El pequeño Libro Rojo del activista en la Red

eldiario.es libros

El pequeño Libro Rojo del activista en la Red

Introducción a la criptografía para redacciones, *whistleblowers*, activistas, disidentes y personas humanas en general

Marta Peirano

eldiario.es libros

Rocaeditorial

Primera edición: enero de 2015

© de esta edición: Roca Editorial de Libros, S. L.
Av. Marquès de l'Argentera 17, pral.
08003 Barcelona
info@rocaeditorial.com
www.rocaeditorial.com

www.eldiario.es

Impreso por LIBERDÚPLEX, S.L.U.
Crta. BV-2249, km 7,4, Pol. Ind. Torrentfondo
Sant Llorenç d'Hortons (Barcelona)

ISBN: 978-84-9918-777-8
Depósito legal: B-6.867-2014
Código IBIC: UBW

RE87778

«Si estamos, como parece, en pleno proceso de convertirnos
en una sociedad totalitaria donde el aparato de Estado
es todopoderoso, entonces el código moral imprescindible
para la supervivencia del individuo libre y verdadero
será engañar, mentir, ocultar, aparentar, escapar, falsificar
documentos, construir aparatos electrónicos en tu garaje
capaces de superar los *gadgets* de las autoridades. Si la pantalla
de tu televisor te vigila, invierte los cables por la noche,
cuando te permitan tenerlo apagado. Y hazlo de manera
que el perro policía que vigilaba la transmisión de tu casa
acabe mirando el contenido de su propio salón.»

PHILIP K. DICK, *The Android and the Human*, 1972

«The internet is on principle a system that you reveal yourself to in order to fully enjoy, which differentiates it from, say, a music player. It is a TV that watches you. The majority of people in developed countries spend at least some time interacting with the Internet, and Governments are abusing that necessity in secret to extend their powers beyond what is necessary and appropriate.»

Edward Snowden, 2013

Prólogo

por Edward Snowden

Nuestra habilidad para entender el mundo en que vivimos depende fundamentalmente de los intercambios no autorizados y no vigilados entre los periodistas de investigación y sus fuentes. La vigilancia persistente del periodismo de investigación debilita las libertades básicas que proporciona la libertad de prensa, socavando estructuras democráticas elementales.

Sin embargo, los periodistas no son expertos en seguridad. Las escuelas de periodismo no ofrecen cursos para aprender a usar herramientas de seguridad diseñadas para proteger la información y las comunicaciones. Y, cuando una fuente decide soltar la liebre y exponer el abuso de un gobierno, los periodistas ya no tienen tiempo de ponerse a aprender las medidas básicas de seguridad. La revelación de los programas indiscriminados de vigilancia de la NSA en Estados Unidos, la GCHQ en Inglaterra y otras agencias de seguridad gubernamentales a lo largo de los últimos años nos ha demostrado que la privacidad digital no es algo que se pueda dar por hecho, especialmente si eres un periodista de investigación.

Gracias a los avances de la tecnología, los sistemas de vigilancia masiva de hoy pueden registrar en tiempo real

todos los metadatos de todas las comunicaciones que se estén dando en cualquier país, todo con un coste y un grado de complejidad tan accesible que está al alcance de literalmente cualquier gobierno del planeta. Esa acumulación de metadatos puede revelar una red completa de vínculos y asociaciones humanos, exponiendo cualquier interacción que pueda ser percibida como una amenaza para el régimen de poder establecido.

Como consecuencia, la vigilancia masiva representa un arma contra aquellos pocos que deciden convertirse en fuentes de información periodística, porque revela sus identidades, sus estructuras de apoyo y sus lugares de residencia o de refugio. Es información que los gobiernos pueden usar para eliminar el riesgo de futuras revelaciones por parte de esa fuente. Sus métodos pueden variar: una citación judicial en Estados Unidos puede hacer el mismo trabajo que una bala en Quetta o Chechenia. Pero el impacto sobre la fuente y el periodismo de investigación es el mismo.

