a surgir controversia por el uso indebido de los datos personales: «Durante un largo período de tiempo después de que Facebook empezara a publicar aplicaciones en su sitio, se engañó a la gente acerca de cuánta información era compartida con las aplicaciones que usaban. Facebook decía que cuando la gente autorizaba una aplicación, ésta solo tendría la información de los usuarios que requiere para trabajar. [Sin embargo] las aplicaciones podían acceder a toda la información del usuario –incluso información sin relación con la operación de la aplicación–» (Fair, 2011).

Si el caso de las aplicaciones resulta llamativo, el de los anunciantes es aún más relevante, ya que en los estatutos de Facebook figura expresamente que la compañía no revelará datos personales a ningún anunciante salvo acuerdo expreso con el usuario. Sin embargo este compromiso fue vulnerado durante el intervalo de septiembre de 2008 a mayo de 2010, período durante el cual se ofreció a anunciantes «la identidad de los usuarios que hicieron click en los anuncios» (Fair, 2011).

4.3. Cambios en la política de privacidad sin consentimiento y reconocimiento facial

En 2011 la Comisión de Protección de Datos de Irlanda (DPC) denunció a Facebook por ausencia de nitidez en sus políticas de protección de privacidad. La empresa, con sede internacional en Irlanda, fue instada «a revisar la protección de la privacidad para los usuarios fuera de Norteamérica, [ya que] sus políticas eran demasiado complejas y les faltaba transparencia» (Facebook y Linkedin se comprometen, 2012). No obstante, el irlandés no ha sido el único país que ha entrado en conflicto con la compañía en Europa. El organismo que regula la protección de datos en Alemania ha reabierto la investigación acerca de la tecnología de reconocimiento de caras de Facebook. Johannes Caspar, el Comisionado en Hamburgo, ha afirmado que «el gigante de las redes sociales está recopilando una inmensa base de datos de usuarios ilegalmente» (O´Brien, 2012). El motivo por el que han reabierto las diligencias se resume en la negativa de la empresa a cambiar sus políticas de privacidad: «nos hemos reunido repetidamente con Facebook pero no hemos sido capaces de conseguir su cooperación en este particular, lo cual tiene graves implicaciones para los datos personales» (O´Brien, 2012). Aunque el reconocimiento facial contraviene la política legal de protección de datos europea, la compañía no ha realizado ninguna modificación para adecuar su software a las leyes comunitarias:

La compañía emplea un software analítico para compilar archivos fotográficos de caras humanas, basado en las fotografías subidas por los miembros de Facebook, el cual ha tenido problemas en Europa, donde las leyes de protección de datos requieren del consentimiento explícito de los individuos para ser llevado a la práctica (O´Brian, 2012).

Pese a que las fotografías pueden desetiquetarse y las cuentas pueden ser desactivadas, la permanencia perenne de la información hace que se mantenga en

la base de datos de la compañía indefinidamente, aunque no sea pública. Este hecho, que infringe las leyes de la Unión Europea, ha suscitado controversia en Reino Unido: «Facebook permite a los usuarios «desactivar» sus cuentas. Esto significa que la mayor parte de su información se convertirá en invisible para otros visitantes, pero se almacena en los servidores de Facebook indefinidamente. Esto está a mano de cualquier usuario que cambia de opinión y decide reincorporarse. Puede escribir su antiguo nombre de usuario y contraseña y aparecerá justo en el sitio –será como si nunca lo hubiera dejado–. Pero no todo el mundo quiere otorgar a Facebook el derecho de conservar todos sus datos indefinidamente cuando no los están usando y para otros propósitos obvios. Si quieren borrarla permanentemente, necesitarán dar la vuelta al sitio y borrar todo lo que hayan hecho. Eso incluye cada mensaje en el muro, cada imagen y cada grupo del que fuera miembro. Para un gran usuario de Facebook, esto podría tomarle varias horas. Incluso días. Y esto podría violar el Acta de Protección de Datos de Reino Unido» (King, 2007).

