

La Red espía tus movimientos

REPORTAJE.- Sofisticados programas informáticos rastrean correos personales y 'blogs' protegidos - No sólo los regímenes autoritarios invaden la intimidad.

Internet, como red de redes sobre la que no gobierna nadie, no conoce fronteras. Pero los regímenes autoritarios, sí. Países como China e Irán han invertido verdaderas fortunas en tecnologías para poner coto a la libertad de expresión en sus conexiones a la Red. Ya no se limitan a cerrar páginas o censurar resultados en motores de búsqueda. Ahora son capaces de espiar al internauta a través de sus proveedores de conexión. Leen sus correos electrónicos y blogs restringidos y controlan al detalle qué páginas visitan. Esa tecnología acaba con la intimidad en la Red. Y no sólo la aplican los Gobiernos no democráticos. Proveedores de Internet de Estados Unidos la utilizan para combatir lo que consideran piratería.

Existe en Internet un nuevo telón de acero cibernético, que separa a los países que respetan la libertad democrática en la Red de los regímenes que la silencian para imponer doctrinas políticas. Lo ha dibujado meticulosamente la organización privada Reporteros Sin Fronteras, que en un informe de marzo del año pasado identificó a los 12 "enemigos de Internet": Irán, China, Cuba, Egipto, Corea del Norte, Siria, Túnez, Arabia Saudí, Vietnam, Myanmar, Turkmenistán y Uzbekistán.

Uno de los métodos más sofisticados para censurar la Red lo ejerce Irán. El Gobierno de aquella nación ha suprimido miles de blogs en los que jóvenes reformistas informaban de las protestas callejeras en contra de la reelección del presidente Mahmud Ahmadinejad. En un país donde no hay libertad de expresión y donde, según un informe de 2008 de la Universidad de Harvard, existen unos 60.000 blogs, aquellos testimonios han sido una valiosa ventana al descontento social que sacude al régimen.

La detención de blogueros es moneda corriente en Irán, y no sólo desde el año pasado, el de las polémicas elecciones presidenciales. A Roozbeh Mirebrahimi le detuvieron en 2004, cuando los reformistas todavía gobernaban el país. Este periodista y bloguero osó escribir en su página web sobre asuntos incómodos para el Gobierno, como las elecciones parlamentarias de 2004, en las que el Consejo de Guardianes prohibió presentarse a miles de candidatos reformistas, o la muerte de la periodista canadiense-iraní Zahra Kazemi, en pleno interrogatorio por parte de la policía iraní.

Pasó dos meses en prisión y fue puesto en libertad bajo fianza. Huyó a París y, en ausencia, fue condenado en febrero del año pasado a dos años de cárcel y 84 latigazos. Hoy, desde el exilio en Nueva York, cuelga en su blog, IranDarJahan, noticias internacionales traducidas al farsi. "En los últimos años, el Gobierno ha gastado mucho dinero en adaptar sus controles a las nuevas tecnologías", explica. "¡Incluso tienen un ejército cibernético para perseguir a ciberperiodistas y blogueros! Antes no sabían nada de la red. Hoy es un medio imprescindible para reducir a los reformistas".

Otros no viven para contarlo. Es el caso del joven Omidreza Mirsayafi, fallecido el pasado mes de marzo en la temida prisión Evin, en Teherán. La versión oficial: se suicidó tomando pastillas para dormir. Su familia, sin embargo, dijo a Radio Farda, una radio en farsi patrocinada por el gobierno norteamericano, que Mirsayafi sufría problemas cardiovasculares y que sus guardas se negaron a someterlo a un examen médico adecuado. Murió encarcelado, posiblemente de un paro cardíaco.

El 2 de noviembre de 2008 se le había juzgado y condenado a la pena máxima de dos años que conlleva insultar al fallecido líder supremo de la revolución, Ruhollah Jomeini, padre de la república islámica. Su delito: haber escrito dos artículos satíricos sobre su país en su blog, Rooznegar, dedicado en su mayoría a comentar las artes de su país.

