

Comunicación: el debate en torno a la autorregulación y la cancelación de datos personales en internet

The debate on self-regulation and cancellation of personal data on the Internet

Carmen Sabater Fernández

Universidad de La Rioja

carmen.sabater@unirioja.es

Resumen

La comunicación trata sobre el derecho a la cancelación de datos personales en Internet (conocido popularmente por el “derecho al olvido”) y la necesidad de una normativa regulatoria del uso indiscriminado de la información personal en la Red. Se presenta el contenido de este derecho, la problemática asociada al mismo derivada de la exposición pública y permanencia de la información personal, más allá del objetivo para el que fue recabada, y las propuestas legislativas presentadas en la Unión Europea sobre la actualización de la privacidad de los datos personal y en Estados Unidos, como propuesta *Privacy Bill of Rights*. Si bien, en la primera, se enfatiza en la necesidad de un control posterior de los datos de bloqueo o eliminación, en la segunda se proponen limitaciones al uso indiscriminado de determinada información personal (religiosa, financiera, médica) pero ambas coinciden en conceder un mayor control de los datos personales a los propios usuarios. Por último, se propone la defensa de un área proactiva de la propia privacidad que contemple los derechos subjetivos fundamentales, sin menoscabar la libertad de expresión.

Palabras clave Derecho al olvido. Derecho a la cancelación de datos personales. Protección de la información. Privacidad en Internet.

Abstract

Communication is about the right to cancel personal data on the Internet (known popularly as the "right to forget") and the need for legislation regulating the indiscriminate use of personal information on the Web is presented the content of this right , the problems associated with it derived from public exposure and retention of personal information beyond the purpose for which it was collected, and the legislative proposals in the European Union on updating the privacy of personal data in the United States, as proposed Privacy Bill of Rights. While, at first, it emphasizes the need for further control data block or delete, the second proposed limitations to the indiscriminate use of certain personal information (religious, financial, medical) but both agree grant greater control of personal data to the user. Finally, we propose proactive defense of an area's own privacy that includes fundamental individual rights without undermining the freedom of expression.

Key words: Right to oblivion. Right to cancellation of personal data. Protection of information. Internet Privacy

Fecha recepción: Febrero 2010

Fecha aceptación: Abril 2010

Introducción

José Luis Rodríguez Álvarez, director de la Agencia Española de Protección de Datos, declara que los avances tecnológicos han puesto seriamente en cuestión los sistemas de garantía de la privacidad: "Hoy en día, esas barreras prácticamente no existen. Nuestros datos personales están fácilmente al alcance de cualquiera" (Dávila, 2011)

La identidad digital (también denominada identidad 2.0) ha cobrado un gran protagonismo en los últimos años. La datos se extienden por la red bien por decisión propia a partir de la creación de perfiles en las redes sociales u otros servicios 2.0, bien a partir de la publicación de nuestros datos personales en sites web institucionales o en boletines oficiales y su

indexación en los buscadores. La realidad es que, cada vez más, la información de nuestra identidad real traspasa la frontera de lo privado y se filtra en el espacio público.

La Red genera un ambiente difuso en constante expansión con grandes posibilidades de información y comunicación pero con mayores dificultades para realizar el seguimiento y control de la información personal. Paradójicamente, los datos que eran únicamente propiedad de la persona se extienden a ficheros comerciales, exceden la audiencia y el tiempo para el que fueron creados o se publican por organismos oficiales sin nuestra autorización explícita.

En este contexto, el derecho a la cancelación de los datos personales (conocido popularmente como "el derecho al olvido" o *"right to be forgotten"*) representa la posibilidad de autorregulación de la propia información personal. Marta Sánchez del Departamento Legal de Áudea lo define como el *"derecho de todas las personas a gestionar sus datos personales, en este caso en Internet, estableciendo todos los mecanismos legales necesarios para que desaparezca toda información negativa publicada, así como su indexación en los principales buscadores, con el objetivo de recuperar y controlar nuestra información, garantizando el derecho a la propia imagen, el honor y a la intimidad personal y familiar"* (Sánchez, 2011). Juristas como Guillermo Borda proponen el desarrollo de un auténtico derecho subjetivo sobre la disposición de la vida digital, como facultad de cada ser humano de construir su propia biografía libre de injerencias que puedan dañarlo (Borda, 2011).

