

## La UE cambiará la ley para proteger a los internautas

# El negocio de los datos personales

Cuando navegamos o entramos en una red social, no solemos ser conscientes de que dejamos un rastro de datos personales que otros ven y aprovechan. La Unión Europea prepara ahora cambios legislativos para que el usuario tenga un mayor control.

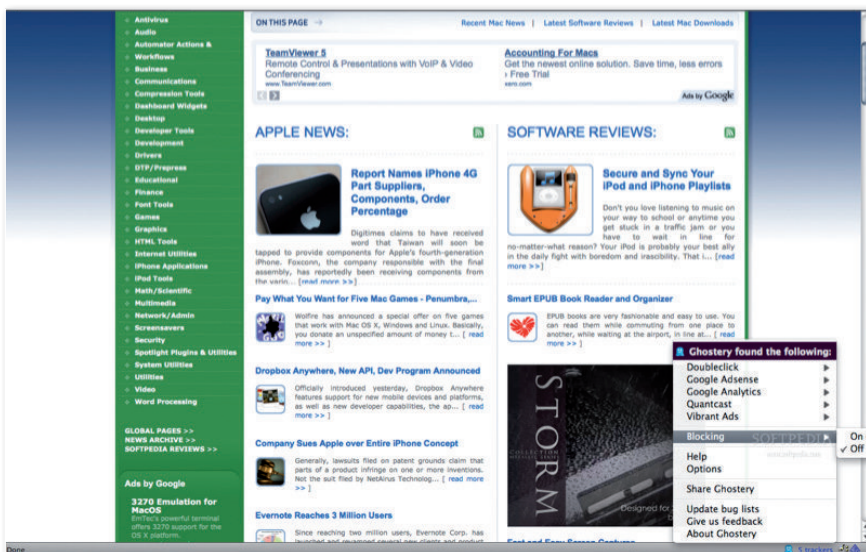


Juan Ignacio Cabrera

**E**n España tenemos una **escasa o nula cultura de la privacidad**, al contrario que en el mundo anglosajón». Lo dice **Víctor Domingo**, presidente de la **Asociación de Internautas**. Hoy en día, navegamos libremente por cientos o miles de páginas, dejamos nuestros datos más íntimos en redes sociales, mientras contestamos al correo electrónico, compramos billetes de avión o contratamos un seguro *on-line*. Aunque pocas veces reparamos en ello, cada vez que acometemos tareas tan cotidianas, **cedemos información a redes publicitarias y compañías** de todo tipo que comercian con unos **datos que nos perfilan al detalle como potenciales consumidores**. Una búsqueda de un coche en un comparador de precios nos llevará a recibir anuncios de esa marca en páginas de todo tipo sin que se pueda hacer mucho al respecto. En

la actualidad, la navegación desde el PC, el móvil o la tableta permite saber a terceros cosas impensables: **dónde estamos en cada momento, dónde vivimos, cuáles son nuestros gustos o fantasías**, e incluso, indagando un tanto en nuestro comportamiento en redes sociales, quién nos fascina. Como subraya **Carolina Armada**, abogada del **despacho Simmons & Simmons**, «el usuario está compartiendo con un número indeterminado de personas información que probablemente nunca debió haber trascendido de su esfera personal más íntima y que, desde luego, es una **poderosísima herramienta para el marketing y la publicidad**, o incluso para prácticas ilícitas y/o fraudulentas». «Hasta ahora el internauta ha sido un gran desconocedor de cómo, quién y para qué manejaban sus datos en Internet», asegura **Francisco Javier Carbayo**, abogado del **bufete Écija**, que está especializado en derecho relacionado con nuevas tecnologías. En los últimos años, lo habitual para darse de alta en nuevos servicios (sobre todo de correo electróni-

co, redes sociales o para el móvil) ha sido **intercambiar gratuidad por información personal**, que luego es usada para vincular anuncios. Hay toda una maquinaria comercial y publicitaria (Google y Facebook ganan miles de millones de dólares cada año con este negocio) que se nutre de nuestra intimidad y, más en concreto, de los detalles de nuestra navegación. **El bloguero y profesor del Instituto de Empresa Enrique Dans** va más allá incluso y asegura que los problemas de la privacidad no provienen de las empresas privadas a las que cedemos los datos, «sino de los **estados supuestamente democráticos** que, recurriendo a excusas como el terrorismo, la pornografía infantil o los derechos de autor, **infringen la ley, fiscalizando y vigilando a sus ciudadanos**». Sea como sea, lo más importante en la Red, nos recuerda Carolina Armada, es «ser conscientes de que **su tan difundido 'anonimato' no es tal**, en la medida que sea posible rastrear datos, identificar direcciones IP, instalar *cookies* y otras mu-



• Con AdBlock, Ghostery o DoNotTrack podemos ver cómo se aprovechan de nuestra navegación.