Según dijo él mismo a la organización Reporteros Sin Fronteras: "Soy un bloguero cultural, no político. De todos mis artículos, sólo dos o tres eran satíricos. No quise insultar a nadie". Es más, Mirsayafi se sentía seguro porque su blog estaba restringido a algunos amigos. Pensaba que el Gobierno no podía leer su diario, escrito sólo para un puñado de personas que debían registrarse y ser autorizadas por él para acceder al blog. Fue un error. Porque si hay algo en lo que

el Gobierno de Irán es sofisticado es en leer correos privados y páginas supuestamente protegidas.

Para ello cuenta con un control total sobre sus conexiones a Internet. Expertos en ciberseguridad afirman que Irán dispone de una sofisticada tecnología conocida como Inspección Profunda de Paquetes, que utilizan otros regímenes, hermanos en represión, como China, para controlar a individuos sospechosos.

El verano pasado, el diario The Wall Street Journal publicó que las empresas europeas Nokia y Siemens habían vendido esa misma tecnología a Irán. Un portavoz de ambas empresas niega este extremo. "Le vendimos a Irán la capacidad de controlar llamadas de móvil en redes 2G, dentro de un servicio de redes más amplio", explica. "No vendimos acceso a Internet en Irán y por lo tanto no podemos ofrecer allí la capacidad de interceptar correos o información de Internet". El año pasado, ambas empresas abandonaron sus negocios en aquel país.

Lo cierto es que Irán puede ejercer esa capacidad, de inspeccionar los mensajes en la Red, sin la ayuda de empresas extranjeras, sólo con el control estatal de las conexiones. Internet funciona como una red de puertos conectados a sistemas autónomos, pequeñas redes que se unen en una gran red de redes no gobernada por nadie. Cada proveedor de una de esas redes se compromete a facilitar, en principio, que cada puerto, desde su dirección IP, comparta información (correos electrónicos, intercambio de archivos, visitas a páginas web) con otros puertos, en cualquiera de las demás redes autónomas.

Cuando es un Gobierno no democrático quien controla esos puertos, puede interferir en la navegación de sus usuarios. Puede prohibir la comunicación entre dos o más puertos. Puede desconectar a internautas. O puede aplicar la censura a su antojo, con aquellos sofisticados programas informáticos, espionando los paquetes que transmiten la información en la Red.

Esos paquetes de información, llamados datagramas, son como pequeñas cartas. Tal y como explicó el ingeniero y padre de Internet David P. Reed ante el Congreso de EE UU en julio de 2008, "cada carta tiene un sobre que contiene una información en su exterior con sólo cuatro elementos: una dirección de envío, un remitente, un identificador de protocolo y algunos marcadores que indican cómo se distribuye el mensaje mientras se transporta en la red. El contenido de cada mensaje se guarda dentro del sobre. Ese contenido sólo es relevante para quienes lo envían o reciben".

En ciertas redes, como las que controlan los ayatolás, los carteros tienen permiso para abrir los sobres y leerlos. Así de sencillo. "El término Inspección Profunda de Paquetes se inventó para describir sistemas que inspeccionan en tiempo real y utilizan contenido de dentro de esos sobres", explica Reed. "Es una tecnología que puede ser explicada como los dispositivos que se instalan en camiones, aviones o almacenes de las empresas de mensajería que pueden examinar rápida y eficazmente qué hay dentro de cada paquete, con rayos X o tal vez llegando a abrir el paquete".

"Es un sistema muy sofisticado de espionaje", explica Justin Brookman, del Centro para la Democracia y la Tecnología, que fue jefe del departamento de Internet del fiscal general de Nueva York. "Hay formas mucho más accesibles de censura, al alcance de cualquier Gobierno. Por ejemplo: China simplemente le debe decir a Google o a Yahoo qué páginas esconder o qué términos silenciar. Y si no cumplen, ordena a los proveedores de Internet nacionales que prohíban esos sitios web".