Este derecho representa, por tanto, la posibilidad de eliminar la información que sea susceptible de perjudicar la vida personal. El Director de la AEPD, Artemí Rallo, plantea algunas de estas situaciones que pueden perjudicar la vida personal, relacionadas con el ámbito laboral (despidos o procesos de selección), y con el ámbito administrativo (publicación de información sensible en boletines oficiales: indultos, condenas, subvenciones a colectivos de exclusión, etc.).

Los problemas derivados de la recopilación de datos personales derivan fundamentalmente de la conversión de información privada a pública sin el consentimiento del interesado y en la permanencia de la misma en Internet.

Problemática: el traspaso “perpetuo” de lo privado a lo público

La gestión de la identidad digital llega hasta la propia naturaleza de la Red, cuyas características de apertura, expansión y turbulencia se mimetizan en los datos individuales que circulan sobre la información personal. La vida privada cada vez presenta una mayor proyección en el mundo virtual de Internet –en muchas ocasiones, vinculada a actos de terceros- y, a su vez, los hábitos tecnológicos ocupan un mayor espacio de nuestra vida diaria (Rallo, 2010).

La problemática es compleja ya que la identidad digital se conforma desde diversos procesos temporales y diferentes dinámicas biográficas. La vida privada personal convive con la vida pública profesional. El propio entorno de la web 2.0 favorece la introducción de herramientas gestionadas por el propio usuario que deviene, de esta forma, en el responsable del almacenamiento y recopilación de su información. Pero el consentimiento del usuario/a excede los límites voluntarios para los que fue cedida ya que factores como la transmisión y venta a empresas comerciales o la indexación favorecen su localización con una simple búsqueda nominal.

El derecho a la privacidad entra en colisión con la libertad de expresión en un límite siempre difuso. La Agencia Española de Protección de Datos (AEPD) señala que *"La libertad de expresión tiene su límite en el respeto a otros derechos fundamentales"* (Gómez, 2011). En este contexto, se genera la defensa de un área proactiva de elección privada cuyos mecanismos de reivindicación son difíciles de implementar a posteriori.

En contrapartida, compañías como Google señalan que se corre el riesgo de convertir este derecho en un arma de censura, sobre todo cuando se solicita a un motor de búsqueda eliminar un artículo periodístico en el que se hace referencia a un tercero. Actualmente,

Google y la AEPD están en un proceso de litigio ante la Corte española debido a la negativa de la firma estadounidense de retirar ciertos contenidos con información personal más sensible de su buscador.

Por su parte, Elliot Schrage, director de Política para Estados Unidos de Facebook, califica el derecho al olvido como un control de la propia información por parte de los usuarios/as, pero considera que una legislación específica es contraria al desarrollo tecnológico, el libre flujo de la información y la conectividad global. *“Lo que queremos es una orientación, una guía clara, una explicación amplia en cuanto al derecho al olvido, tenemos que ver cómo ofrecer mejores herramientas a la gente [...] La idea de una regla estricta que diga 'derecho al olvido' no es la evolución de la tecnología”* (Sánchez Onofre, 2011)

Estas compañías protegen sus intereses lucrativos ya que el principio que tendría que prevalecer es la decisión voluntario del internauta. La realidad actual es que las filtraciones de lo privado en la esfera pública de Internet no son controlables por el propio usuario, que se ve sometido a una exposición pública que no ha elegido de forma voluntaria. La problemática estriba principalmente en la información que puede atentar contra el respeto a la dignidad personal. Es el caso, por ejemplo, de una mujer cuyo nombre aparecía vinculado a un indulto en los buscadores. Como establece la ley, la resolución fue publicada en el *Boletín Oficial del Estado* (BOE). La digitalización del boletín multiplicó su difusión hasta el infinito. Google convirtió esa conmutación de pena -una noticia de escaso interés salvo, naturalmente, para la afectada- en una noticia pública. Introducir su nombre en el buscador revelaba automáticamente que fue indultada en 1995. Tras solicitar infructuosamente a Google que cancelara sus datos personales, la mujer, indultada 13 años antes, acudió en 2008 a la AEPD que hizo prevalecer sus derechos al tratarse de una información que atentaba contra su dignidad personal (Gómez, 2010).

