CENSURA Y VIGILANCIA DE PERIODISTAS: UN NEGOCIO SIN ESCRÚPULOS

REPORTEROS
SIN FRONTERAS
POR LA LIBERTAD DE INFORMACIÓN

INFORME DE REPORTEROS SIN FRONTERAS
REZA MOINI / BENJAMIN ISMAIL / ELODIE VIALLE

ÍNDICE

Tapa : ©FRED TANNEAU / AFP

INTRODUCCIÓN

CON OCASIÓN DEL DÍA MUNDIAL CONTRA LA CIBERCENSURA, REPORTEROS SIN FRONTERAS (RSF) DEPLORA LA SUMISIÓN DE LOS GIGANTES DE LA WEB, QUE NO DUDAN EN RESPONDER A LAS EXIGENCIAS DE LOS REGÍMENES AUTORITARIOS EN MATERIA DE CENSURA.

TAMBIÉN LAMENTA QUE LA FALTA DE MECANISMOS INTERNACIONALES DE REGULACIÓN DE LA TECNOLOGÍA DE VIGILANCIA PERMITA QUE LAS EMPRESAS VENDAN HERRAMIENTAS DE VIGILANCIA EN LÍNEA A REGÍMENES AUTORITARIOS, HACIENDO DE LADO LOS DERECHOS HUMANOS PARA GANAR UN SEGMENTO DE MERCADO.

1 CENSURA: LOS GIGANTES DE LA WEB ENTRE SUMISIÓN Y COLABORACIÓN ACTIVA

En noviembre de 2016 The New York Times (NYT) reveló que Facebook –de manera confidencial y con el apoyo de su fundador, Mark Zuckerberg– desarrollaba un programa para censurar los contenidos de los usuarios de la red social, según su ubicación geográfica. Empleados de Facebook señalaron que la empresa estadounidense busca poder responder a las exigencias del régimen chino en materia de censura. Con esta herramienta, la firma vislumbra su regreso al mercado chino, del que fue expulsada en 2009, durante las rebeliones de la minoría uigur en Xinjiang, que usaba Facebook para difundir información sobre la represión de las protestas.

La firma californiana suscita preocupación debido a su colaboración activa con ciertos Estados, a la supresión de contenidos periodísticos y a su política opaca de «moderación" de contenidos. Por ejemplo, en diciembre pasado Facebook bloqueó varios días la Fan Page del sitio informativo ARA News, sin ninguna explicación. Este medio de comunicación, que publica generalmente información sobre Siria, Irak, Turquía y Oriente Medio, afirma que recibe miles de visitas al día en esta página de Facebook.

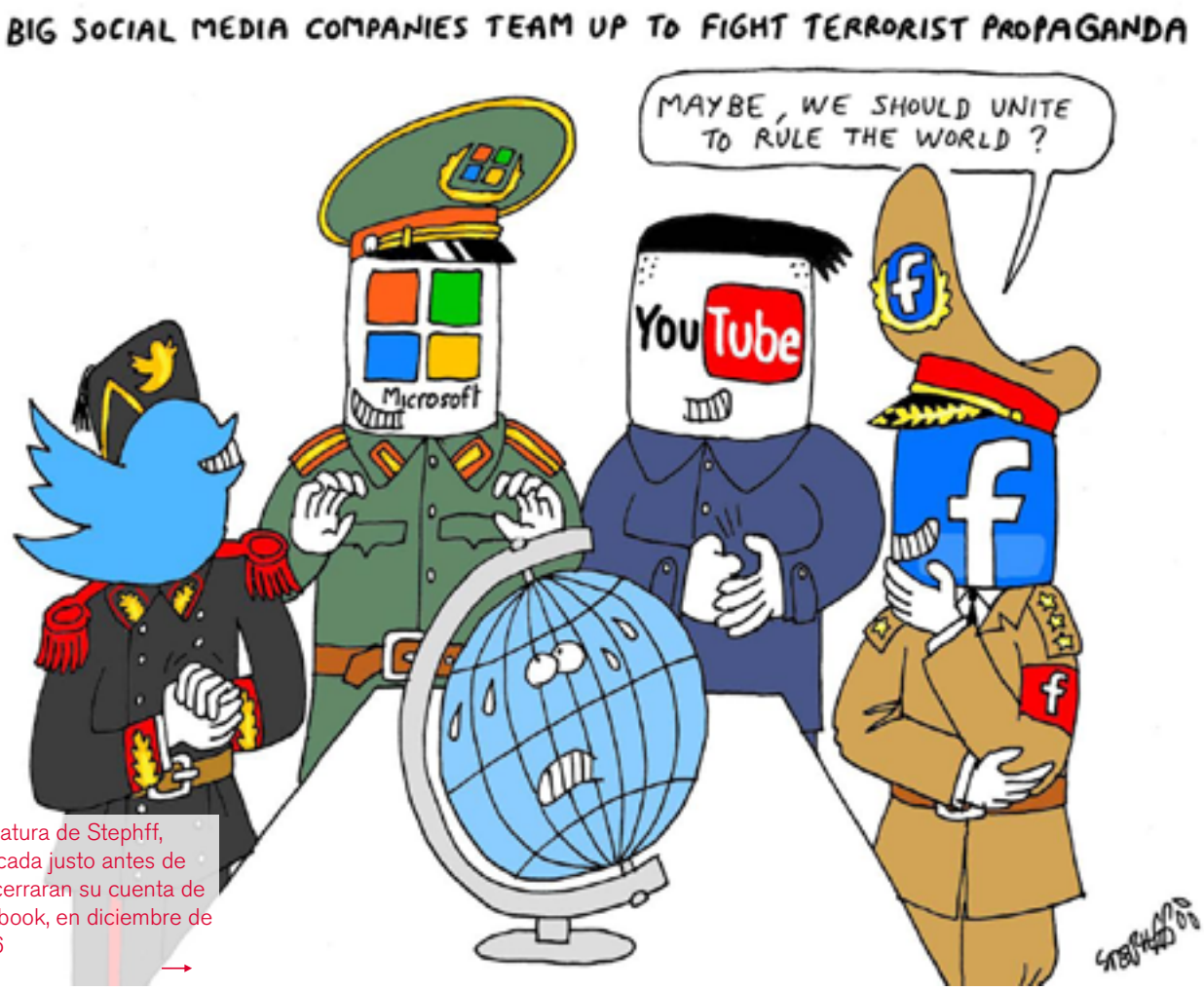
En Tailandia, al caricaturista Stephff, conocido por sus irónicos dibujos, le suprimieron su cuenta Facebook justo después de que publicó en ella una caricatura de las redes sociales, entre ellas Facebook. En junio de 2016 Facebook también suprimió la cuenta de David Thomson, periodista de RFI especializado en yihadismo, debido a la publicación de una foto en la que se entreveía una bandera del grupo Estado Islámico. Asimismo, Facebook suprimió la cuenta del periodista Kevin Sessums y la foto de la niña vietnamita herida por el napalm. Estos son sólo algunos de los numerosos casos de censura arbitraria que se han saldado con la recuperación del contenido o de la cuenta, la supresión de la prohibición de publicación e incluso con mensajes de disculpa: "lo sentimos por este error". "El mensaje fue eliminado por error y recuperado en cuanto pudimos abrir una investigación". "Nuestro equipo trata millones de reportes cada semana y en ocasiones cometemos errores".