Al crear un perfil en Facebook, el usuario le otorga a la empresa el derecho a almacenar de por vida sus datos. Como menciona la propia Licencia y Términos de uso firmada por cada usuario: «Nos concedes una licencia no exclusiva, transferible, con derechos de sublicencia, libre de derechos de autor, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook» (Facebook Licencia y Términos, n.d.).

En la legislación española los usuarios están amparados por el derecho de cancelación, el cual les permite solicitar a las empresas que eliminen sus datos una vez se ha extinguido la relación entre ambos: «La legislación española prevé, especialmente a través del ejercicio del derecho de cancelación, que un ciudadano pueda solicitar el borrado de todos aquellos datos personales cuya retención no esté amparada por otro derecho. En el caso de una red social, los datos que voluntariamente publicamos en nuestros perfiles deberían ser borrados una vez retiramos nuestro consentimiento» (Romero, 2012). Pese a ello, Facebook también se arroga el derecho de variar la política de privacidad sin previo aviso y sin consentimiento expreso de los miembros de la red, incluso: «algunos datos que los usuarios han designado como privados –como las listas de amigos– han sido hechos públicos amparados por la nueva política» (Fair, 2011). Asimismo: «Ha designado cierta información del perfil de los usuarios como pública cuando había sido sujeta previamente a los marcos restrictivos de privacidad [y] anuló las decisiones previas de privacidad de los usuarios. Haciéndolo, la compañía cambió materialmente la privacidad de la información de los usuarios y retrospectivamente aplicó estos cambios a toda la información previamente recogida» (Fair, 2011).

> «Supongo que podríamos resignarnos y aceptar que el mundo actual es así. La privacidad ha muerto. Acostúmbrate», como aconsejó en una ocasión Scott McNealy, cofundador de Sun Microsystems. O bien podemos defendernos, intentar recuperar parte de nuestra intimidad perdida. Podemos hacerlo fijando nuestras propias normas y compartiéndolas con otros. Podemos hacerlo ejerciendo presión sobre empresas como Facebook, cuya fuente de ingresos, al fin y al cabo, somos nosotros. También podemos exigir a nuestros Gobiernos tres cosas: que frenen sus intromisiones en nuestra intimidad; que regulen mejor a las empresas entrometidas; y que castiguen las infracciones particulares […] Las mismas tecnologías de redes que reducen nuestra privacidad pueden también ayudarnos a defendernos.

Al albor de los excesos en materia de intimidad y vida privada de la compañía, algunas plataformas ciudadanas como «Europe vs Facebook» han emergido con el único objeto de aportar luz y transparencia a la política de privacidad de la empresa norteamericana.

5. Discusión y conclusiones

En vista de la documentación aportada, es legítimo afirmar que Facebook ha obtenido un estatus de privilegio del que ninguna empresa ha sido valedora hasta el momento. Sin embargo, la vulneración de los derechos de los usuarios ha provocado el reclamo para la red social de un control más cercano por parte de los gobiernos y una reformulación de los protocolos de apropiación de imágenes y contenidos sensibles por parte de la empresa. Hemos comprobado cómo su contrato de cesión de derechos ha sido criticado por distintos estados de Europa y por Canadá, a pesar de que la empresa siga manteniendo oscuridad en el tratamiento, transferencia y apropiación de datos de los usuarios. También que muchos ciudadanos han decidido paliar la desregulación en políticas de privacidad denunciando el abuso a organismos competentes en distintos países. Hemos expuesto cómo el desconocimiento y la «extimidad» de los usuarios han provocado que la recolección de datos personales sea en la Web 2.0 más sencillo que nunca: «Proteger el perfil personal», «mantener el nombre fuera de las fotos» y «comprobar la visibilidad» (Boutin, 2010), son elementos que pocos usuarios tienen en cuenta a la hora de realizar actividades en Facebook.