El usuario/a puede encontrarse en una situación delicada cuando se encuentra con mecanismos costosos y lentos para eliminar una información “confidencial” que no desea que adquiera un alcance público permanente. Precisamente, la normativa europea

pretende facilitar los trámites para el borrado de datos, cuya presencia puede perjudicar o al interesado.

Los problemas se insertan en la biografía individual ya que la información en la Red adquiere un carácter de permanencia, incluso, una vez que se ha extinguido el objeto para el que fue recabado. En la normativa española, la información publicada en boletines oficiales no tendría porqué ser perpetua ya que existen límites tanto temporales (plazos) como de relación con un interés público. Sin embargo, las posibilidades de búsqueda de boletines anteriores o la falta de actualización de algunas webs inciden en la estabilidad de una información sin fecha de caducidad. La historia biográfica del pasado crea unas “huellas” en la vida individual del presente, pudiendo provocar consecuencias en la búsqueda de un trabajo o en la imagen personal. En la *33ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad*, organizada por el *Instituto Federal de Acceso a la Información y Protección de Datos* (IFAI), Marie Hélène Boulanger, de la Comisión Europea, señaló la importancia del tiempo que debe estar la información en la red y declaró que el periodo de retención de la información es un asunto controversial. Su propuesta propone analizar el tema para fijar un periodo de conservación de la información (Dávila, 2011).

Por último, cabe destacar que se presentan mayores dificultades e, incluso, la imposibilidad de retirar la información, cuando ésta es publicada con el consentimiento del propio/a usuario/a ya que ha otorgado la autorización para su publicación. Martínez Ferre (2011) señala que, como regla general, cualquier persona no debe soportar que sus datos personales queden accesibles de forma permanente en Internet como consecuencia de la inclusión de sus datos en los buscadores. Para ello, habría que atender a dos circunstancias:

- La finalidad por la que fueron publicados estos datos. Si ésta fue la de notificación al interesado de un determinado acto administrativo, una vez efectuada ésta, y transcurridos los plazos de ejercicio de los posibles recursos, la finalidad quedaría cumplida, y por tanto no sería necesario el mantenimiento de estos datos para su búsqueda a través de los buscadores.

- La condición de personaje público del titular de los datos, y que el hecho tenga de relevancia pública. En consecuencia cualquier persona o hecho que no reúna estas características no debería soportar por tiempo indefinido la inclusión de sus datos en Internet. Pero los hechos pueden tener un interés público en un determinado momento, dejando de tener este carácter pasado un tiempo.

El derecho a la privacidad se presenta de forma activa y previa al uso de sus datos, y no sólo como la posibilidad de retirar el consentimiento al procesamiento posterior de datos. De esta forma, encontramos dos visiones diferenciadas de este derecho en la administración europea y americana. Mientras que la administración europea aboga más por el tratamiento que se hace en Internet de la propia imagen personal que se traduciría en el “derecho a ser olvidados” y en el control de la información “a posteriori”; en la administración americana se propugna la autorregulación por el propio usuario en una actitud más permisiva a la observación de la vida privada individual debido a su histórica defensa de la libertad de expresión (Hendel, 2011). Sin embargo, también ha llegado hasta EE.UU. la necesidad de limitar el acceso indiscriminado a los datos personales.

A continuación, se presentan las propuestas legislativas realizadas en la Unión Europea y en Estados Unidos.