> "A VECES NOS EQUIVOCAMOS "

La icónica foto de La niña del Napalm es uno de los casos de censura arbitraria de Facebook

©www.presse-citron.net

←

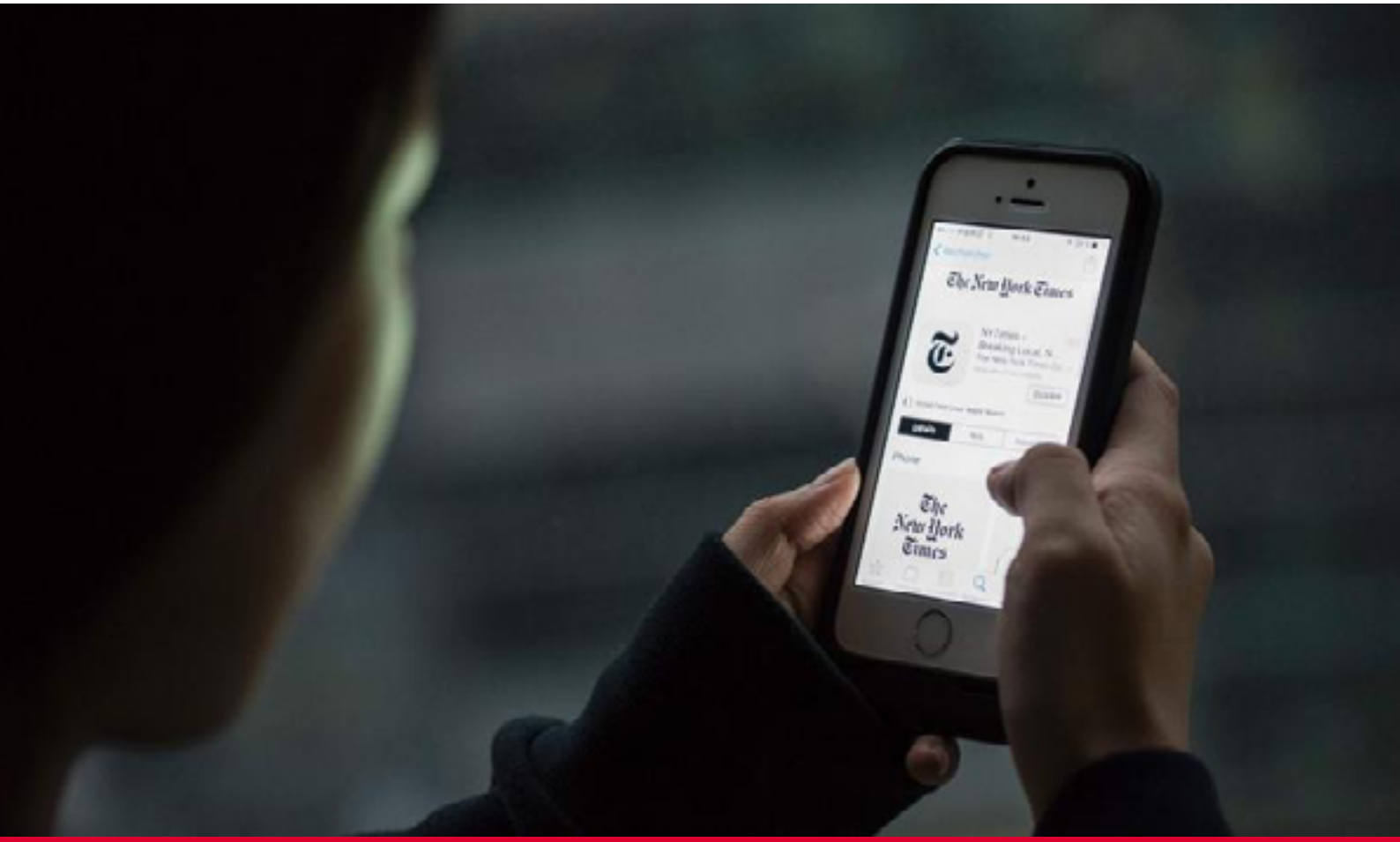


Caricatura de Stephff, publicada justo antes de que cerraran su cuenta de Facebook, en diciembre de 2016

Los otros gigantes de la Web no se quedan atrás. En 2016 Twitter enfrentó acusaciones de censurar a periodistas, en varias ocasiones. Fue en 2014, en Turquía, cuando Twitter decidió utilizar su herramienta de gestión local de contenidos, que prohíbe el acceso a una cuenta o a un tweet desde una conexión turca. En 2016 en Turquía la red social, que afirma en su sitio web que sólo toma en cuenta las solicitudes válidas y definidas correctamente, hizo todo lo posible por aplicar las órdenes dadas por el régimen días después del intento de golpe de Estado del 15 de julio, censurando al menos una veintena de cuentas de periodistas y de medios de comunicación. La mayoría de las cuentas censuradas son de ex reporteros y editores del diario Zaman Amerika. La lista también incluye a un periodista kurdo, @AmedDicleeT, que tiene 186.000 seguidores; al diario kurdo Özgür Gündem (@ozgurgundemweb1), y la cuenta oficial de la agencia de prensa kurda DIHA (@DicleHaberAjans).