La cesión de datos privados, la complejidad de la arquitectura del sitio, la perpetuidad de almacenamiento o los intereses de terceras empresas, son algunos de los temas controvertidos que implican a Facebook, sin que se haya propuesto un nuevo modelo de regulación de datos privados en la red social. No obstante, la Oficina del Comisionado de Protección de Datos de Irlanda ha realizado un informe donde recoge algunas medidas necesarias para la salvaguarda de los datos privados en Facebook, informe cuyas conclusiones pueden ser generalizadas para amparar la intimidad en la red social, como constituir:

• Un mecanismo de opción informada acerca de cómo es usada y compartida la información de los usuarios en el sitio web, también en relación con aplicaciones de terceras partes.

• Una amplia actualización de la política de usos y privacidad para tener en cuenta las recomendaciones y destino de la información entregada por los usuarios.

• Transparencia y control de los usuarios a través de los llamados plugins sociales y como parte de su interacción diaria con el sitio web.

• La eliminación de la información de usuarios y no usuarios a través de los llamados plugins sociales y más ampliamente el borrado de los datos resultantes de las interacciones del usuario con el sitio web.

• Incremento de transparencia y control del uso de datos personales con fines publicitarios.

• Una forma adicional de notificación para los usuarios en relación con el reconocimiento facial y las sugerencias de etiquetado para que Facebook (Irlanda) se asegure de que se está realizando la mejor práctica según la ley (irlandesa).

• Mejora de la capacidad de control del usuario del etiquetado y publicación en los perfiles de otros usuarios.

• Mejora de la capacidad de control del usuario de su adhesión a grupos por sus amigos […] (Report of Data Protection, 2012).

Hasta que estas medidas se normalicen a nivel internacional, los usuarios pueden recurrir a la autorregulación, mostrando un conocimiento y celo mayores con respecto a las informaciones que quieren difundir: «Supongo que podríamos resignarnos y aceptar que el mundo actual es así. La privacidad ha muerto. Acostúmbrate», como aconsejó en una ocasión Scott McNealy, cofundador de Sun Microsystems. O bien podemos defendernos, intentar recuperar parte de nuestra intimidad perdida. Podemos hacerlo fijando nuestras propias normas y compartiéndolas con otros. Podemos hacerlo ejerciendo presión sobre empresas como Facebook, cuya fuente de ingresos, al fin y al cabo, somos nosotros. También podemos exigir a nuestros Gobiernos tres cosas: que frenen sus intromisiones en nuestra intimidad; que regulen mejor a las empresas entrometidas; y que castiguen las infracciones particulares […] Las mismas tecnologías de redes que reducen nuestra privacidad pueden también ayudarnos a defendernos (Garton, 2010).

En la actualidad, y hasta que exista una regulación unitaria, habrá que reclamar a los usuarios la protección de sus derechos, aunque ello implique decidir en qué términos y de qué modo ceden sus datos.

Referencias

ACEBEDO, R. (2011). *La historia de Facebook desde adentro*. La Tercera, 29-01-2011. (www.latercera.com/noticia/tendencias/2011/01/659-341582-9-la-historia-de-facebook-desde-adentro.shtml) (10-11-2012).

BILTON, N. (2010). Price of Facebook Privacy? Start Clicking. The New York Times, 12-05-2010. (www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=0) (10-10-2012).

BOUTIN, P. (2010). 3 Essential Stops to Facebook Privacy. The New York Times, 13-05-2010. (http//gadgetwise.blogs.nytimes.com/2011/06/21/3-essential-steps-to-facebook-privacy) (05-11-2012).

BOYD, D. & ELLISON, N. (2007). Social Network Sites: Definition, History and Scholarship. Journal of Computer-Mediated Communication 13, 210-230. (DOI:10.1111/j.1083-6101.2007.00393.x) (28-03-2013).