## Un botón de «No me sigas»

Las iniciativas para proteger los datos personales no solo vienen de Europa. En EE UU, el Gobierno de Obama anunció en febrero que prepara una ley que da el derecho a los internautas de **controlar los datos personales que recogen las empresas y cómo los utilizan**. También insistirá en que las políticas de privacidad queden expuestas de una forma clara y comprensible. Sin embargo, una de las novedades más llamativas será la obligación de incluir **un botón de «no me sigas»** (en inglés, *do not track button*) **en los buscadores** que, en caso de ser pulsado, obligará a las empresas a no utilizar la información del usuario para confeccionar publicidad a su medida. En principio (el texto es todavía un borrador, aunque está previsto que entre en vigor durante 2012), esta medida no limitaría por completo el acceso de las compañías a los datos de los usuarios, y sus referencias podrían utilizarse para hacer estudios de mercado.



Para cambiar las cosas y extender la confianza en la Red, **la Unión Europea prepara ahora un cambio legislativo de gran calado**. A finales de enero, la vicepresidenta de la Comisión, Viviane Reding, anunció un proyecto normativo que pretende **unificar las políticas de protección de datos** de todos los estados miembros (27) y **poner al día unas leyes que datan de la segunda mitad de la década de los 90**, cuando los usuarios de Internet eran minoría, nadie compraba *on-line* y las redes sociales no existían.

Aunque el proceso llevará su tiempo (para ver esta norma habrá que esperar uno o dos años), Europa quiere sobre todo **evitar las fugas de datos privados** y que las empresas se tomen más en serio qué hacen con la información de sus clientes. Así, cualquier **robo** de información deberá ser **notificado en un plazo de 24 horas** (y no casi una semana, como pasó con Sony). Además, las empresas negligentes en la custodia de la información podrán ser tener **multas de hasta un 1% de su facturación mundial**. Además, el proyecto que estudia Europa incluye que **la privacidad total se garantice por defecto**.

Es decir, cuando un usuario active un servicio, las opciones de privacidad estarán activadas desde el principio, en lugar de tener que configurarlas en el momento del alta. Esto evitará lo que hoy les pasa a los usuarios de Facebook, que tienen que ingeniárselas para ocultar ciertos datos que la red social, por sistema, enseña a cualquier persona que pulula por Internet. Otro **derecho** que protegerá la Comisión Europea será el «**del olvido**». Una vez entre en vigor la nueva norma, **los interesados deberán poder borrar sus datos** personales de la Red si no hay motivos de fuerza mayor para que un tercero los retenga. Además, la Comisión plantea que los usuarios estén informados en todo momento de qué ocurre con sus datos (quién los almacena, con qué propósito, dónde, cuánto tiempo...). En el fondo, lo ►

## «Existen mecanismos para protegernos en Internet, pero no están muy a la vista y su uso sigue siendo complejo para la mayoría»

chas estrategias que permitan identificar a aquellos que han facilitado información personal de interés para terceros».

En cualquier caso, parece que las cosas están cambiando y que el **debate sobre la privacidad en Internet empieza a preocupar** a los usuarios y a los políticos. El debate no es retórico y se ha visto alentado por algunos **hechos indeseados** originados por la ciberdelincuencia. En el último año han trascendido brechas de seguridad de servicios muy populares en Internet, que han multiplicado las preguntas de los usuarios. La más significativa fue la sufrida por **Sony** en abril de 2011, que vio cómo un intruso accedía a datos personales y de tarjetas de crédito de 70 millones de suscriptores de la plataforma de juegos *on-line* PlayStation Network. Hasta **330.000 tarjetas de pago espa-**

**ñolas quedaron expuestas**. Otro caso sonado fue el de **Citibank**, que vio en junio cómo los *hackers* se hacían con datos personales y bancarios de **200.000 clientes norteamericanos con tarjeta**. En España, la Agencia de Protección de Datos **sancionó a Vodafone** en 2010 tras detectar que en su página web un cliente podía acceder a información de terceras personas.

