

EL RASTRO DIGITAL

El reguero de datos privados que dejamos al usar aparatos digitales, internet y redes sociales cuenta ya más de nosotros que nuestra memoria. La información personal se ha convertido en la materia prima del siglo XXI, por la que puján las grandes entidades de la red. La Comisión Europea quiere poner orden, pero la tecnología corre más que la norma. Nuestra huella digital es imborrable.

La huella imborrable

Como el niño que se sumerge en su nuevo juguete sin ponderar los riesgos que entraña su uso, los ciudadanos hemos adaptado nuestra vida a los entornos digitales sin reparar en el torrente de información personal que vamos dejando al interactuar con los soportes electrónicos, navegar por internet o participar en las redes sociales. Borrarnos mensajes de nuestra cuenta de correo electrónico pensando que así desaparecen, pero su contenido se conserva en nuestro ordenador y en la empresa que ofrece el servicio del correo, como comprobaron recientemente **Iñaki Urdangarín** y sus socios **al ver publicados en la prensa los e-mails que ellos creían eliminados**.

PIRATEO: Era una foto sexi privada para el novio. Pero un 'hacker' entró en el móvil de Scarlett Johansson y todos vieron la trastienda del asunto. El tipo fue detenido.

Formateamos la tarjeta de la cámara creyendo que así borramos las fotos, pero estas continúan ahí, para desgracia de los autores del incendio de Horta de Sant Joan en el que murieron cinco bomberos, detenidos después de que los **Mossos recuperaran de sus cámaras digitales las instantáneas que se habían tomado junto a las llamas**, y que ellos habían intentado borrar inútilmente. Usamos el móvil como un almacén portátil de nuestra intimidad, ignorando que cualquier informático con conocimientos básicos puede acceder a él fácilmente y robar nuestros datos personales, como le ocurrió a la actriz Scarlett Johansson, obligada a compartir con todo el planeta el autorretrato que se hizo en la ducha, y que un *hacker* difundió tras piratear su teléfono.

Subimos fotos a nuestros perfiles en las redes sociales y luego, arrepentidos, las quitamos, creyendo que así han desaparecido, pero los buscadores que se dedican a registrar todo lo que aparece en internet ya las han copiado, pudiendo así ser recuperables. Entramos en la red pensando que nadie nos ve, pero nuestra navegación deja un rastro imborrable, como pudo comprobar el internauta que acosó a la presentadora **Eva Hache a través de su cuenta de Twitter**: el perfil falso bajo el que creía camuflado no le sirvió de nada.

DELATORES DE INFIDELIDADES

Nuestro **historial digital** ya cuenta más acerca de nosotros que nuestra propia memoria. En el 80% de los procesos de divorcio que se tramitan en Estados Unidos se usa información obtenida de redes sociales y chats privados, infalibles delatores de infidelidades. El estudiante austriaco **Max Schrems** solicitó recientemente a Facebook todos los datos que tenían sobre él y la compañía le envió un cedé con 1.200 páginas donde no solo aparecía lo que él mostraba en su perfil, sino también sus conversaciones privadas, notas que había eliminado, referencias sobre sus gustos, sus intereses y hasta sus opiniones religiosas.

No exagera Stefan Gross-Selbeck, el presidente de la red social para profesionales Xing, cuando afirma que **"los datos personales son el petróleo del siglo XXI"**. La Comisión Europea pretende poner orden en este océano de datos privados que navegan por la red o duermen peligrosamente en todo tipo de soportes digitales, pero los expertos en informática e internet dudan de la eficacia de esta directiva comunitaria. La tecnología corre más que la norma.

¿LOS ARCHIVOS QUE BORRO DE MI ORDENADOR DESAPARECEN?

La inmensa mayoría de usuarios de soportes digitales --ordenadores, tabletas, cámaras de fotos, *smartphones*-- **creemos que acudir al icono de la papelera es garantía suficiente** para deshacernos de un archivo. Sin embargo, cuando enviamos un documento a la papelera y luego la vaciamos, lo único que hacemos es ocultar el

indicador que identifica ese archivo en la memoria del ordenador, no borrar su contenido, que permanece en el disco duro, de donde es fácilmente recuperable.