En enero de 2017 la firma Apple también generó controversia cuando el NYT dio a conocer que las versiones en inglés y chino de su aplicación habían sido eliminadas de iTunes Store a petición de la Administración del Ciberespacio en China (CAC), el órgano del Partido Comunista Chino que controla Internet. La autocensura en iTunes Store comenzó a observarse poco después de que Apple instaló su primera tienda en China, en 2008. Desde entonces, Apple ha bloqueado numerosas aplicaciones como las del Dalai Lama y las relacionadas con temas tabú en el país. A finales de 2015 un empresario estadounidense observó que cuando iba de Hong Kong a China continental se bloqueaba la aplicación "News". Apple no sólo emplea esta política en China.
En septiembre de 2015 bloqueó la aplicación de Josh Begley, periodista de The Intercept, que registraba todos los ataques de drones realizados por Estados Unidos, y otra sobre la matanza ocurrida en Ferguson, en el estado de Missouri.

Apple había retirado de iTunes Store la aplicación del periódico New York Times en China. ↓



2 EL NEGOCIO DE LA VIGILANCIA: CUESTIONABLE, PERO LUCRATIVO

La vigilancia de la Web y de las telecomunicaciones es una práctica inherente a los "Enemigos de Internet" –los países más represivos del mundo en materia de libertad de información en la Red–, que estos suelen llevar a cabo evocando los "intereses vitales de la Nación". A la cabeza de este grupo se encuentran regímenes autoritarios como China, Irán, Siria e Uzbekistán, que han adquirido y continúan abasteciéndose de tecnología que les permite rastrear el mínimo acto o gesto de periodistas, blogueros e internautas críticos.

En el caso de países democráticos –como Francia, Reino Unido, Estados Unidos, Australia y México (ver abajo)– que recurren a la vigilancia en nombre de la seguridad del país, surge la cuestión de la protección de las fuentes periodísticas.

¿Es posible que las empresas de telecomunicaciones entren de manera ética en el mercado iraní?

En lo que se refiere al control de los internautas, Irán es uno de los mejores ejemplos de país represivo. La ciberpolicía vigila de manera permanente las actividades en línea de los iraníes. En los últimos tres años, en diferentes ciudades del país, más de una centena de internautas, entre ellos numerosos periodistas (profesionales y ciudadanos), han sido citados de forma arbitraria, arrestados y, algunos de ellos, condenados a largas penas. La mayoría de estos periodistas, sean profesionales o ciudadanos, son víctimas de vigilancia y seguimiento efectuados con tecnologías de "vigilancia lícita" (Lawful Interception Management System, LIMS). Sin embargo, bajo el régimen de los Guardianes de la Revolución, incluso las tecnologías conocidas con estas siglas se usan de manera ilegal.

Desde el histórico acuerdo en el sector nuclear, firmado en enero de 2015, un creciente número de empresas del sector de telecomunicaciones (Vodafone, Telecom Italia, AT&T y Nokia) tiene planes de invertir en el país. La compañía francesa Orange comenzó negociaciones para hacerse un lugar en la capital de la firma MCI –líder iraní de la telefonía móvil que se encuentra en manos de los Guardianes de la Revolución–, sin manifestar claramente sus intenciones: "como otros operadores internacionales, el grupo estudia las oportunidades que se presentan en el mercado iraní", señaló la empresa. Richard Marry, uno de los responsables de Vivaction, otra compañía francesa que también está "en fase de descubrimiento del mercado", explica: "hace más de doce meses que vamos a Teherán una vez al mes para conocer el ecosistema de las telecomunicaciones".

"Sabiendo que la tasa media de penetración de los teléfonos móviles es superior a 100% y que uno de cada dos hogares posee un contrato de conexión fija a Internet, no sólo es legítimo querer conocer la manera en que las empresas extranjeras desean establecerse en el país, también es fundamental que estas compañías demuestren transparencia en los acuerdos que firmaron o se disponen a firmar con el régimen", señaló Reza Moïni, responsable del Despacho Irán-Afganistán de Reporteros sin Fronteras*. "Sobre todo, no queremos nuevos casos como los de Nokia-Siemens y Ericsson",* precisó.

En septiembre de 2011, Reporteros sin Fronteras denunció que empresas occidentales cooperaban con el régimen iraní y solicitó que se aplicaran sanciones internacionales si se comprobaba que la tecnología o la infraestructura adquirida por el país permitía al régimen vigilar y reprimir a su población.

Hacking Team y NSO: empresas a la sombra de los Enemigos de Internet

En marzo de 2013, Reporteros sin Fronteras publicó un informe especial sobre la vigilancia en línea en el que daba a conocer por primera vez una lista de empresas "mercenarias de la era digital". En ella se mencionaban los nombres de cinco compañías, ubicadas en Reino Unido, Alemania, Italia, Francia y Estados Unidos, cuyos productos eran usados por países represivos para cometer violaciones a los derechos humanos y la libertad de información. En esta lista aparecía la empresa de Milán Hacking Team, por haber vendido tecnología "ofensiva" de vigilancia a Marruecos y a los Emiratos Árabes Unidos, regímenes que la utilizaron para espiar sitios web informativos y de activistas defensores de los derechos humanos.

En julio de 2015 de nuevo la empresa dio de qué hablar. Piratearon cientos de gigas de sus datos, en los que se encontraba gran cantidad de información sobre sus clientes y la tecnología que les había vendido. Estos documentos confirmaron que países como Francia, Marruecos, Sudán y Tailandia estaban interesados en la tecnología desarrollada por la firma italiana, en particular en su Remote Control System (RCS), concebido únicamente para las agencias gubernamentales, que permite descifrar datos codificados. Gracias a los documentos pirateados también se supo que el gobierno de Ruanda había intentado comprar el RCS en 2012, sin éxito, y que México era el principal cliente de Hacking Team. Las compras efectuadas por este país ascendían a cerca de seis millones de euros y fueron realizadas por diversas entidades gubernamentales: la Secretaría de Gobernación, la Policía Federal, el ejército, la marina, el Centro de Investigación y Seguridad Nacional (Cisen), la Procuraduría General de Justicia, gobiernos regionales, incluso Petróleos Mexicanos (PEMEX), compañía que pertenecía al Estado.