Propuestas sobre la privacidad para la regulación de la información personal

Unión Europea: Propuesta legislativa sobre la privacidad de los datos personales

Viviane Reding defiende una propuesta legislativa sobre la revisión de la legislación vigente -que data de 1995- sobre la privacidad de los datos personales. Esta propuesta surge de la extensión de la información personal compartida a través de Internet, que precisa de la necesidad de crear un conjunto claro y actualizado de normas, que garantice un alto nivel de protección de datos y de privacidad a todos los usuarios. Las redes sociales, en concreto Facebook, serán uno de los principales objetivos de estas nuevas normas. *“Nuestros datos están siendo recogidos sin nuestro consentimiento y, a menudo, sin nuestro conocimiento.*

Aquí es donde deben intervenir las leyes europeas... La gente debe tener el derecho de decir "no" siempre que lo desee" (Reding en Martínez, 1 de Febrero de 2010).

El proceso legislativo puesto en marcha por la Comisión Europea pretende reforzar la protección de datos de los ciudadanos y adaptar las viejas normas al entorno virtual, donde los documentos no solo tienen un alcance global sino que, también, son permanentes (Gómez, 07/01/2011).

En esta línea, la Comisaria presentará una propuesta legislativa para aumentar la protección del derecho a la cancelación de los datos personales en las redes sociales online. El objetivo de esta iniciativa es que empresas como *Facebook* borren efectiva y completamente los datos personales y fotografías cuando un/a usuario/a se dé de baja en el servicio, algo que en la actualidad no hacen pese a existir legislación en varios países que obliga a ello, como la LOPD en España. *"Las personas deben tener el derecho de retirar su consentimiento al procesamiento de datos"*, defiende la Vicepresidente de la Comisión Europea (European Commission, Bruselas 16 de Marzo de 2011).

La reforma se dirige tanto a la regulación del almacenamiento en Internet de datos personales que no son de interés público como a la desaparición de los mismos en buscadores, redes sociales y servicios 2.0 si el interesado así lo solicita. Los/as usuarios/as de redes sociales como Facebook o Tuenti podrán así tener el control de sus datos y exigir el completo borrado de su información personal (escrita, gráfica y audiovisual) cuando se den de baja en el servicio. Una tarea que, en la actualidad, se presenta como titánica y, a menudo, frustrante (Gómez, 07/01/2011).

El objetivo es que las nuevas leyes sean más estrictas. La propuesta exigirá que la configuración de redes sociales garantice la privacidad por defecto, de forma que el uso de los datos para cualquier otro objetivo que vaya más allá del que esté especificado en la contratación del servicio, sólo se permitirá con el consentimiento explícito del usuario. La carga de la prueba recae en las empresas, que deben demostrar por qué es necesario almacenar una determinada información personal.

Con la modernización de la legislación, se quiere conseguir de forma expresa que las personas tengan y disfruten de este derecho de forma activa y previa al uso de estos datos, y no sólo como la posibilidad futura de retirar su consentimiento al procesamiento posterior de datos.

Otro objetivo de la normativa es que los proveedores de Internet, los buscadores y las redes sociales almacenen la menor cantidad posible de datos personales. La Comisaria Reding expone que *“Cualquier compañía que opera en el mercado europeo o para cualquier producto en línea que tenga como compradores a consumidores de la Unión Europea debe cumplir con la reglas de la UE”* ((European Comission, Bruselas 16 de Marzo de 2011).

La UE exigirá mayor transparencia a las empresas gestoras de estas comunidades virtuales, que estarán obligadas no sólo a informar a los usuarios sobre los datos que van a recoger, con qué objetivos y cómo pueden ser usados por terceras partes (como ya especifica la legislación actual) sino también a comunicar a los usuarios cuáles son los riesgos potenciales. La vicepresidente ha remarcado que *“esto es particularmente importante para los internautas más jóvenes”* (Europa Press, 17/03/2011). De esta forma, se exigirán normas que dejen claro a los/as niños/as qué consecuencias tiene el registrarse en una red social, explicando en términos claros y asequibles donde localizar la información sobre el tratamiento de datos personales.