Todo lo que eliminamos en nuestros ordenadores mediante los habituales sistemas de borrado **queda registrado y no desaparece**, ya se trate de textos, fotos, vídeos, *e-mails*, conversaciones de chat o el historial de navegación en internet. En la práctica, un documento grabado en un soporte digital nunca se borra.

La única manera de eliminarlo es escribiendo otro archivo encima, pero esto es más complicado, ya que nada garantiza que el nuevo documento se haya situado en el mismo lugar del disco duro donde estaba aquel que queríamos fulminar. Hay programas dedicados a sobrescribir archivos concretos, para garantizar un borrado más eficaz, pero incluso este *software* a veces deja intactos algunos fragmentos del documento que deseábamos hacer desaparecer.

"No hay ningún sistema que garantice al cien por cien la eliminación de un archivo en un soporte digital", aseguran Daniel Creus y Mikel Gastesi, expertos en seguridad informática y autores del libro *Fraude Online: abierto 24 horas*. Ni siquiera sobrescribiendo varias veces un documento encima del que queremos borrar es seguro que no quede algún dato antiguo que pueda ser recuperado.

NI A MARTILLAZOS

Tampoco romper a martillazos el disco duro o la tarjeta gráfica de una cámara evita que se pueda extraer de su interior parte de la información que albergaban. **"El usuario medio no tiene conciencia del riesgo con el que convive a diario"**, advierten estos técnicos de la compañía de seguridad informática S21sec.

Esta propiedad resistente al borrado que tiene nuestro rastro digital da lugar a situaciones paradójicas, como las vividas por los usuarios que, al comprar discos duros de segunda mano, han accedido a información privada de sus anteriores dueños, que ingenuamente solo habían formateado estos soportes antes de venderlos. Los culpables del incendio de Horta de Sant Joan, que se saldó con la muerte de cinco bomberos, **también creían que habían borrado sus huellas del crimen** tras vaciar las fotos que tomaron con una cámara digital junto a las llamas, pero los técnicos informáticos de los Mossos pudieron recuperar las imágenes de la tarjeta gráfica.

¿Y LOS 'E-MAILS' QUE ELIMINO DE MI CUENTA DE CORREO?

Iñaki Urdangarín y sus colaboradores debieron de sentir una incómoda sensación de desnudez el 12 de enero cuando abrieron la prensa y vieron publicados los correos electrónicos que se habían enviado en el pasado, y que ellos creían eliminados de sus cuentas de *e-mail*. Si es difícil borrar el rastro que dejamos en los soportes digitales físicos, más complicado aún es hacer desaparecer nuestra huella cuando pisamos internet, para mandar un correo, participar en un chat, poner un mensaje en Twitter o hacer un comentario anónimo en un foro.

A las marcas que dejan en el disco duro los *e-mails* que eliminamos (que creemos que eliminamos) enviándolos a la papelera del ordenador, se unen los registros que permanecen de dichos mensajes en los ordenadores centrales de las empresas que ofrecen el servicio de correo electrónico. Los servidores de **Yahoo y Gmail**, por ejemplo, **guardan durante 18 meses los e-mails que borramos** de las cuentas personales.

Lo que hacen las entidades de correo con nuestros *e-mails* es un misterio para los usuarios, que confiamos ciegamente en ellas pidiéndoles que lleven y traigan nuestras informaciones privadas, pensando que estas permanecen opacas a ojos extraños. Nada más alejado de la realidad. Los robots de Google, por ejemplo, **leen y escanean los mensajes que enviamos por Gmail para ofrecernos publicidad relacionada** con los temas que tratamos en nuestros correos.

EL ANONIMATO NO EXISTE

"Es más fácil ocultar una infidelidad a tu pareja que a Google, que no tarda en ponernos anuncios de escapadas de fin de semana cuando nos lee mensajes románticos", denuncia Alejandro Suárez Sánchez-Ocaña, autor de *Desnudando a Google*, un libro que revela hasta qué punto este gigante de internet tiene *fichados* a sus millones de clientes. **"Cada vez que usamos Chrome, Youtube, Gmail o el buscador, Google toma nota de nuestros gustos, horarios, localización geográfica e intereses personales. Esta empresa**

ofrece servicios buenísimos, pero no son gratis, como creemos ingenuamente. Pagamos con nuestra privacidad", concluye este analista.