Como profesionales, los periodistas tienen la responsabilidad de aplicar las mejores prácticas de seguridad antes de ponerse en contacto con un confidente por primera vez. Dicho de otra manera: nadie espera que un paciente que entra en una consulta médica le tenga que recordar a su médico que se cambie los guantes. Un periodista hoy en día necesita poseer un conocimiento funcional de las técnicas para anonimizar y de las herramientas de cifrado. También deben aprender a usarlas de manera efectiva.

A la luz de las revelaciones sobre las capacidades de los gobiernos, esta nueva responsabilidad puede resultar abrumadora. No basta con que los periodistas sepan establecer una clave pública PGP. Un periodista debe entender cómo funcionan las herramientas de seguridad y cómo no funcionan, y adaptar sus actividades a las limitaciones de esa tecnología. Por ejemplo, hay muchas herramientas de seguridad digital que protegen muy bien un contenido, pero dejan los

metadatos al aire. Esto significa que el cifrado de un correo es tan seguro y efectivo como las palabras que elegimos para poner en el asunto o el nombre que le damos a un adjunto.

El periodista también debe conocer a su adversario. Debe saber cómo se interceptan las llamadas telefónicas, y que una línea segura tiene que estar protegida a ambos lados de la comunicación. Debe valorar las maneras en que la falta de tiempo, el margen de error y la reducción de recursos pueden devaluar el plan de seguridad más sensato y sus implementaciones. Deben tener siempre un plan B y prever circunvalaciones cuando el ordenador o el correo de una fuente ha sido comprometido. Deben conocer las técnicas para asegurar y corroborar la información pública que han acumulado.

Por este y otros motivos, *El pequeño Libro Rojo del activista en la Red* es un recurso esencial para asegurar que aquellos que recogen, analizan y transmiten información a la sociedad puedan proteger, no solo su trabajo, sino también —y por encima de todo— a sus fuentes.

La democracia depende de la existencia de una prensa valiente y con capacidad para realizar un periodismo de investigación, una que mide su éxito en su capacidad para exponer los abusos de la autoridad al gran público. Por eso, cada vez que un aparato de vigilancia masiva se pueda usar para monitorizar todos los encuentros «no autorizados» entre un reportero de investigación y su fuente, la prensa libre se tambaleará. Y sin la prensa libre, todas las instituciones de librepensamiento de la sociedad desaparecerán.

EDWARD SNOWDEN
Diciembre 2014

CÓMO COMBATIR LA VIGILANCIA ONLINE

Navegación

1. TOR BROWSER BUNDLE

Incluye todo lo que necesitas para acceder a la Tor Network. Hace que sea más difícil rastrear tu actividad en Internet: historial de navegación, *posts*, mensajes instantáneos y otros formatos de comunicación. No previene el tráfico de entrada y salida a la red. Mientras Tor te protege contra el análisis del tráfico, no puede prevenir la confirmación del mismo (también llamada *e2e*).

2. BLEACH BIT

Tiene varias herramientas con las que podrás limpiar, liberar espacio en tu ordenador y resguardar tu privacidad.

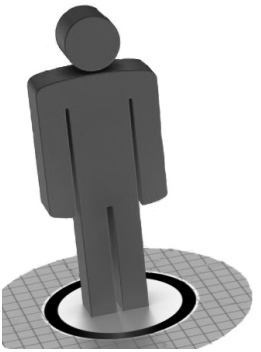
↳ www.torproject.org
↳ www.bleachbit.sourceforge.net

Seguridad portátil

3. TAILS

Un sistema operativo vivo. Puede instalarse en cualquier PC con un DVD o un pendrive. Protege tu privacidad y anonimato. Tiene incorporadas muchas aplicaciones preconfiguradas con el fin de preservar toda tu información sobre navegadores, mensajes instantáneos, e-mails, aplicaciones para oficina y más.