La Comisión también incidirá en la obligación de las empresas que procesen datos de ciudadanos de la UE pero que tengan su sede legal en un país que no sea miembro, a cumplir estas reglas. Para ello, se dotará de poderes a las agencias de protección de datos de cada país de la Unión, para cooperar más efectivamente entre sí y para perseguir legalmente a las empresas extranjeras con el fin de que adecuen su actividad a esta nueva legislación. Este tema es básico para la garantía de los usuarios/as ya que las redes sociales con mayor penetración en nuestro país –con la excepción de Tuenti- tienen su sede en Estados Unidos por lo que no están obligadas a cumplir la normativa europea.

La Unión Europea aspira a dotar de transparencia el brumoso mundo digital. Su objetivo es que los proveedores de servicios de Internet o los buscadores recojan los mínimos datos de los usuarios y que realicen este proceso de recogida de forma clara, comunicando quién los almacena, cómo, con qué finalidad y durante cuánto tiempo. Además, se propone simplificar y mejorar el ejercicio de los derechos de acceso, rectificación y supresión de contenidos relacionados con el usuario. La intención del Ejecutivo comunitario es poner coto al omnímodo poder de los buscadores y proveedores de servicio.

La defensa de estos derechos se ha producido como reacción por las presiones ciudadanas –en especial, por el aumento de las quejas y reclamaciones- y por los problemas jurídicos que se han producido en los últimos años, sobre todo vinculados con empresas estadounidenses como Google (en especial, con su polémico servicio Street View de Google Maps) y Facebook.

La multinacional Google se ampara en las lagunas legales actuales, alegando que los datos y su posible uso no son responsabilidad de la compañía, ya que el servicio se presta desde EE.UU. De esta forma, la directiva europea de protección de datos y la ley española que la aplica, no les afectan. Además, alegan que el propio webmaster debe ser el que instale ciertas etiquetas para evitar que la Web sea rastreada por el googlebot, ya que su tecnología no permite la modificación del contenido (Gómez, 07/01/2011). Por ello, la cooperación es vital, tal y como señala Artemí Rallo, Presidente de la AEPD: *"Internet es un marco global y necesita una norma global, con tratados internacionales de protección de privacidad. Esa es la única lógica que puede satisfacer la exigencia de proteger la privacidad. La fuerza está en la unión"* (Gómez, 07/01/2011).

Esta problemática también ha llegado a España, en especial a partir del año 2009, fecha en la que las redes aumentaron su penetración. Así, el exdirector de la AEPD, Artemí Rallo, indicó en Marzo de 2010 que las redes sociales están *"obligadas a realizar una actualización urgente"* de sus plataformas digitales para respetar el derecho a la privacidad de sus usuarios/as (Editor DJ, 15 de Abril de 2010). La propia Agencia anima a los ciudadanos a solicitar la cancelación de sus referencias privadas en foros, blogs, redes

sociales o buscadores si estiman que se vulnera el respeto de su dignidad personal: *"Ningún ciudadano que no goce de la condición de personaje público ni sea objeto de un hecho de relevancia pública tiene que resignarse a que sus datos personales circulen en la Red"* (Gómez, 07/01/2011).

En España, los problemas de la información en Internet derivan:

1.- De su permanencia y de su expansión global. Tal y como explica Artemí Rallo *"el problema no es el alud de información sobre una persona que puede albergar Internet, sino que esa información sea imperecedera... El derecho al olvido se refiere al efecto multiplicador de Google y los motores de búsqueda. Se puede borrar la información personal de un medio digital o datos que aparecen en el BOE, como multas, sanciones o indultos. Esa información, a diferencia de lo que ocurre en el papel, adquiere una expansión global y temporalmente eterna. Es bastante razonable que algo que sucedió hace 30 años no esté en los índices de un buscador"* (Gómez, 07/01/2011).

Para Artemi Rallo, el derecho al olvido reconoce la cancelación de un dato personal que se ha recabado legítimamente para que se retire cuando se agote la finalidad para la que fue obtenido. Equivale a hacer realidad el poder de cualquier ciudadano a disponer de toda la información de la que es titular y a que la memoria digital no se convierta en algo perpetuo (Gómez, 07/01/2011).