Frente a la insidiosa generalización de la vigilancia en línea efectuada por las autoridades mexicanas, hubo protestas. En marzo de 2016, en representación de un grupo de periodistas, defensores de los derechos humanos y estudiantes, la organización Red en Defensa de los Derechos Digitales (R3D) presentó un amparo contra artículos de la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) relativos a la conservación de metadatos de comunicaciones. El 11 de mayo de 2016, la Segunda Sala de la Suprema Corte de Justicia de la Nación decidió negar el amparo solicitado por R3D y validar la disposición de la LFTR (Federal Telecommunications Act) que permite conservar un registro masivo de metadatos (origen, destino, fecha, hora y duración de todas las comunicaciones), así como conocer la localización geográfica de los dispositivos de los usuarios; para acceder a los metadatos es necesario obtener una autorización judicial previa, pero para el monitoreo de la localización de un usuario no se requiere una autorización judicial. Aunque la coalición R3D apeló esta decisión ante la Corte Interamericana de Derechos Humanos, periodistas, blogueros y ciberactivistas se encuentran en una situación de vulnerabilidad frente a los abusos del gobierno. Las relaciones comerciales de las autoridades mexicanas con el Hacking

©Captura de pantalla de la página de Hacking Team ↓

Podrían contestarme, interrogándose sobre este tema, que estas personas se defendieron señalando la necesidad de luchar contra el terrorismo y recordando que responden a las leyes de los países en los que se han implantado, como hizo Hacking Team en Italia. «*Esto no basta, pues sus tecnologías siguen siendo utilizadas por regímenes autoritarios, enemigos de Internet, para vigilar y encarcelar a periodistas*", explicó Christophe Deloire.

"Al constatar las relaciones comerciales que existen entre múltiples organismos gubernamentales mexicanos y uno de los principales exportadores de tecnología de vigilancia, nos preguntamos qué margen se deja a los periodistas para investigar de manera independiente y para proteger a sus fuentes", señaló Emmanuel Colombié, responsable del Despacho América Latina de RSF. *"La opacidad de las autoridades respecto al uso que planean dar a esta tecnología, hace que esta preocupación crezca. Deben darse garantías para prohibir que sea usada de forma sistemática contra todos los actores de la información, profesionales de los medios de comunicación, blogueros y defensores de los derechos humanos",* agregó.

EL MALWARE PODÍA TENER ACCESO A TODA SU INFORMACIÓN PERSONAL, VER SUS FOTOS Y ARCHIVOS, LOS CONTENIDOS DE SUS LLAMADAS, LEER SUS MENSAJES DE SMS, CORREOS ELECTRÓNICOS, CONVERSACIONES EN WHATSAPP, SKYPE E INCLUSO TELEGRAM.

Lo que le ocurrió al periodista de investigación mexicano Rafael Cabrera, caso en el que estuvo implicada la empresa israelí NSO Group, muestra el abuso en la vigilancia cometido por las autoridades mexicanas. En agosto de 2016 Citizen Lab y Look out informaron que existía un programa espía que permitía controlar por completo los iPhone aprovechando sus fallas de seguridad (que después fueron corregidas): "Pegasus". El software malicioso (malware) se instalaba en el teléfono móvil de la víctima de la siguiente manera: la persona recibía un mensaje SMS en su teléfono (en apariencia confiable) seguido de un link; al abrirlo, su teléfono quedaba infectado y el malware podía tener acceso a toda su información personal (contactos), ver sus fotos y archivos, los contenidos de sus llamadas, leer sus mensajes de SMS, correos electrónicos, conversaciones en WhatsApp, Skype e incluso Telegram (sistema de mensajería que no obstante es conocido por su seguridad). También podía usar a distancia la cámara del iPhone, escuchar sus conversaciones encendiendo el micrófono y saber en todo momento dónde se encontraba su propietario, activando el GPS.

Rafael Cabrera, periodista del sitio web informativo Aristeguinoticias.com, fue víctima de Pegasus en agosto de 2016 después de haber participado en una investigación sobre la “Casa Blanca” del presidente Enrique Peña Nieto. Este reportaje sacó a la luz un escándalo de corrupción en el que estaba implicada la familia del presidente. El periodista recibió mensajes sospechosos supuestamente del canal UNO TV en los que le “informaban” que la presidencia demandaría por difamación a quienes publicaron el reportaje de la Casa Blanca y que podría encarcelar a los periodistas que participaron en la investigación.

Rafael Cabrera, periodista del sitio web informativo Aristegui Notícias , fue víctima de Pegasus. →

Según el NYT, el gobierno mexicano pagó 15 millones de dólares a NSO por tres proyectos que no especificó. NSO se defendió afirmando que los programas que vendía sólo eran usados para la vigilancia legal. Sin embargo, cuando se hicieron estas revelaciones, Citizen Lab dio a conocer que Ahmed Mansoor, bloguero emiratí, administrador del foro de debate democrático Al-Hewa, sufrió un ataque similar. El 10 y 11 de agosto de 2016, el bloguero recibió dos veces un SMS en su iPhone 6, en el que le decían que diera clic en un enlace para saber más sobre los ataques cometidos por el régimen de los Emiratos Árabes Unidos. Este SMS fue analizado por el Citizen Lab, lo que permitió encontrar la huella de NSO y de su programa Pegasus.

Contactada por RSF, la NSO declaro que : «NSO contribuye a volver el mundo más seguro proporcionando a los organismos gubernamentales autorizados tecnologías que les ayuden a combatir el terror y la criminalidad. Los clientes pueden utilizar nuestros productos exclusivamente para la investigación y la prevención del crimen y el terror. El uso ético y legal de estos productos por parte de los clientes es de importancia capital para la empresa. En caso de presunta violación del contrato, la empresa tomará las medidas adecuadas con el cliente en cuestión”, afirmaciones que RSF no estuvo en medida de verificar.

3 REGULACIONES INTERNACIONALES FUNCIONAN O BLOQUEADAS POR LOS LOBBIES

En su 32ª sesión, realizada del 13 de junio a 1 de julio de 2016, el Consejo de Derechos Humanos de la Organización de las Naciones Unidas (ONU) adoptó una resolución sobre la promoción, la protección y el disfrute de los derechos humanos en Internet. Ésta afirma una vez más que deben protegerse en línea los mismos derechos de los que gozan las personas fuera de Internet, en particular el de la libertad de expresión, que debe ejercerse independientemente de las fronteras y del medio empleado, conforme a los artículos 19 de la Declaración Universal de los Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos. Además, la resolución exhorta a todos los Estados a abordar las preocupaciones de seguridad en Internet respetando sus compromisos internacionales relativos a los derechos humanos, para garantizar la protección de la libertad de expresión y de asociación, el derecho a la vida privada, entre otros los derechos humanos en línea, a través de instituciones nacionales democráticas y transparentes, basadas en los principios de la ley, de manera que se asegure la libertad y la seguridad en Internet.

