¡Ya ha llegado el nuevo «cookie»!

FRANÇOIS SETTEMBRINO

Coordinador Académico de CRESEPT. Bélgica.
Anterior Presidente de FERMA (Asoc. Europea de Asociaciones de Gerencia de Riesgos) y BELRIM (Asoc. de Gerencia de Riesgos de Bélgica)

La captación no autorizada de información de los usuarios de las redes electrónicas representa una amenaza virtual, difícil de demostrar por parte de quien resulte agredido. Por ello, la protección funcional, lógica y jurídica se hace más necesaria para evitar tal incertidumbre.

Todos recibimos correo personalizado enviado a nuestro nombre, procedente de asociaciones a cual más caratitativa, o emitidos por empresas y organizaciones en busca de negocio. Todas las misivas empiezan por nuestro nombre y todas rivalizan en inventiva y creatividad para sacarnos donativos o para alabar los méritos, verdaderos o supuestos, de bienes y demás servicios que podemos conseguir a cambio de moneda contante y sonante o a cambio de pago, mucho más silencioso, mediante dinero electrónico.

Nuestro nombre y nuestra dirección se sacan, como todo el mundo se puede imaginar, de un fichero cuyos datos se han conseguido de forma onerosa de unos especialistas en la materia, que han recopilado, a veces con grandes gastos, una amplia serie de detalles que nos conciernen. La forma de recoger dichas informaciones es particularmente sútil. Para conseguir la más mínima información, para beneficiarse de los tentadores anuncios de regalos que abundan en nuestros buzones o en cualquier publicación, hay que dar un montón de informaciones sobre uno mismo, sobre su familia y sobre cualquier cosa, sin olvidar añadir dirección, número de teléfono, dirección electrónica. En virtud de las distintas reglamentaciones relativas a la protección de la intimidad, algunos se toman la precaución de re-

querir no contestar a todo, y que, por supuesto, las informaciones que hubiesen dado sólo se utilizarán dentro del marco o con el fin de que ha sido objeto la transacción. Los más correctos y completos le autorizan (es su derecho más estricto por otra parte) a consultar y comprobar los datos que le afectan y a corregirlos si fuera necesario.

El uso exacto del o de los ficheros sigue siendo, sin embargo, totalmente desconocido. El comerciante (o la cadena de supermercados) cuyo ticket de caja le saluda con su nombre exacto, posee por sí solo una mina de informaciones asombrosas. Conoce sus hábitos mejor que usted mismo, el importe, la periodicidad y los medios de pago que prefiere. Conoce tanto a sus banqueros como a sus números de cuenta, así como su calidad de buen o mal pagador. Gracias a las tarjetas de «fidelidad» conoce su dirección y demás especificaciones. Algunas personas -entre las cuales se cuenta el autor- se empeñan en no dar nunca su dirección de manera regular, basta con no poner mayúsculas por doquier, con poner el número de calle antes o después, con dar el o los nombres antes o después del apellido completo, abreviado o con iniciales. Resulta instructivo cuando el correo personalizado le llega; la sola lectura de la dirección le demuestra la diversidad de las fuentes. Si, además, se dedica a crear su propio banco de datos, puede identificar fácilmente donde han pescado su nombre.

Los sondeos espontáneos u organizados en los que haya participado constituyen otra fuente de informaciones. Habitualmente están llenos de preguntas complementarias que dan amplia información sobre la composición de su familia, las respectivas edades de sus miembros y sobre cualquier otra condición. Existen también los profesionales del fichero que poseen en sus sistemas centenares o miles de datos sobre millones de hogares. Para clientes más específicos, poseen unos paneles muy elaborados, que dan todas las informaciones posibles que uno pueda imaginar sobre consumidores potenciales, desde el jabón que utilizan hasta el tipo de seguro de jubilación que han elegido. Incluso los proveedores de servicios, con las sociedades telefónicas en cabeza, están en ello. En cada uno de ellos, por unos céntimos de euro por cabeza, obtendrá una serie de datos en la materia que le interesa, por categoría, por dirección, por localidad, por cualquier tipo de equipamiento (coche, casa, lavadora, número de hijos, etc.).

Los medios electrónicos están para que los utilicemos, ¿verdad? Se dice que algunos grandes países han llenado los sistemas de seguridad (policía, etc.) del mundo entero con puertas traseras («back doors»). Un «back door» consiste en una puerta de entrada desconocida para el usuario, ya instalada antes de la entrega de su material, y que permite el acceso por «detrás» a todo lo que haya sido grabado, sin tener que preocuparse de las claves y demás protecciones. Estremecedor... ¡El «Gran Hermano» no anda muy lejos!