2.- Del problema del consentimiento, en el caso de que la información se haya facilitado por voluntad propia. Marc Carrillo, catedrático de Derecho Constitucional de la Universidad Pompeu Fabra, explica que la pretensión de un particular de borrar los datos que hacen referencia a su persona en la Red *"es legítima en los casos en los que su aparición en la misma no ha sido por voluntad propia, sino como consecuencia de figurar en un archivo, público o privado, y el motivo de ello carezca de interés público"* (Gómez, 07/01/2011).

Pero esta pretensión no se sostiene si el particular, por ejemplo, es autor de un delito condenado por sentencia firme al ser un hecho de interés público, y en el caso de la información publicada en redes sociales ya que se ha realizado por voluntad propia. La única vía podría ser que las administraciones de las webs se doten de las adecuadas medidas informáticas que permitan evitar la indexación de la noticia.

La AEPD también actúa para cancelar datos publicados en foros de Internet facilitados por un tercero sin el consentimiento del afectado. En este caso, la agencia precisa que los comentarios introducidos en Internet entran dentro de la libertad de expresión, pero matiza: *"La libertad de expresión tiene su límite en el respeto a otros derechos fundamentales"*. Expone que, aunque la información publicada en ese foro fuera veraz, *"al no referirse a asuntos públicos de interés general resulta preferente el derecho fundamental a la protección de datos"* (Rallo, 2010).

Los expertos coinciden en señalar que el ciudadano debe tener mecanismos a su alcance para cancelar datos personales e impedir su mantenimiento universal en la Red.

Propuestas en Estados Unidos: *Privacy Bill of Rights*

En Estados Unidos, en diciembre de 2010, la *Federation Trade Comission* (FCT) propuso la creación de una herramienta para que los consumidores pudiesen impedir su seguimiento online (gustos, visitas, búsquedas, etc.), desde la idea expuesta por el responsable de la Comisión, Jon Leibowitz de que *"la auto-regulación sobre privacidad no ha funcionado adecuadamente hasta ahora y no está funcionando de forma adecuada para los consumidores americanos"* (Angwin & Valentino-Devries, 02/12/2010). En esta misma fecha, el Partido Demócrata defendía la elaboración de una ley que regulara el seguimiento de la navegación de niños menores de 13 años por Internet, con el fin de que fuera necesario obtener el permiso de los padres antes de recoger datos personales, como los nombres o direcciones de mail de los niños/as (Stecklow, 23/12/ 2010).

En Marzo de 2011, se empezó a difundir la necesidad de ampliar la defensa de la privacidad mediante la elaboración de una *"Privacy Bill of Rights"*¹ (Johnson, 3/02/2011). Esta *Carta* regularía la recopilación comercial de datos de los usuarios online, qué se puede registrar y qué no, y qué uso sería aceptable dar a los datos recogidos. La FTC sería la encargada de vigilar que estos códigos de conducta fuesen respetados, cumpliendo una misión análoga a la que ya realiza en España la Agencia de Protección de Datos.

Según el Secretario de Comercio estadounidense, Gary Locke, *"la autorregulación del sector no es suficiente"*. (Johnson, 3/02/2011) ya que el uso de datos personales ha aumentado tanto que se necesita una legislación específica que, mediante medidas de obligado cumplimiento, permita que se recupere la confianza online de los consumidores, al tiempo que se establezca un marco para que las empresas puedan seguir realizando sus negocios en la Red.

En Abril de 2011, los senadores John Kerry y John McCain propusieron la legislación para crear la *"Privacy Bill of Rights"* (Proyecto de ley de privacidad de derechos) para proteger a las personas de las prácticas cada vez más invasivas de recolección de datos comerciales de la industria. Este proyecto de ley, denominado *Commercial Privacy Bill of Rights Act of 2011*, impone nuevas normas para las empresas que recopilan datos de carácter personal, como la consulta previa sobre el acceso a los datos o la capacidad de bloqueo de que la información sea usada o distribuida. De esta forma, las empresas tendrían que pedir permiso antes de recopilar y compartir datos sensibles (información religiosa, médica y financiera) con entidades externas (Angwin, 2011).