No existe el anonimato en la red. En cuanto asomamos, nuestra presencia deja un rastro fácilmente localizable, sea cual sea el servicio que utilicemos, como pudo confirmar el año pasado el usuario de Twitter que con este sistema acosó a la presentadora de televisión Eva Hache. Para su treta se sirvió de un perfil falso en esta red social, pero la Guardia Civil tardó 48 horas en pillarlo. Su rastro digital le había delatado.

¿QUIÉN PUEDE ESPIAR MI PASADO DIGITAL?

A la hora de gestionar las marcas que va dejando cuando enciende su ordenador o se conecta a internet, el usuario medio suele ser tan inocente como inexperto de cara a hacer un uso malicioso de la información ajena. Sin embargo, alguien con mayores conocimientos sí puede controlar ese rastro con fines dudosos.

Un hacker que asalte nuestro ordenador con un virus troyano ¿un programa que se instala de forma fantasma en el sistema operativo cuando navegamos sin protección o descargamos archivos maliciosos¿ puede usar ese enlace para conocer lo que guardamos en nuestra computadora o usarla de apoyo para cometer delitos informáticos. De igual modo, puede servir para que una entidad espíe lo que sus empleados hacen con sus ordenadores o quede a la luz una infidelidad ¿amorosa o empresarial¿ que permanecía oculta.

EL INFORMÁTICO FORENSE

El manejo científico de los datos que archivamos en formato digital ha alumbrado una profesión con futuro: el informático forense. Su nombre excita la imaginación del asiduo consumidor de series policiacas como *C.S.I.*, y en la práctica su trabajo no dista mucho de lo que vemos en las películas de espionaje. Igual que un forense analiza la escena de un crimen, así escrutan estos analistas informáticos los aparatos digitales.

"Un ordenador lo cuenta todo. Sólo necesitamos hacer una copia del disco duro y crear una línea de tiempo de su uso para saber quién ha hecho qué en cada momento, incluso si ha habido intentos de borrar las huellas", explica Daniel Creus. Estos informes tienen validez como prueba para litigios judiciales en situaciones como fugas de información corporativa a manos de empleados despechados o en divorcios.

¿QUÉ CUENTA MI MÓVIL SOBRE MÍ?

Los expertos en seguridad informática aseguran que **los teléfonos móviles de última generación son nuestro principal semillero de rastros digitales**, así como el mayor boquete de seguridad informática con el que convivimos. En la práctica, los **smart-phones** son ordenadores de bolsillo, donde no solo guardamos fotos personales, listas de contactos y archivos de trabajo, sino también el correo, las contraseñas y a veces hasta aplicaciones para interactuar con el banco. Un simple hurto permite tener acceso a toda esa información. Por eso es raro encontrar a un profesional de la informática que no lleve su iPhone bloqueado con una clave que solo él conoce. El Consejo Nacional Consultor sobre Cyberseguridad ¿asociación que agrupa a las principales entidades de seguridad informática de España¿ ha elaborado un recetario de buenos usos del móvil que incluye consejos como **utilizar programas de cifrado para que la información que guardamos en él sea ilegible** por miradas extrañas, no conservar en su interior datos que sean sensibles, descargar solo aplicaciones fiables y vigilar el uso del *bluetooth* y el *wifi*. Atención también a lo que contamos vía Wasapp: los mensajes que enviamos a través de esta aplicación no van cifrados, por lo que son fácilmente accesibles desde otro teléfono móvil.

IPHONE CLAVE EN UN DESPIDO

"Cuando nos conectamos a una antena de wifi libre desconocida ignoramos que el tráfico de datos que realizamos a través de esa señal puede ser espiado. Con un software sencillísimo, en los aeropuertos se pueden espiar los paquetes de información que los usuarios se transfieren a través del iPhone. La gente no sabe el peligro que tienen estos aparatos", advierte el perito informático Carlos Aldama, quien recientemente trabajó en un proceso judicial donde el rastro digital escondido en un iPhone resultó clave: un

empleado despedido aseguraba que había estado atendiendo sus obligaciones contractuales, pero el GPS de su teléfono móvil le delató; en realidad había estado ausentándose de su destino laboral.

¿Y SI ME ARREPIENTO DE SUBIR MI FOTO A FACEBOOK?