LAS RESOLUCIONES DEL CONSEJO SON TEXTOS NO VINCULANTES Y SON INEFICACES CUANDO SE TRATA DE FRENAR A LOS ESTADOS MÁS REPRESIVOS EN MATERIA DE LIBERTADES INDIVIDUALES EN LÍNEA.

Otra resolución del Consejo de Derechos Humanos de la ONU adoptada en septiembre de 2016 subraya que en la era digital los periodistas deben poder contar con herramientas de encriptamiento y que protejan su anonimato para poder practicar libremente su profesión y ejercer sus derechos humanos –en particular el derecho a la libertad de expresión y el derecho al respeto de la vida privada–, asegurar sus comunicaciones y proteger la confidencialidad de sus fuentes. Asimismo, pide a los Estados que eviten la injerencia usando tales tecnologías a través de la imposición de restricciones, y cumplan así sus compromisos respecto a la legislación internacional de los derechos humanos. Sin embargo, las resoluciones del Consejo son textos no vinculantes y son ineficaces cuando se trata de frenar a los Estados más represivos en materia de libertades individuales en línea.

Desde las revelaciones de Edward Snowden y el fin de la hegemonía estadounidense en la gobernanza de la Web, los Enemigos de Internet ejercen presión para tener un rol mayor en la regulación de las redes, sobre todo a través de agencias de la ONU, como la Unión Internacional de Telecomunicaciones (UIT), la Organización de Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco) y la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD por sus siglas en inglés). Todas ellas han hecho declaraciones en defensa de las libertades fundamentales en línea y la gobernanza de Internet. Después de la Declaración de Principios de la Cumbre de Ginebra, realizada en 2003, la Cumbre Mundial sobre la Sociedad de la Información constituye una de las principales plataformas multilaterales de gobernanza de Internet, en la que aún no se ha presentado ningún texto vinculante a fin de impedir que los regímenes autoritarios censuren y vigilen masivamente a su población.

"*Cada vez más se corre el riesgo de que la lucha en torno a la cuestión estratégica de la gobernanza de la Web dé lugar a la oficialización de un Internet fragmentado y censurado*", señaló Benjamin Ismaïl, responsable del Despacho Asia de RSF. "*Si cada país se pone a reclamar su soberanía en Internet, se creará un sistema en el que los regímenes autoritarios tendrán toda la legitimidad para restringir la libertad de expresión y el derecho a informar en línea. Para evitar que esto suceda, es vital que se establezcan mecanismos internacionales vinculantes, a fin de garantizar la existencia de un Internet libre y mundial. Hoy más que nunca esta garantía pasa por un estricto control de las empresas de la Red y de las compañías que exportan tecnologías de vigilancia masiva*", explicó.

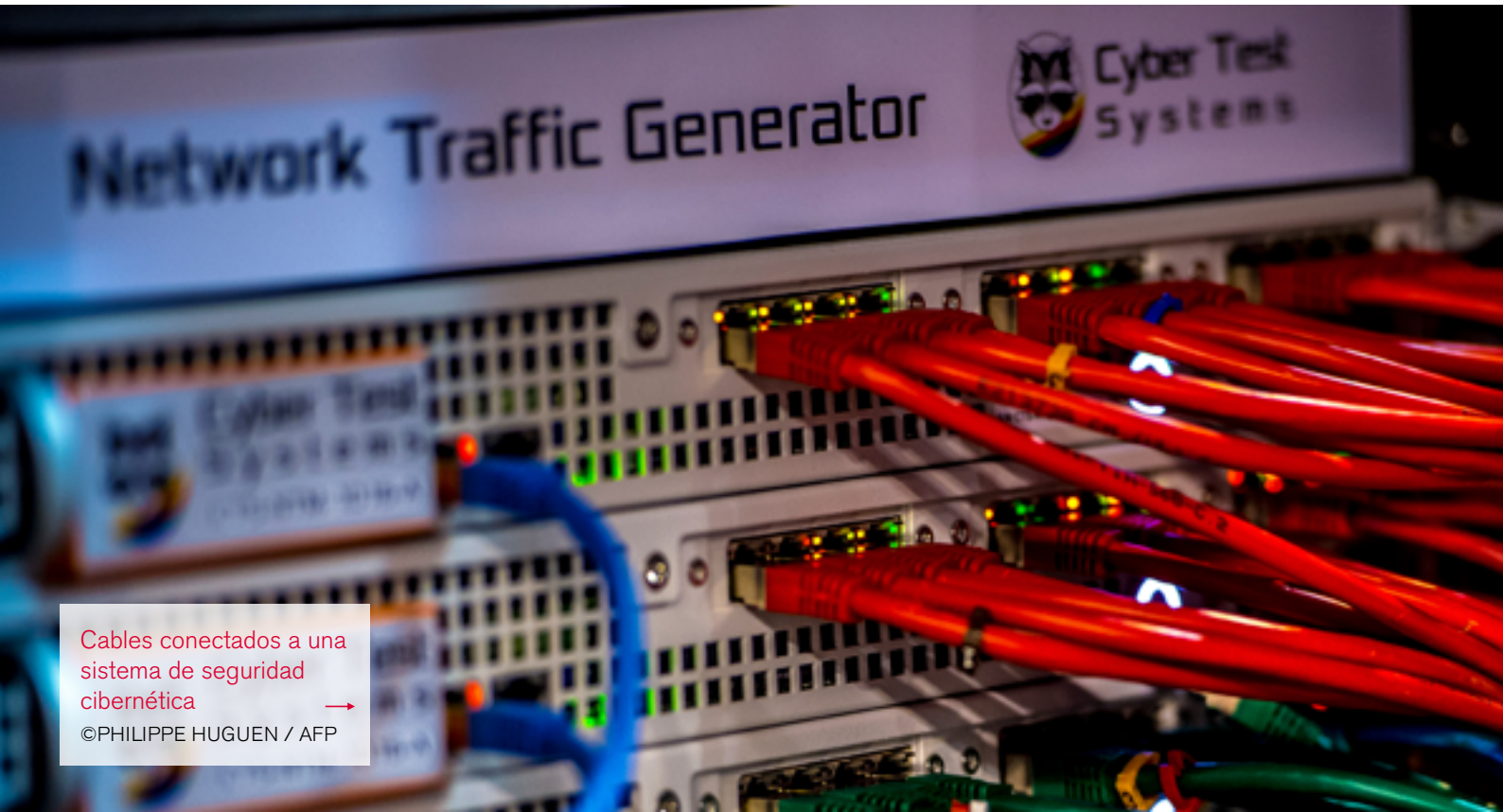
Exanalista de seguridad de la NSA que denunció el espionaje electrónico masivo, Edward Snowden.
©FREDERICK FLORIN / AFP ↓