Las manipulaciones electrónicas nos afectan a todos si utilizamos una conexión a Internet. Una sociedad americana, llamada Dejanews, archiva todo lo que se refiere a cualquier participante en un foro de debate, pero además archiva todos los mensajes que se han intercambiado. Si se explora con atención el sitio (http://www.dejanews.com) uno se entera de que más de 22 millones de personas pueden encontrar allí noticias procedentes de sus parientes y amigos, o ¡de su jefe! Pero no crean que hace falta formar parte de un foro para quedar al desnudo. Basta con navegar de un sitio a otro para que le espíen. Dicho espía no va recubierto de virutas de chocolate o de almendras, es diabólico y le han llamado «COOKIE». En cuanto alguien se conecta al sistema Microsoft, queda parasitado al instante. El «cookie» llega por el cable telefónico y va a esconderse en el disco duro. Y desde allí, lo observa y lo apunta todo, desde la o las claves hasta los trabajos realizados. Los cookies son

multiformes: algunos no se quedan más que el tiempo de una utilización, y otros permanecen al acecho en su rincón durante períodos más largos o ilimitados. Algunos sólo comen y regurgitan datos previamente escogidos como objetivo, y otros son omnívoros; todos actúan en beneficio de las organizaciones que los mandaron con esta misión.

¿Es ciencia ficción o acaso estamos todos contaminados ya? Eche un vistazo al CNL, Comisión Francesa de Informática y Libertad... En su dirección (http://www.cnil.fr) se demuestra cómo se recolectan las informaciones relativas a cualquier internauta. Todo se sabe: el navegador -Navigator de Netscape o Internet Explorer de Microsoft son los más utilizados-, el tipo de ordenador, los programas, el anterior sitio visitado, etc. y todo ello en cada conexión.

Según el Electronic Privacy Information Center de Estados Unidos, la mitad de los destinos poseen informaciones más o menos elaboradas sobre aquellos que los visitan. De tránsito en tránsito, en el proveedor de acceso del emisor, en cada proveedor intermedio y en el proveedor de acceso al destinatario, las pausas duran algunos segundos, y a veces mucho más. Esto basta para seleccionar ciertas informaciones en el recorrido del correo y de las conversaciones. En un debate se planteó la pregunta crucial respecto de las protecciones jurídicas, a falta de protecciones técnicas, y la respuesta no fue nada tranquilizadora. De hecho, no habrá respuesta hasta que pase mucho tiempo, sobre todo porque la técnica no entiende de fronteras ni de los derechos relacionados con éstas. Cualquier sitio puede infiltrar en el ordenador de cada usuario, uno o varios «ciber espías». Mientras éste se limita a registrar unas informaciones de uso puramente comercial, podemos lamentarlo, pues cada uno de nosotros se convierte en un objetivo definido para las empresas comerciales, que aprovecharán para proponer su mercancía con argumentos más afinados, para así seducirle mejor. Pero los deslices son inevitables y pueden convertirse en una voluntad de dañar. Los nuevos virus pueden adoptar las mismas estrategias que los «cookies». El último, denunciado por la propia Microsoft, absorbe por completo la sustancia del disco duro y regurgita, no se sabe donde, todo lo que ha encontrado, incluso las claves. Se presenta bajo el prometedor aspecto de un ahorrador de pantalla propuesto con toda amabilidad, pero se vuelve despiadado cuando se le ordena que actúe.

En ausencia de virus, el «cookie» puede todavía desvelar aspectos ocultos de su personalidad. Si la información llega a manos o a oídos desconocidos, no resulta muy grave, aunque a nadie le gusta ver su vida expuesta públicamente, y menos aún mundialmente. Pero si la información cae en manos de gente próxima, de un jefe o de una autoridad, es decir de personas que le conocen, los daños pueden ser incalculables e irreparables.

Otro aspecto de la protección de la información atañe a todas las organizaciones que no han puesto barreras entre su Intranet e Internet -nos podemos preguntar, por otra parte, si existen realmente barreras infraqueables-. Su gerente de riesgos tendrá que encontrar algunas protecciones fiables. Algunos, en previsión de lo que está ocurriendo, han separado totalmente ambas actividades. El interno funciona únicamente sobre sí mismo, en Intranet absoluto, y un segundo sistema es el encargado del exterior, hacia Internet. La dificultad consiste en encontrar los puentes adecuados y que puedan funcionar con total seguridad. ¡Resulta, sin duda, todavía más arduo que el eficaz control del Síndrome del Milenio! ■