La propuesta bipartidista representa la primera ley integral de privacidad y adopta, en gran medida, las recomendaciones realizadas por la administración de Obama en el año 2010. Las leyes actuales norteamericanas sólo cubren el uso de ciertos tipos de datos de carácter personal, tales como información financiera y médica. Esta legislación responde a la

¹ Traducción al castellano: *Carta de derechos a la privacidad*.

necesidad de que los usuarios/as tengan un control en el acceso de los datos a terceros y a la limitación del uso comercial de los datos personales.

En este debate, las redes sociales representan el primer frente de la batalla, debido a que han sido las aplicaciones tecnológicas que más han influido en el cambio de la privacidad, por su gran penetración entre los internautas y por la identificación personal de los usuarios/as (que, en la mayoría de ocasiones, comparten datos reales). En particular, *Facebook* que ha estado siempre en el centro de la polémica.

En EE.UU., existen sitios web que convocan a los internautas a abandonar la red *Facebook* como <http://www.quitfacebookday.com/>, mientras algunas organizaciones norteamericanas como *MoveOn.org* o *Electronic Frontier Foundation* han publicado informaciones sobre la regresión de *Facebook* en sus prácticas para proteger la intimidad de sus miembros. El grupo europeo de agencias de protección de datos envió una carta el 12 de mayo de 2010 a *Facebook* denunciando los cambios en las opciones de gestión de la privacidad que, por defecto, abrían los contenidos a terceros. Una gestión de opciones compleja porque el internauta debía evaluar 170 alternativas. Algunos senadores norteamericanos se sumaron a las protestas (El País, 26/05/2010).

La reforma se dirige a regular el almacenamiento en Internet de datos personales que no son de interés público, limitando su recogida indiscriminada, aportando mayor transparencia en su gestión, información al usuario sobre su uso y la posibilidad de hacer desaparecer los datos personales de Google, Yahoo, Youtube o de las redes sociales, si el interesado así lo solicita. La propuesta exigirá que la configuración de redes sociales garantice la privacidad por defecto, de forma que el uso de los datos para cualquier otro objetivo que vaya más allá del que esté especificado en la contratación del servicio, sólo se permitirá con el consentimiento explícito del usuario.

La defensa de estos derechos se ha producido como reacción por las presiones ciudadanas –en especial, por el aumento de las quejas y reclamaciones- y por los problemas jurídicos que se han producido en los últimos años, sobre todo vinculados con empresas

estadounidenses como Google. En este debate, las redes sociales representan el primer frente de la batalla, debido a que han sido las aplicaciones tecnológicas que más han influido en el cambio de la privacidad, por su gran penetración entre los internautas y por la identificación personal de los usuarios/as (que, en la mayoría de ocasiones, comparten datos reales).

Conclusiones

El derecho al olvido representa un derecho subjetivo que defiende prerrogativas fundamentales (derecho a la imagen, al honor, a la dignidad personal...) que entran en colisión con otros derechos básicos, como la libertad de expresión. La Red genera un nuevo entorno tecnológico que afecta a los intereses personales del sujeto, creando situaciones de indefensión derivadas de la perpetuidad y la publicidad de la información.

La propuesta defiende la defensa de un área proactiva de la privacidad del sujeto. Se estima que debe prevalecer este derecho en circunstancias que suponen un grave perjuicio para el individuo, especialmente si la información extiende su divulgación más allá del plazo para el que fue creada y en el caso de que no tenga relevancia pública o ésta se haya agotado. Sin embargo, se considera que tendría que adoptar una forma flexible que no suponga censura y que interfiera de la forma más reducida posible en la libertad de la información. La normativa tendría que analizar las posibles situaciones (en especial, si el sujeto ha otorgado su consentimiento a la publicación o ésta depende de terceros), limitar el uso indiscriminado de la información más sensible (médica, académica, financiera, ideológica, datos de localización) y verificar los perjuicios para el interesado.