Desde 2014 RSF ha pedido al Consejo de Derechos Humanos de la ONU que se cree un convenio internacional sobre la responsabilidad de las empresas en materia de derechos humanos, para imponer a los Estados un estricto control de la exportación de tecnologías de vigilancia y que se establezca un recurso para los individuos que hayan sido víctimas de la vigilancia y padecido las consecuencias de ésta (arrestos, encarcelamientos, violencia física, tortura).

El 28 de noviembre de 2014 RSF, Privacy International, Digitale Gesellshaft, la Federación Internacional de Derechos Humanos (FIDH) y Human Rights Watch celebraron el «primer paso de Europa a favor de un mayor control de las tecnologías de vigilancia», al añadir en la lista de tecnologías de doble uso (dual use technology) a las tecnologías de vigilancia de la Red. El 2 de diciembre de 2014 los miembros de la Coalición contra las Exportaciones de Vigilancia Ilegal (Coalition Against Unlawful Surveillance Exports, CAUSE), RSF, Amnistía Internacional, Digitale Gesellschaft, la FIDH, Human Rights Watch, Open Technology Institute y Privacy International enviaron una carta abierta a los Estados participantes en la Asamblea Plenaria del Arreglo de Wassenaar sobre la reglamentación de Exportaciones de Armas Convencionales y Bienes y Tecnología de Doble Uso –tratado que reúne a 41 países, la mayoría de ellos de la Unión Europea (UE)– para pedirles que tomaran medidas contra la alarmante proliferación de las tecnologías de vigilancia accesibles a los países represivos, conocidos por cometer constantemente violaciones a los derechos humanos.

A TRES AÑOS DE ESTOS LLAMADOS A FAVOR DE UN CONTROL EFICAZ DE LAS EMPRESAS PRIVADAS, LA UE PARECE HABER DADO MARCHA ATRÁS

Bajo la presión del lobby de la industria de la tecnología digital, la regulación de las tecnologías de vigilancia se encuentra en un punto muerto. Los grupos de presión –en particular el que representa la asociación DigitalEuropa, cuya instancia dirigente está conformada por directivos de empresas como Nokia, Siemens, AMETIC, IBM, ANITEC, Cisco y Microsoft, con el apoyo de un grupo de diplomáticos de nueve países (Austria, Finlandia, Francia, Alemania, Polonia, Eslovenia, España, Suecia y el Reino Unido)– lograron que se hicieran modificaciones a la propuesta de "regulación del Parlamento Europeo y del Consejo" para amputar la lista inicial de tecnologías que debían encontrarse bajo control –como cierto equipo para interceptar telecomunicaciones, programas de intrusión, centros de vigilancia y sistemas de conservación de datos.



Cables conectados a una sistema de seguridad cibernética →
©PHILIPPE HUGUEN / AFP

La última propuesta ya no contiene los controles previstos inicialmente sobre los equipos biométricos, los sistemas de geolocalización o las tecnologías DPI (Deep Packet Inspection), que permiten interceptar e inspeccionar los paquetes de datos que circulan en Internet. En un contexto de vigilancia, el uso de productos DPI permite tener acceso al contenido de correos electrónicos, a conversaciones instantáneas y comunicaciones por VoIP (Voice Over Internet Protocol, transmisión de voz a través de Internet), así como descubrir si una comunicación se encuentra encriptada. La propuesta no menciona la obligación de los Estados europeos de informar a la población sobre las empresas a las que autorizan exportar esta tecnología.

En las Naciones Unidas, la UE, así como en la mayoría de las legislaciones nacionales, el marco jurídico relativo a la vigilancia de Internet, la protección de datos y la exportación de equipo de vigilancia informática sigue estando incompleto y continúa siendo insuficiente respecto a las normas y los estándares internacionales de protección de los derechos humanos. Por lo que sigue siendo primordial la adopción de un marco jurídico que proteja las libertades en Internet, tanto por la cuestión general de la vigilancia de Internet, como por el problema particular de las empresas exportadoras de equipo de vigilancia.

4 LAS RECOMENDACIONES DE RSF PARA LUCHAR CONTRA LA CIBERCENSURA

Con ocasión de este Día Mundial contra la Cibercensura, RSF pide:

A las empresas:

- Que sistematicen y mejoren los informes de transparencia; que hagan públicas las solicitudes judiciales de los gobiernos que les pidan suprimir contenidos o cuentas de los usuarios.
- Que respeten la Declaración Universal de los Derechos Humanos y los convenios de las Naciones Unidas relativos a los derechos humanos.
- Que respeten los Principios Rectores sobre las empresas y los derechos humanos de la ONU y establezcan compromisos precisos para que se sigan.
- Que adopten cartas éticas y mecanismos eficaces de "seguimiento" de las tecnologías que exportan.
- Que se prohíban la exportación de tecnología de vigilancia a países no democráticos o represivos, y que cumplan con su deber de vigilancia para que puedan identificar los riesgos y prevenir ataques graves a los derechos humanos, las libertades fundamentales y la seguridad de las personas.
- Que apliquen los "Principios de contratación responsable" elaborados por el Representante Especial del Secretario General de la ONU para la cuestión de los Derechos Humanos y las Empresas Transnacionales y otras Empresas, John Ruggie, que consideran que las empresas son en parte responsables de las violaciones a los derechos humanos que puedan cometerse con sus tecnologías.

A los Estados :

- Que incluyan en los derechos fundamentales del país: el libre acceso a Internet y el respeto de las libertades digitales.