Ahora, después de un ataque sufrido en sus servidores en diciembre, Google ha dejado abandonar la censura en China. Ha tardado cuatro años en tomar esa decisión. Y tres desde que el periodista Shi Tao acabó en la cárcel con la inestimable ayuda de otro gigante de la Red norteamericano, también con intereses en China: Yahoo.

En 2004 el Gobierno de Pekín prohibió mediante decreto que los periodistas informaran del 15 aniversario de la masacre de la plaza de Tiananmen, en la que murieron unas 3.000 personas. Para ello, difundió una nota secreta a diversos medios, entre ellos la revista Actualidad Empresarial, donde trabajaba Tao. En una reunión de la redacción se reveló la existencia de ese decreto y se anunció a los periodistas que era confidencial y no se podía informar de su existencia. Tras la reunión, Tao envió un correo revelando la existencia de la ordenanza a Hong Zhesheng, de la Fundación por un Asia Democrática, en Nueva York. Usó su cuenta de correo personal de Yahoo.

Cuando el Gobierno chino pidió a Yahoo información sobre aquella filtración, Yahoo cumplió. Y no se quedó corto en la información que puso al alcance de los policías. Esta es una prueba que se cita en el veredicto de la corte criminal de la provincia de Hunan que condenó a Tao a 10 años de cárcel en 2005, según una traducción de la organización privada Global Voices: "Yahoo Holdings (Hong Kong) Ltd., confirma que la dirección IP 218.76.8.201, a las 23:32:17 p.m. del 20 de abril de 2004, el usuario correspondiente se conectó con la línea de teléfono 0731-4376362 situada en el edificio de Actualidad Empresarial en Hunan; dirección: 2F, Edificio 88, Nueva Villa de Jianxiang, Distrito de Kaifu, Changsa". Más precisión, imposible. Tao ya ha pasado en la cárcel cinco años.

El Congreso de EE UU abrió una investigación y la Cámara de Representantes interrogó al entonces consejero delegado Jerry Yang y al Consejero General Michael Callahan. "Si piensan ustedes que nuestros dos testigos están incómodos hoy aquí, sentados en esta sala con aire acondicionado y rindiendo cuentas por los actos serviles e irresponsables de sus acciones, imagínense la vida de Shi Tao, que está pasando 10 largos años en una mazmorra china por intercambiar información públicamente", dijo entonces el ya fallecido representante demócrata Tom Lantos.

Yang, máximo responsable de la empresa, no nombró en su testimonio a Tao ni una sola vez. Es más, dijo: "Aun creemos en seguir presentes en China. ¿Por qué? Hoy en día, a pesar de las amplias limitaciones en asuntos políticos sensibles, los ciudadanos chinos saben más que nunca sobre asuntos de salud pública local, causas medioambientales, política, corrupción, derechos de los consumidores, empleo e incluso relaciones internacionales".

Y mientras, Tao en la cárcel. Y Yahoo ya sin poder hacer nada. En 2005, tras el arresto de Tao, la empresa matriz vendió Yahoo China a una empresa local, Alibaba, de la que, a su vez, compró acciones. Ahora es Alibaba quien censura Yahoo en chino, y en la sede de Yahoo en EE UU no tienen, ni siquiera, que lavarse las manos, en su papel de mero "accionista minoritario", como se presentó Yang -que ya no trabaja en la empresa- al Congreso en 2007.

El Congreso de EE UU lo tenía entonces fácil para condenar públicamente a Yahoo por su colaboración con el régimen chino. Pero la clase política de EE UU no lo tuvo tan fácil cuando el problema apareció en casa. En 2005 se supo que el ex presidente George Bush autorizó en 2001 a la Agencia de Seguridad Nacional (NSA por sus siglas en inglés) que interceptara las comunicaciones de Internet de individuos investigados por supuestas actividades terroristas, sin necesidad de autorización judicial previa. Y para ello, la NSA contó con la Tecnología de Inspección de Paquetes y la ayuda de operadoras de telefonía nacionales como AT&T.