↳ https://tails.boum.org

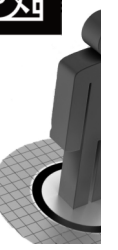


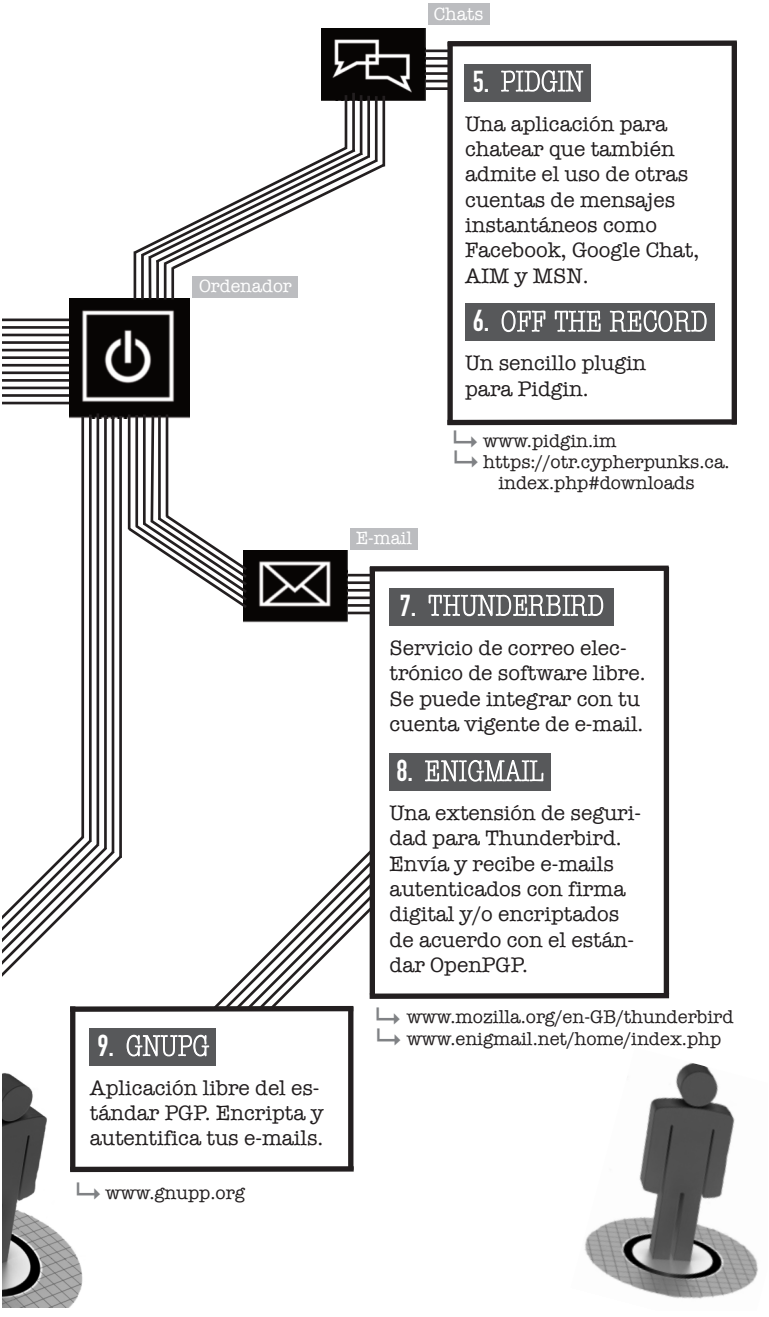
Disco encriptado

4. TRUECRYPT

Crea discos duros virtuales que encriptarán cualquier archivo que guardes en ellos. Usa varios tipos de encriptación.

↳ www.truecrypt.org





5. PIDGIN

Una aplicación para chatear que también admite el uso de otras cuentas de mensajes instantáneos como Facebook, Google Chat, AIM y MSN.

6. OFF THE RECORD

Un sencillo plugin para Pidgin.

↳ www.pidgin.im
↳ https://otr.cypherpunks.ca.index.php#downloads

7. THUNDERBIRD

Servicio de correo electrónico de software libre. Se puede integrar con tu cuenta vigente de e-mail.