- Que adopten leyes que garanticen las libertades digitales, en particular, que contemplen el respeto a la vida privada y a los datos personales, para protegerlos de la intrusión de las fuerzas del orden o de los servicios de inteligencia, y que creen mecanismos de recurso adecuados.

- Que se aseguren de que las medidas de vigilancia de las comunicaciones respetan como es debido los principios de legalidad, necesidad y proporcionalidad, conforme al artículo 19 del Pacto Internacional de Derechos Civiles y Políticos

- Que procuren que exista una mayor transparencia en las solicitudes de vigilancia que hacen a las empresas, especificando su número, sus bases legales y objetivos.

- Que alineen sus políticas a las de los Estados que controlan mejor la exportación de tecnología y sancionen a las empresas que hayan colaborado con regímenes autoritarios.

A la Unión Europea

- Que incluya en la Carta de los Derechos Fundamentales de la UE: el libre acceso a Internet y las libertades digitales.

- En las relaciones entre miembros de la UE y con terceros Estados, así como con las instancias internacionales, en particular con la Organización Mundial del Comercio (OMC), que considere los mecanismos de vigilancia de Internet como mecanismos proteccionistas y barreras al intercambio, y que los combata como tales.

- Que garantice la armonización e uniformización de las sanciones y los procesos encaminados a regular la vigilancia y el control de tecnologías de vigilancia.

A la Organización de Naciones Unidas :

- Que refuerce la misión del grupo de trabajo sobre la cuestión de los “Derechos humanos y las empresas transnacionales”, habilitándolo para recibir denuncias individuales e investigar casos individuales de violaciones a los derechos humanos relacionados con las empresas.

- Que reflexione si es posible elaborar un convenio internacional sobre la exportación de tecnologías de vigilancia de internet que permita controlar estas tecnologías y prohibir el acceso a ellas si existe un riesgo sustancial de que este equipo sirva para cometer o facilitar violaciones a los derechos humanos.

5 PERIODISTA, PROTEGE TUS DATOS Y TUS COMUNICACIONES

Para luchar eficazmente contra la vigilancia y la censura, los periodistas –profesionales o ciudadanos– pueden usar programas desarrollados por organizaciones de la sociedad civil y emprender acciones concretas gracias a guías de ciberseguridad disponibles en línea. En 2015 RSF actualizó su Guía práctica de seguridad de los periodistas, que incluye numerosos consejos prácticos en materia de ciberseguridad.

Los consejos que presentamos a continuación pueden ser válidos tanto para un ordenador como para un teléfono inteligente, sin embargo, se trata de un resumen, no son exhaustivos. Reporteros sin Fronteras organiza regularmente sesiones de formación en ciberseguridad y propone tutoriales gratuitos.

Atención: siempre investiga más sobre las herramientas y las técnicas que vas a utilizar. La tecnología avanza rápidamente y los consejos que te proporcionamos actualmente pueden no tener la misma utilidad mañana.

Periodistas siguen el congreso nacional del partido comunista chino
©AFP PHOTO / Greg BAKER

Comportamiento general en línea:

Antes de pensar en incrementar la seguridad de tu ordenador o de instalar programas para codificar las comunicaciones o los datos, es importante que adoptes una buena higiene digital. Te damos algunos consejos (de sentido común) que te ayudarán a evitar que tu cuenta de correo o tu ordenador sean pirateados.

Evita las miradas indiscretas:

- Evita trabajar de espaldas a una ventana.
- Cuando viajes en tren o en avión, coloca un filtro de privacidad en la pantalla de tu ordenador. Este protector es una hoja transparente que, una vez colocada, permite que sólo la persona ubicada frente al ordenador (tú) vea perfectamente la pantalla e impide la visión lateral (que las personas ubicadas a los lados puedan verla).
- En la medida de lo posible, evita separarte de tu equipo cuando te desplaces. Esto permite evitar que una persona malintencionada pueda obtener archivos de tu ordenador o introducir en él un Caballo de Troya.
- Todos los sistemas operativos (Windows, Mac os y Linux) permiten proteger tu sesión de trabajo con una contraseña. Utilízala siempre.
- No descargues archivos ni des clic en enlaces que recibas de remitentes desconocidos.
- Verifica cuidadosamente la dirección de correo electrónico o la cuenta Twitter de quienes comparten un enlace contigo. Si tienes dudas, verifica la identidad del remitente a través de otros contactos o de un motor de búsqueda.
- Si un archivo o el remitente te parecen sospechosos, contacta a expertos para que te ayuden. Citizen Lab es un organismo que analiza los virus enviados a disidentes o activistas y les ayuda a protegerse mejor.

Además de tomar estas medidas, puedes instalar los siguientes programas y activar las funciones de protección de tu dispositivo:

- Utiliza un antivirus y un anti malware (como Malwarebytes).
- Activa tu firewall (cortafuegos).
- Actualiza constantemente tu sistema operativo (Windows, Mac OSX, etc.).

Rastros digitales:

Si trabajas en un cibercafé o en un ordenador que no es tuyo, procura no dejar rastro cuando hayas terminado tu trabajo:

- Si consultaste tu mail, tu cuenta de Facebook o Twitter, desconéctate.
- Borra el historial de navegación. Éste contiene mucha información que puede permitir a un experto acceder a tus cuentas en línea.
- Cuando trabajes en un ordenador público nunca guardes tu contraseña en el navegador. Si lo hiciste por error, bórralo de la memoria del navegador cuando hayas terminado tu trabajo.
- Borra los campos de formulario.
- Suprime las cookies.

La limpieza de estos datos se realiza de manera diferente en cada navegador. Un buen medio de evitar equivocaciones es usar la "navegación privada" de Firefox o de Chrome.

Mensajería y acceso a los servicios en línea:

La mayoría de los servicios en línea (Twitter, Facebook, WordPress, Tumblr, Skype, etc.) permiten recuperar una contraseña perdida enviando otra al buzón de correo electrónico. Por ello es fundamental que protejas tu buzón de correo electrónico lo mejor posible. Si éste se encuentra en riesgo, es muy probable que toda tu identidad digital lo esté también.