El programa duró seis años. En 2007, Bush ordenó a su fiscal general (ministro de justicia) Alberto Gonzales que retirara aquella autorización a la NSA, ante las críticas de políticos y grupos civiles. La Fundación Frontera Electrónica, sin embargo, había presentado una demanda colectiva contra AT&T en 2006 por violar las cláusulas de privacidad firmadas con sus clientes. No importó. Bush, antes de dejar la Casa Blanca, en 2008, firmó un decreto en el que concedía inmunidad retroactiva a las empresas de telefonía que hubieran participado en aquel programa. En 2009 un juez de California desestimó la demanda.

Aquello, sin embargo, abrió los ojos a muchos ciudadanos: la inmensa mayoría de proveedores de Internet en EE UU disponen de esa misma tecnología que tantos estragos causa en China o Irán. Y la usan. "Hay usos de la Inspección de Paquetes que son legítimos, de acuerdo con la ley, como cuando la seguridad nacional está en juego o cuando se trate de luchar contra la piratería o ataques de hackers. En esos casos su uso es legal", explica el abogado Brookman, del Centro para la Democracia y la Tecnología.

Las empresas usan, es cierto, esa tecnología, pero con fines, aseguran, puramente legales y comerciales. Acceden a esos sobres de información y si descubren que el usuario está enviando paquetes que contienen archivos descargados a través de un programa de intercambio de archivos P2P, potencialmente ilegales, pueden ralentizar la conexión. Lo hacen, aseguran, para poder ofrecer servicios de máxima calidad y para que la Red no se colapse, hundida por canciones y películas compartidas ilegalmente.

La Comisión Federal de Comunicaciones, en 2008, desautorizó a uno de los mayores proveedores de Internet de EE UU por ese mismo motivo en un informe: "Se nos encargó que consideráramos si Comcast, proveedor de banda ancha a través de cable, está interfiriendo selectivamente sobre ciertas conexiones de programas de P2P. Aunque Comcast asegura que debe hacerlo necesariamente para combatir la congestión de la Red, nosotros concluimos que esas prácticas, discriminatorias y arbitrarias, coartan la existencia de un Internet abierto y accesible y no conforman una gestión de redes razonable".

La profesora de derecho de la Universidad de Santa Clara Catherine Sandoval considera que se trata de una práctica que entraña serios riesgos y puede llevar a infracciones de la ley. "Comcast dice que sólo accede a la información que está en el encabezado, en los sobres de esos paquetes, para discriminar qué información es legítima y cuál no", explica. "Pero no puede saber si dos personas que intercambian archivos P2P están enviándose documentos de trabajo o archivos personales, totalmente legales, a menos que entre dentro de esos sobres y tenga acceso a la información".

"Los proveedores de Internet están demonizando una serie de programas, como BitTorrent, y con ello pretenden hacer lo que les venga en gana a la hora de gestionar las conexiones que ofrecen a sus clientes. Y claro, utilizan una tecnología que se usa en Irán y en China para otros fines, y que encierra en sí misma las posibilidades de inspeccionar totalmente las comunicaciones en la Red e infringir la legislación vigente sobre derecho a la privacidad".

Al fin y al cabo, incluso los robots de Google leen los correos electrónicos que se envían y reciben a través de su servicio de correo, Gmail, para incluir en ellos publicidad relevante y de supuesto interés para el internauta. El de Internet es un mundo todavía caótico, con normas vigentes en unos países y totalmente ausentes en otros. Diversas técnicas de censura campan a sus anchas en países totalitarios. Pero toman la forma de control legal del tráfico de Internet en países que respetan el libre mercado y la libertad de información.

[EL PAÍS](#)

Fecha artículo: lun 08 feb 2010 05:59:00 CET

Cristino Martos, 4
28015 Madrid

Tel 91 540 92 82 Fax 91 548 28 10
comfia@comfia.ccoo.es