### Nueva legislación europea

Datos del Eurobarómetro, publicado por la Comisión Europea a mediados del año pasado, decían que **el 62% de los ciudadanos del continente no confían en que las compañías de Internet** (buscadores, redes sociales o servicios de correo) **protejan adecuadamente los datos** de carácter personal. En España, ese nivel de desconfianza era similar.



• Algunas compañías, como NetClean4.me, han visto negocio en la posibilidad de borrar los datos que los internautas van dejando cuando navegan por Internet.

que se busca es garantizar el «derecho a la portabilidad», lo que permitirá, entre otras cosas, obtener una copia de la información que se ha almacenado en una red social para trasladarla a otra. A las empresas de más de 250 empleados y a la Administración se les impondrá la obligación de contratar a una persona que supervisará el cumplimiento de la legislación en materia de protección de datos (*data protection officer*). La reforma legislativa, en palabras de **Alba Bonet**, abogada de **Alcatraz-LOPDgest**, una firma especializada en software y consultoría de protección de datos, «es más que necesaria porque llevamos 15 años trabajando con la misma normativa y se ha quedado muy desfasada».

### ¿Es posible olvidar del todo?

Eso sí, la ley deberá aclarar cómo aplicar una legislación de carácter europeo a empresas como Facebook, que tiene su sede en California y que en la cláusula de las condiciones de prestación de su servicio específica que el usuario da permiso para transferir sus datos a Estados Unidos. ¿Adónde deberá recurrir un usuario que siente vulnerados sus derechos y qué legislación le ampara? «Habrán dificultades, aunque no insalvables, para armonizar la nueva normativa europea con las reglas estadounidenses», advierte **Paloma Bru**, abogada de la firma **Jones Day**.

Además, también hay problemas técnicos e incluso éticos que impiden, por ejemplo, una aplicación literal del «derecho al olvido». Por el momento, **no existen herramientas que permitan extraer automáticamente de la Web toda la información referente a una persona**. En muchos casos, se impone el trabajo manual. «Este derecho es una falacia», indica Enrique Dans, «detrás de él hay intereses peligrosísimos. Y es que no se puede 'obligar a la red a olvidar', del mismo modo

que antes no se podía retirar la información de las hemerotecas».

Una escenificación de los problemas que puede traer este derecho la tuvimos en España a principios de año, cuando **el propietario del Camping de los Alfaques (Tarragona) pretendía que Google dejase de mostrar la tragedia ocurrida en esa instalación en 1978**, cuando un camión cisterna con combustible explotó en el lugar y mató a más de 200 personas, porque la consideraba perjudicial para su negocio actual. Como no podía ser de otro modo, el dueño del camping perdió su batalla contra Google.

Además, el «derecho al olvido» será una cuestión controvertida, pues afecta a datos que traspasan fronteras y límites temporales. Por ejemplo, hace unas semanas, **los magistrados de la Audiencia Nacional enviaron una serie de preguntas jurídicas a la Unión Europea** para saber cómo actuar ante la petición de particulares que reclaman la desaparición de datos privados en sitios de Internet que en muchos casos tienen su sede y los servidores que contienen la información en el extranjero.

### Recomendaciones generales

A la espera de que llegue la nueva normativa sobre privacidad, los expertos recomiendan prestar atención para mantener el control sobre nuestros datos personales en Internet. «El usuario debe formarse, y para ello hay inmensos recursos gratuitos en Internet, sobre qué debe hacer y qué no. Sin embargo, **lo primero es utilizar algo tan 'viejo' como el sentido común**, que nos debería llevar, por ejemplo, a no revelar en Internet lo que no revelarías en el mundo físico», dice Francisco Javier Carbayo, abogado de Écija. Otra cosa muy recomendable es **leer atentamente las políticas de privacidad de los servicios on-line**, a pesar de que en muchas oca-

