EL RASTRO DIGITAL

Viene de la página anterior

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 correos electrónicos que borramos de las cuentas personales.

El anonimato no existe

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.

«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 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 manejo científico de los datos que archivamos en formato digital ha alumbra-

EL ACOSADOR
Un individuo amenazó por Twitter a Eva Hache. La cuenta tenía una identidad falsa, pero la Guardia Civil siguió su rastro y lo cazó en 48 horas.

do 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. Solo 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 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 *smartphones* son ordenadores de bolsillo, donde no solamente guardamos fotos personales, listas de contactos y archivos de trabajo, sino también el correo electrónico, 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 *bluethoot* 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 una 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 sbió 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.

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.

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 Microsiervos, 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. ≡