8. ENIGMAIL

Una extensión de seguridad para Thunderbird. Envía y recibe e-mails autenticados con firma digital y/o encriptados de acuerdo con el estándar OpenPGP.

↳ www.mozilla.org/en-GB/thunderbird
↳ www.enigmail.net/home/index.php

9. GNUPG

Aplicación libre del estándar PGP. Encripta y autentifica tus e-mails.

↳ www.gnupp.org

Glenn Greenwald, Edward Snowden y la importancia de saber cifrar

La historia ya es leyenda: Glenn Greenwald estuvo a punto de perder el mayor bombazo periodístico de las últimas décadas solo porque no quiso instalarse la PGP. Él mismo la contaba con sana ironía cuando, seis meses más tarde, le invitaron a dar una conferencia como cabeza de cartel en el congreso del Chaos Computer Club, el mismo festival de *hackers* donde cinco años antes se presentó WikiLeaks. Todo empezó cuando el 1 de diciembre de 2012 Greenwald recibió una nota de un desconocido pidiéndole su clave pública para mandarle cierta información de suma importancia.

A pesar de tratar con fuentes delicadas y escribir sobre asuntos de seguridad nacional; a pesar de su apasionada defensa de WikiLeaks y de Chelsey (entonces Bradley) Manning, Glenn Greenwald no sabía entonces lo que era una clave pública. No sabía cómo instalarla ni cómo usarla y tenía dudas de que le hiciera falta, así que, cuando llegó un misterioso desconocido pidiendo que la utilizara, simplemente le ignoró. Poco después, el desconocido le mandó un tutorial sobre cómo encriptar correos. Cuando Greenwald ignoró el tutorial, le envió un vídeo de cifrado para *dummies*.

«Cuanto más cosas me mandaba más cuesta arriba se me hacía todo —confesó Greenwald más tarde a la revista *Rolling Stone*—. ¿Ahora tengo que mirar un estúpido vídeo?» La comunicación quedó atascada en un punto muerto, porque Greenwald no tenía tiempo de aprender a cifrar correos para hablar con un anónimo sin saber lo que le quería contar y su fuente no podía contarle lo que sabía sin asegurarse de que nadie escu-

chaba la conversación. Lo que hoy parece obvio entonces no lo era, porque ahora todos sabemos lo que la fuente sabía pero Greenwald ignoraba: que todos y cada uno de sus movimientos estaban siendo registrados por la Agencia de Seguridad Nacional norteamericana. La fuente lo sabía porque trabajaba allí.

Pero Greenwald recibía correos similares cada día. A medio camino entre el periodismo y el activismo, gracias a su trabajo en la revista *Salon*, su cuenta en Twitter y su columna en *The Guardian*, el periodista se había convertido en la bestia negra del abuso corporativo y gubernamental y su carpeta de correo estaba llena de anónimos prometiendo la noticia del siglo que luego quedaban en nada. Después de un mes, la fuente se dio por vencida. Seis meses más tarde, Greenwald recibió la llamada de alguien que sí sabía lo que era la PGP: la documentalista Laura Poitras.

Poitras no solo sabía encriptar correos; se había pasado los dos últimos años trabajando en un documental sobre la vigilancia y el anonimato. Había entrevistado a Julian Assange, a Jacob Appelbaum y a otros. No era un tema al que estaba naturalmente predispuesta, sino al que se vio empujada desde que la pararon por primera vez en el aeropuerto internacional de Newark, cuando la cineasta iba a Israel a presentar su último proyecto, *My Country, My Country*.

Se trataba de un documental sobre la vida del doctor Riyadh al-Adhadh y su familia en la Bagdad ocupada. Poitras había convivido con ellos mientras filmaba la película y un día estaba en el tejado de su casa con la cámara cuando tuvo lugar un ataque de la guerrilla local en el que murió un soldado norteamericano. Que Poitras estuviera por casualidad en el tejado y lo grabara todo generó rumores entre las tropas. Los soldados la acusaron de estar al tanto de la insurrección y de no haberles avisado para así asegurarse material dramático para su documental. Aunque nunca fue acusada formalmente, y nunca hubo pruebas, sus billetes fueron marcados como «SSSS» (Secondary Security Screening Selection). Poitras ya no pudo coger un avión sin ser interrogada y sus pertenencias registradas.