## Los puntos clave de la futura legislación

- 1. Mayores multas.** Las penalizaciones podrán llegar hasta un 1% de la facturación anual de la compañía infractora en todo el mundo. Por ejemplo, en el caso de Google, esto podría suponer unos 300 millones de dólares.
- 2. Comunicación en 24 horas.** Cualquier robo masivo de información deberá ser notificado por la empresa o el organismo afectado en un plazo de 24 horas, y no en seis días, como pasó con Sony en la primavera de 2011.
- 3. Consentimiento expreso.** La privacidad total se garantizará por defecto. Es decir, cuando un usuario active un servicio, las opciones de privacidad estarán activadas desde el principio, en lugar de tener que configurarlas en el momento del alta.
- 4. Derecho al olvido.** Los interesados deberán poder borrar sus datos personales de la Red, siempre que no haya motivos de fuerza mayor para que un tercero los retenga.
- 5. Portabilidad.** Permitirá, entre otras cosas, obtener una copia de la información que se ha almacenado durante su uso en una red social para trasladarla a otra.
- 6. Transparencia.** Los usuarios deberán estar informados en todo momento de qué ocurre con sus datos: quién los almacena, con qué propósito, dónde, cuánto tiempo...

siones son documentos farragosos, están llenos de jerga legal y tienen longitud enciclopédica. También está la opción de dejar de usar un servicio por algo tan simple como que su política de privacidad es «un galimatías de difícil comprensión». Víctor Domingo, de la Asociación de Internautas, lo tiene muy claro: «Hay que saber que todo lo que hacemos en Internet deja huella y que cuando navegamos estamos

## Consejos para controlar nuestra privacidad

- Debemos actuar con **sentido común**. No debemos revelar en Internet lo que no revelaríamos en el mundo físico.
- A pesar de que sea un poco farrogoso y lleve un tiempo, es muy recomendable **leer atentamente las políticas de privacidad** de los servicios *online*. Al final, es un contrato que firmamos y que nos compromete.
- También está la opción de **dejar de usar un servicio** por algo tan simple como que su política de privacidad sea «un galimatías de difícil comprensión».
- No estaría mal que, cada vez que apaguemos el ordenador, **borremos nuestro historial de navegación**.
- Podemos configurar el navegador para **vaciar las cookies guardadas** o directamente bloquearlas, o activar el bloqueo de publicidad del antivirus.
- Puede ser interesante la **instalación de herramientas** como Adblock, Ghostery o DoNotTrack, que bloquean la publicidad o nos dan una idea del nivel de explotación de los datos al que estamos sometidos cuando navegamos por Internet.



abriendo la puerta de nuestra casa de par en par, y por eso hay que tener una llave que sirva para cerrarla, y sobre todo no dar información de carácter personal si no queremos perder el control sobre nuestra privacidad». Además, Domingo aconseja que, **cada vez que apaguemos el ordenador, borremos nuestro historial de navegación**.

Enrique Dans, por su parte, indica que puede ser interesante la **instalación de herramientas como Adblock, Ghostery o DoNotTrack**. «Son interesantes para hacerse una idea del nivel de explotación de los datos al que estamos sometidos cuando navegamos, pero conviene utilizarlas con responsabilidad. Si un sitio no te bombardea con publicidad intrusiva, no te resulta molesto o no te hace sentirte como te tuvieras que proteger, deberías excluirlo de los filtros para posibilitar que pueda generar recursos económicos con lo que hace porque, si no, su modelo resultará simplemente insostenible».

El usuario también puede **configurar el tratamiento de las cookies de su navegador o activar el bloqueo de publicidad** en su antivirus. En todo caso, como recuerda Alba Bonet, de Alcatraz-LOPDgest, el problema con el que se encuentra el usuario no es la inexistencia de **mecanismos de protección**, sino la complejidad de usarlos. «Un usuario medio de Internet no localiza fácilmente dónde se encuentran estos mecanismos e incluso, una vez localizados, no sabe cómo configurarlos correctamente. Debería exigirse a los buscadores o redes sociales que la privacidad se proporcione por defecto, de forma que el usuario no se viera obligado a investigarlas y configurarlas». Es la línea que quiere seguir ahora la Unión Europea.