DEBATIN, B. LOVEJOY, J.P. HORN, A.K. HUGHES, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended

Consequences. *Journal of Computer-Mediated Communication. 15, 1,* 83-108. (DOI:10.1111/j.1083-6101.2009.01494.x). (02-11-2012).

Ehrlich, P. & Ehrlich, A. (2013). Can a Collapse of Global Civilization be Avoided? Proceedings of *The Royal Society B. 280: 20-122845. Royal Society Publishing. Biological Sciences.* (http://dx.doi.org/10.1098/rspb.2012.2845) (29-03-2013).

El Economista (30-05-2010). *La historia oculta de Facebook.* (www.eleconomista.es/interstitial/volver/acierto/telecomunicaciones-tecnologia/noticias/2188124/05/10/La-historia-oculta-de-Facebook-La-gente-confia-en-mi-son-tontos-del-culo.html) (04-11-2012).

Ellison, N., Steinfield, L. & Cliff, C. (2007). The Benefits of Facebook «Friends»: Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer-Mediated Communication, 12,* 1.143-1.168. (DOI:10.1111/j.1083-6101.2007.00367.x) (27-03-2013).

El Mundo (Ed.) (2012). Facebook y Linkedin se comprometen a reforzar su privacidad. *El Mundo, 29/06/2012.* (www.elmundo.es/elmundo/2012/06/29/navegante/1340955573.html) (04-11-2012).

El País (Ed.) (2009). Más intimidad en Facebook. *El País, 27-08-2009.* (http//tecnologia.elpais.com/tecnologia/2009/08/27/actualidad/1251363663_850215.html) (01-11-2012).

Facebook (Ed.) (2012). *Facebook s Data Pool. Europe vs Facebook. 03-04-2012.* (http//europe-v-facebook.org/EN/Data_Pool/data_pool.html) (03-11-2012).

Fair, L. (2011). *The FTC's settlement with Facebook. Where Facebook went wrong.* Federal Trade Commission Protecting America´s Consumers. 29-11-2011. (http//business.ftc.gov/blog/2011/11/ftc%E2%80%99s-settlement-facebook-where-facebook-went-wrong) (02-11-2012).

Federal Trade Commission (Ed.) (2011).Facebook settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises. *Federal Trade Commission Protecting America s Consumers, 29-11-2011.* (http//ftc.gov/opa/2011/11/privacysettlement.shtm) (03-10-2012).

Garton, T. (2010). Facebook: restablecer la privacidad. *El País, 11-10-2010.* (http//elpais.com/diario/2010/10/11/opinion/1286748011_850215.html) (04-10-2012).

González-Gaitano, N. (1990). *El deber de respeto a la intimidad. Información pública y relación social.* Pamplona: EUNSA.

Horvát E.A., Hanselmann M. & al. (2012). One Plus One Makes Three (for Social Networks). *PLoS ONE 7(4),* e34740. (DOI: 10.1371/journal.pone.0034740) (27-03-2013).

Johnson, D.G. (2010). *Ética informática y ética e Internet.* Madrid: Edibesa.

Jones, J.J., Settle, J.E., Bond R.M. & al. (2013). Inferring Tie Strength from Online Directed Behaviour. *PLoS ONE 8(1),* e52168. (DOI:10.1371/journal.pone.0052168) (29-03-2013).

Kanai, R., Bahrami, B., Roylance, R. & al. (2012): *Online Social Network Size is Reflected in Human Brain Structure.* Proceedings of The Royal Society B. 280: 20122845. Royal Society Publishing. Biological Sciences, 2012 279. (DOI:10.1098/rspb.2011.1959) (28-03-2013).

Kieran, M. (Ed.). (1998). *Media Ethics*. London: Routledge.

King, B. (2007). Facebook Data Protection Row. *Channel 4, 17-11-2007.* (www.channel4.com) (01-11-2012).