Después de los ataques a las Torres Gemelas, el gobierno norteamericano empezó una lista negra de posibles terroristas

que ha llegado a tener un millón de nombres. Un agente en el aeropuerto de Viena le explicó a Poitras que su pasaporte había sido marcado con la alerta máxima («400 en la escala Richter», le dijo) y que en ningún aeropuerto del mundo la dejarían volar sin antes registrarla. En su entrevista con el *Times*, Poitras dice que ya no recuerda cuántas veces la detuvieron en los siguientes seis años pero que fueron más de cuarenta. En muchos casos, los agentes del aeropuerto exigieron acceso a sus cuadernos y ordenadores para poder copiar su contenido y, en al menos una ocasión, requisaron todo su equipo durante varias semanas. Un día se le ocurrió que, si estaba en la lista negra y la paraban cada vez que viajaba, lo más probable era que su correo y su historial de navegación también estuvieran comprometidos.

«Supongo que hay cartas de seguridad nacional en todos mis correos», dice Poitras en la misma entrevista. La «carta de seguridad nacional» (National Security Letter o NSL) es una orden de registro que reciben los proveedores de servicios —las compañías telefónicas o los servidores de red— para que faciliten los datos de un usuario. Todas las comunicaciones electrónicas son susceptibles de recibir una sin que sea necesaria la intervención de un juez, y la proveedora tiene prohibido advertir el registro a su cliente. En 2011, Laura Poitras empezó a trabajar en su documental sobre la vigilancia gubernamental y, en el proceso, aprendió a proteger sus comunicaciones.

Empezó a dejar el móvil en casa, un dispositivo que no solo registra las conversaciones sino que funciona como localizador, incluso cuando todos los sistemas de localización y hasta el propio teléfono han sido desactivados. Dejó de tratar asuntos delicados por correo y empezó a usar un anonimizador para navegar por la Red. Aprendió a encriptar sus e-mails con una llave de clave pública. Empezó a usar diferentes ordenadores: uno para editar sus documentales, otro para mandar correos y un tercero sin tarjeta de red para almacenar material sensible. Por eso, cuando un anónimo le escribió para pedir su clave pública, Poitras se la dio inmediatamente. Una vez convencida de la seriedad de su contacto y la legitimidad de sus documentos, Poitras se puso en contacto con Greenwald, al que había entrevistado para su documental y, a cambio, había escrito sobre ella en *Salon*

(«U.S. Filmmaker Repeatedly Detained at Border», abril 2012). En junio de 2013 volaron juntos a Hong Kong para encontrarse con Edward Snowden y destapar el mayor caso de espionaje masivo de la historia.

Todos los periodistas a los que les cuento esta historia se ríen, pero es raro encontrar a uno que tenga software diseñado para proteger sus comunicaciones en su ordenador. «Me sorprendió darme cuenta de que había gente en los medios que no sabía que todo correo enviado sin cifrar a través de la red acaba en todas las agencias de inteligencia del planeta —dijo Snowden en una entrevista cuando se publicó esta historia—. A la vista de las revelaciones de este año, debería estar ya suficientemente claro que el intercambio no cifrado de información entre fuentes y periodistas es un descuido imperdonable.» Snowden es un experto en seguridad informática cuyo acceso a los numerosos programas de vigilancia total desarrollados por y para la *National Security Agency* (NSA, Agencia de Seguridad Nacional) fundamentaron su puntillosidad. Gracias a su cuidadosa estrategia ha sido capaz de controlar las circunstancias de sus extraordinarias revelaciones y escapar de Estados Unidos antes de ser encarcelado, como Bradley Manning. Si no hubiera sido tan paranoico, le habría pasado lo mismo que a las fuentes del cineasta Sean McAllister en el país más peligroso del mundo para periodistas y disidentes: Siria.