### Google mueve ficha

El último capítulo en esta controversia de los datos personales lo ha puesto Google, que desde el pasado 1 de marzo tiene una **nueva política de privacidad**. Aunque la iniciativa ha generado polémica, desde esta compañía insisten en los beneficios

Google Políticas y principios

Descripción general Privacidad Condiciones de servicio

Política de privacidad Publicidad Principios Herramientas Preguntas frecuentes

Versión actual

Versiónes anteriores

Marcos de autorregulación

Términos clave

### Política de privacidad

Última modificación: 1 de marzo de 2012 (ver versiones archivadas)

Puedes utilizar nuestros servicios de muchas maneras, tanto para buscar y compartir información como para comunicarte con otros usuarios o para crear contenido nuevo. Cuando compartes datos con nosotros (por ejemplo, al crear una cuenta de Google), podemos mejorar aún más esos servicios para mostrarte resultados de búsqueda y anuncios más relevantes y ayudarte a ponerte en contacto con otros usuarios o compartir de forma más rápida y sencilla. Como usuario de nuestros servicios, queremos informarte claramente acerca de cómo utilizamos tus datos y cómo puedes proteger tu privacidad.

La presente Política de privacidad describe:

- qué datos recogemos y los fines para los que llevamos a cabo su recogida,
- cómo utilizamos esos datos,
- las opciones que ofrecemos, incluyendo cómo acceder a los datos y actualizarlos.

Aunque hemos intentado proporcionar una descripción lo más sencilla posible, si no estás familiarizado con términos clave tales como «cookies», «dirección IP», «contadores de visitas» y «navegador», consulta esta página para informarte de su significado antes de continuar. Tu privacidad es importante para Google, por lo que con independencia de que seas un usuario nuevo o un usuario avanzado, te recomendamos que leas nuestra política y te pongas en contacto con nosotros si tienes cualquier duda.

Datos recogidos por Google

La recogida de datos se realiza para mejorar el servicio que ofrecemos a todos nuestros usuarios (desde aspectos básicos como deducir el idioma que hablan hasta aspectos más complejos como determinar qué anuncios les puedan resultar más útiles o qué usuarios son más importantes para ellos en la Web).

- **Google ha unificado en marzo las políticas de seguridad de 60 servicios para competir con Apple o Facebook. Una iniciativa que no ha sido del agrado de todo el mundo, incluida la Unión Europea.**

que trae para el usuario. Así, **la firma ha simplificado en un solo documento las políticas de seguridad de 60 servicios diferentes**, en el que expone «con un lenguaje sencillo» cómo se recogen los datos y cómo se utilizan. Además, el cambio **permitirá a Google dar un mejor servicio global**. Si una persona, explican, tiene que ir a una reunión, la combinación de datos de sus servicios permitirá avisarle de que llega tarde porque combinará información de localización, calendario, previsión del tiempo y tráfico.

Pero también se puede ver esta iniciativa de otra manera. Y es que, en la práctica, esto quiere decir que un usuario que quiera encontrar información de coches en el buscador o busque videos sobre el tema en YouTube recibirá publicidad en Gmail y en otros servicios casi sin mover un dedo. Google oficializa de una vez que todas sus aplicaciones están conectadas y el movimiento responde a **la necesidad de la compañía de construir un ecosistema alrededor de su plataforma que compita con Apple y Facebook**, que tienen datos personales de cientos de millones de usuarios y saben cómo sacarles partido. «La iniciativa confirma lo que sospechábamos: que **los datos de nave-**

**gación se cruzan y se obtienen perfiles de nuestro uso en la Red**. Eso debería tener un límite y un control que en estos momentos está en manos de Google», reclama Víctor Domingo. Desde el despacho de abogados Écija dicen que **el usuario pierde capacidad de decisión porque la misma política se aplica a todos los servicios**. Según Francisco Javier Carbayo, abogado de esta firma, «la opción de Google ha sido excesivamente ambiciosa y unilateral como para que su puesta en marcha no venga acompañada de muchas dudas y polémicas». Efectivamente, **la organización que agrupa a las agencias de protección de datos europeas ha solicitado a la compañía que paralice los cambios** hasta haber estudiado el alcance de los mismos, que no afecta a unos pocos miles de ciudadanos, sino a decenas de millones en todo el continente. La iniciativa tiene el apoyo de la comisaria Viviane Reding, que inicialmente aplaudió la decisión del buscador. La Unión Europea cree que Google podría combinar informaciones personales obtenidas en sus diferentes servicios sin explicar de forma transparente a los clientes su uso. Las espadas de la Unión Europea y del buscador seguirán en alto en los próximos meses. ■