De visitantes pasivos de webs, los usuarios hemos pasado en pocos años a ser suministradores de contenidos, sobre todo relacionados con nuestras vidas. Abiertamente y sin pudor alguno publicamos todo tipo de datos, opiniones y fotos en las redes sociales, sin reparar en los riesgos que esto entraña. Con cierta maldad ¿por tratarse de la competencia¿, pero sin exagerar, el presidente de Google, Erich Schmidt, alerta que los jóvenes están exhibiendo tantos detalles de sus vidas en Facebook que **"al cabo de unos años muchos desearán cambiar de nombre"**.

Esta reflexión lleva implícita otra aún más grave: **si quieres eliminar tu pasado en internet, será mejor que confíes en cambiar de identidad**, porque borrarlo es imposible. Los gestores de las principales redes sociales no se cansan de repetir que el usuario es libre de marcar la privacidad que desea tener y que puede eliminar los datos personales que quiera. Ocultan una letra pequeña de internet: en la misma red donde flota mi muro de Facebook, navegan también las páginas que se dedican a copiar y almacenar todo lo que se publica, desde Google a sitios como Archive.org, que tiene registrada la memoria de la red al completo.

Esto significa que **si tu página de Facebook ha sido captada** por uno de estos buscadores mientras estuvo colgada esa foto que te has arrepentido de publicar, **ya es tarde**: la dichosa foto ha quedado capturada para siempre en internet. Que se lo digan a Lucía Etxebarria: la escritora subió recientemente una foto semidesnuda a su perfil de Facebook y tardó unos minutos en advertir el error. Cuando quiso eliminarla, la instantánea se había difundido ya por toda la red.

¿PUEDO DESAPARECER DE INTERNET?

La **Agencia Española para la Protección de Datos** recibió en el 2010 casi un centenar solicitudes de ciudadanos que deseaban que sus referencias personales dejaran de estar visibles en internet. La cifra puede parecer ridícula, pero delata un síntoma novedoso: hasta ahora nadie había reparado en el valor que tiene la información personal que circula por la red, pero según esta entidad, que aún no ha publicado los datos del 2011, esa preocupación se está disparando.

Testigo de este fenómeno son las empresas que han surgido en los últimos meses para gestionar la demanda de los usuarios que desean que sus datos dejen de estar colgados permanentemente de forma *on line*.

Salirdeinternet (www.salirdeinternet.com) es una de ellas: echó a andar hace un año y medio y en este tiempo han acumulado una cartera de 600 clientes, así como algunos sonados éxitos.

Este equipo de abogados logró obligar a **Microsoft** a eliminar de su buscador, **Bing**, los datos de un directivo que había sido absuelto por una trama de corrupción, a pesar de lo cual seguía apareciendo como imputado en 100 páginas indexadas por este buscador. También han conseguido hacer desaparecer de Google algunos datos de otros clientes. **"¿Tiene sentido que personas indultadas sigan viendo, después de 20 años, sus publicaciones en los buscadores y en los medios que los publicaron?"**, se pregunta Miguel Cobacho, responsable de Salirdeinternet.

La Comisión Europea pretende ofrecer respuesta a esta demanda mediante una directiva que dará rango legal al **Derecho al Olvido**. La normativa exigirá a las empresas que ofrecen servicios en internet a cuidar con mayor celo los datos privados que tienen de sus usuarios y a que estos sean borrados si sus titulares así lo desean. Como sucede con todas las vallas que se intentan poner al campo de internet, la ley choca con un problema tecnológico. Así como el cierre de la web de intercambios de archivos **Megaupload** ha supuesto el crecimiento de otros portales P2P, los expertos creen que asegurar el borrado absoluto de datos personales en internet va a ser complicado. **¿Qué sucede con las copias** que quedan en los servidores de los buscadores que registran todo lo que se sube a la red?

QUEDA PARA SIEMPRE

Igualmente, estos también pueden eliminar datos de estas bibliotecas virtuales, si se les solicita, pero se tarda más. Durante ese tiempo, la información puede haber sido reproducida por infinidad de webs. En opinión de Álvaro Ibáñez, socio del blog de tecnología Microservos, vamos hacia un cambio de paradigma en relación con la privacidad, en el que este concepto será cada vez menos importante para la población. **"La gente aún no es consciente, pero va camino de serlo, de que todo lo que publicamos en la red es público, y queda para siempre"**, dice este experto