Kosinskia M., Stillwella, D. & Graepelb, T. (2013). *Private Traits and Attributes are Predictable from Digital Records of Human Behaviour. Proceedings of the National Academy of Sciences (PNAS).* University of California, Berkeley. (DOI:10.1073/pnas.1218772110) (29-03-2013).

Lacalle, C. (2011). La ficción interactiva. Televisión y Web 2.0. *Ámbitos, 20.*

Libreros, E. (2011). *Las redes sociales en España 2011.* IEDGE, 01-12-2011. (http//blog.iedge.eu/direccion-marketing/marketing-interactivo/social-media-marketing/eduardo-liberos-las-redes-sociales-en-espana-2011) (02-11-2012).

López-Reyes, Ó. (1995). *La ética en el periodismo. Los cinco factores que interactúan en la deontología profesional.* República Dominicana: Banco Central.

Marshall, T. (2012): Facebook Surveillance of Former Romantic Partners: Associations with PostBreakup Recovery and Personal Growth. *Cyberpsychology, Behavior and Social Networking, 15,* 10 (DOI:10.1089/cyber.2012.0125) (29-03-2013).

Morse, G. & Watts, D. (2003). The Science behind Six Degrees. *Harvard Business Review Online,* Febrero. (http//hbsp.harvard.edu/b02/en/hbr/hbrsa/current/0302/article) (05-11-2012).

Olen, J. (1988). *Ethics in Journalism. Englewood Cliffs.* New Jersey: Prentice Hall.

O'Brien, K. (2012). Germans Reopen Investigation on Facebook Privacy. *The New York Times, 15-08-2012.* (www.nytimes.com/2012/08/16/technology/germans-reopen-facebook-privacy-inquiry.html) (01-11-2012).

O´Reilly, T. (2007). What is the Web 2.0. Design Patterns and Business Models for the Next Generation of Software. *Munich Personal RePEc Archive (MPRA),* 4.580, 07-11-2007. (http//mpra.ub.uni-muenchen.de/4580) (05-11-2012).

Pérez-Lanzac, C. & Rincón, R. (2009). Tu «extimidad» contra mi intimidad. *El País, 24-03-09.* (www.elpais.com) (20-10-2012).

Report of Data Protection Audit of Facebook Ireland Published (2012). *Oficina del Comisionado de Protección de Datos de Irlanda* (www.dataprotection.ie/viewdoc.asp?DocID=1175) (02-11-2012).

Romero-Coloma, A.M. (1987). *Derecho a la intimidad, a la información y proceso penal*. Madrid: Colex.

Romero, P. (2012). A las redes sociales les cuesta 'olvidar'. *El Mundo, 05-03-2012.* (www.elmundo.es/elmundo/2012/02/20/navegante/1329751557.html) (03-11-2012).

Ruiz, C., Masip, P., Micó, JL. & al. (2010). Conversación 2.0 y democracia. Análisis de los comentarios de los lectores en la prensa. *Comunicación y Sociedad, XXIII, 2.*

Varios (Ed.). *Declaración de licencia y términos de uso del sitio web de Facebook.* (www.facebook.com/legal/terms) (05-11-2012).

Varios (2007). *Psicología social.* Madrid: McGraw Hill.

Warren, S. & Brandeis, L. (1890). *El derecho a la intimidad.* Madrid: Civitas.

Watts, D.J. (2004). *Six Degrees. The Science of a Connected Age. (Primera edición de 1971).* New York: W.W. Norton & Company.

Yuste, B. (2010). Twitter, el nuevo aliado del periodista. *Cuadernos de Periodistas, diciembre, 86.* Madrid: Asociación de la Prensa de Madrid.

Zainab, A. & Mamuna, K. (2012). Users' Perceptions on Facebook's Privacy Policies. ARPN *Journal of Systems and Software, 2, 3.* (http//scientific-journals.org) (DOI.10.1111/j.1083-6101.2009.01494.x).