Frente a las disyuntivas del derecho al olvido, nos sumamos a la opinión de Marie Hélène Boulanger, representante de la Comisión Europea, que estima que el derecho a ser olvidado debe ser exclusivo del control de las personas. *“Las autoridades en protección de datos se tienen que reforzar para proporcionar una respuesta. No es el derecho a ocultar, es un equilibrio entre la libertad de expresión y el derecho a la protección de los datos”* (Sánchez Onofre, 2011).

Pero, sin duda, la opción más idónea en un entorno turbulento es que el propio internauta adopte una actitud de prudencia y piense, antes de publicar su información privada, en las posibles consecuencias actuales y futuras de su uso. Así mismo, se considera fundamental que tanto los sujetos jurídicos (compañías comerciales, organismos públicos) como los sujetos individuales tengan una actitud de mayor cautela en el tratamiento de los datos personales, sobre todo con los que ostentan una naturaleza privada.

Bibliografía

ANGWIN, J. (2011). "Senators Offer Privacy Bill to Protect Personal Data". *The Wall Street Journal*. Recuperado de <http://online.wsj.com/article/SB10001424052748703385404576258942268540486.html>

ANGWIN, Julia & VALENTINO-DEVRIES, Jennifer (2010) "FTC Backs Do-Not-Track System for Web". *The Wall Street Journal*. Available in <http://online.wsj.com/article/SB10001424052748704594804575648670826747094.html>

DÁVILA, René (2011). El derecho al olvido debe estar garantizado en el mundo digital, piden autoridades internacionales de protección de datos. *Journalmex*. Recuperado de <http://journalmex.wordpress.com/2011/11/04/el-derecho-al-olvido-debe-estar-garantizado-en-el-mundo-digital-piden-autoridades-internacionales-de-proteccion-de-datos/>

EUROPA PRESS (2011). Bruselas garantizará por ley el 'derecho al olvido' en redes sociales como Facebook. *Portaltic.es sector*. Recuperado de <http://ciberderechos.wordpress.com/>

FANJUL, MARTÍNEZ, Diego (2010). Criterios de ámbito de aplicación normativa a buscadores. Recuperado de <http://www.abogadoprotecciondatos.com/p/es/blog/derecho-al-olvido-i.php>

HENDEL, John (2011). Europe, a Right to Be Forgotten Trumps the Memory of the Internet in The Atlantic. Recuperado de <http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/>

JOHNSON, Rich (2011, Febrero 3). A Privacy Bill of Rights?. in Site Jabber Blog.. Recuperado de <http://www.sitejabber.com/blog/2011/02/03/a-privacy-bill-of-rights/?display=wide>

PLAZA, ALBA, Esther (2011). El mundo interconectado requiere nuevas respuestas. *Profesiones*, 130, 38-39. Recuperado de <http://www.profesiones.org/var/plain/storage/original/application/9ad0c95661d7b82853fa0414f186ea51.pdf>

RALLO, LOMBARTE, Artemí (2010). El derecho al olvido y su protección: a partir de la protección de datos, *Telos: Cuadernos de comunicación e innovación*, 85, 104-108. Recuperado de http://sociedadinformacion.fundacion.telefonica.com/seccion=1268&idioma=es_ES&id=2010110416500001&activo=6.do#

SÁNCHEZ, ONOFRE, Julio (2011, Noviembre 2). El derecho al olvido: ¿Oportunidad o censura?. *El economista*. Recuperado de <http://eleconomista.com.mx/tecnociencia/2011/11/02/derecho-olvido-oportunidad-o-censura>

STECKLOW, Steve (2010, Diciembre 23). Proposed Law Would Prohibit Web Collection of Data on Kids. *The Wall Street Journal*. Recuperado de

[http://online.wsj.com/article/SB10001424052748703865004575649140574658582.ht
ml](http://online.wsj.com/article/SB10001424052748703865004575649140574658582.html)