Gmail, el servicio de mail de Google, ofrece una medida de seguridad suplementaria: la «verificación en dos pasos». Este servicio permite proteger tu cuenta de correo electrónico con:

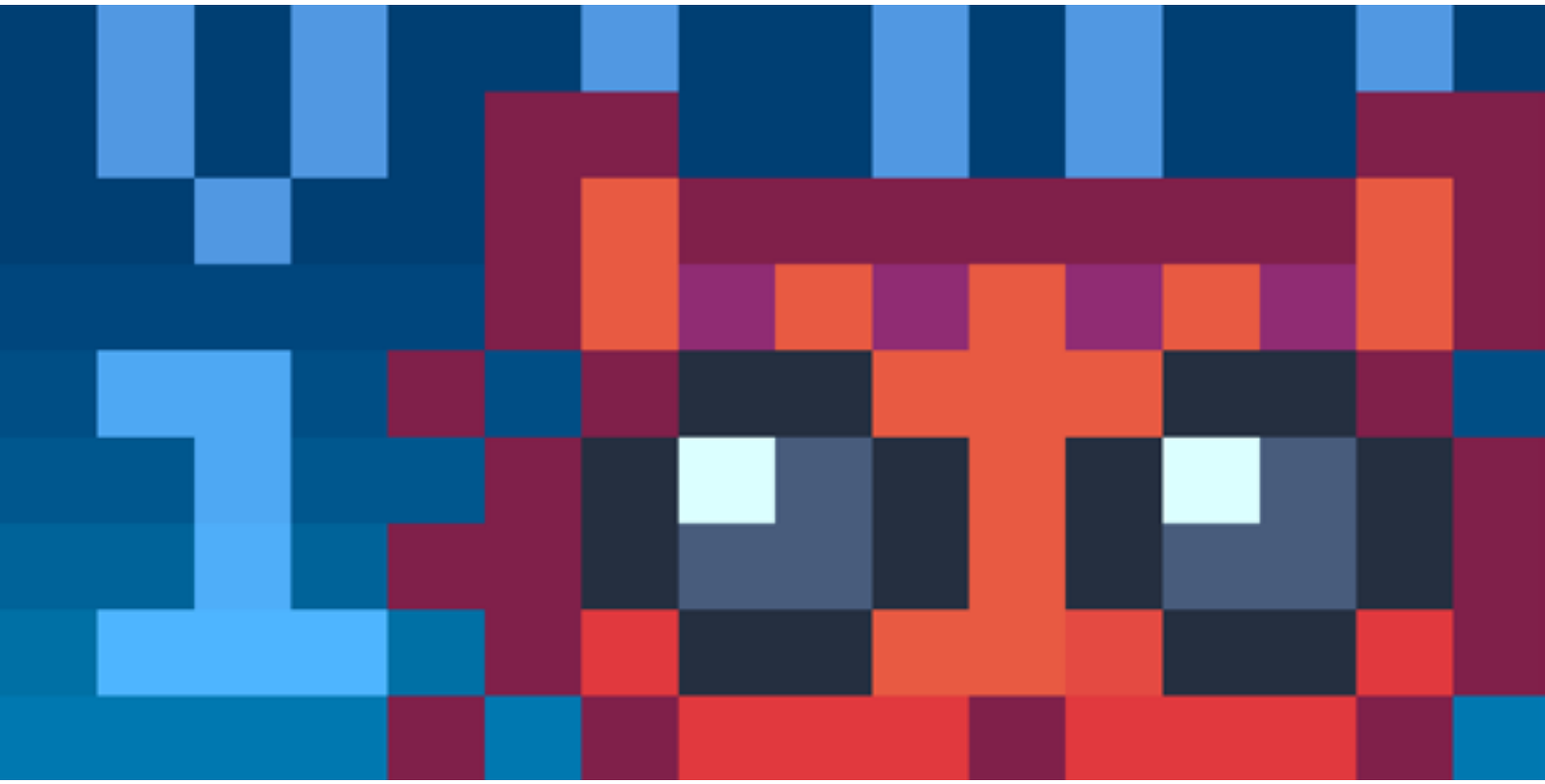
1. un nombre de usuario
2. una contraseña
3. un código que recibes en tu teléfono móvil cada vez que te conectas a tu bandeja de entrada.

De esta manera, sin el teléfono móvil no es posible acceder a tus mails.

Cuando te conectes a tu correo de Gmail, no olvides dar clic en el enlace «detalles», que aparece en la parte inferior de la página. Éste abre una ventana que muestra todos los accesos recientes a tu buzón. Así, puedes detectar si existe una actividad anómala.

También deberías encriptar tus mails. Existen herramientas de codificación muy fáciles de utilizar. Asimismo, puedes recomendar a tus fuentes que las usen para conversar con ellos de manera cifrada:

- Cryptocat, una extensión que se instala en tu ordenador, codifica las conversaciones instantáneas de principio a fin y las destruye después.
- Los sitios web Privnote y Zerobin permiten crear URL (Uniform Resource Locator) que conducen a mensajes cifrados que pueden autodestruirse después de ser leídos.
- ¿Quieres hacer una llamada a tus fuentes a través de Internet? No hay problema, pero utiliza Jitsi Meet, el «Skype libre».



Logo « Cryptocat » una extensión que ↑
se instala en tu ordenador y codifica
las conversaciones instantáneas
©Cryptocat

Frases de contraseña:

La extensión de una contraseña es el factor principal de su seguridad. De allí que ya no se hable de contraseñas a evitar, sino de emplear “frases de contraseña” (contraseña larga, una frase que entre los caracteres alfanuméricos incluye espacios y caracteres especiales), que son el único método para resistir un “ataque de fuerza bruta”. Cada vez que crees una frase de contraseña:

- Crea una frase en la que incluyas números, letras minúsculas y mayúsculas, para obtener una secuencia de caracteres relativamente compleja y, al mismo tiempo, más fácil de memorizar que una contraseña corta pero abstracta (números más caracteres especiales).
- Utiliza una frase de contraseña diferente para cada servicio en línea.
- Usa un programa para gestionar tus contraseñas. Por ejemplo LastPass, que permite registrar todas tus frases de contraseña y está disponible en forma de extensión de Firefox, Chrome y Safari.

Huellas en las redes sociales:

Facebook y Twitter son herramientas muy eficaces para comunicarse. Sin embargo, debes controlar la información que das a conocer en público. Estos tutoriales te ayudarán a gestionar mejor tu presencia en línea:

- Verifica tu presencia en Internet con “namechecker”.
- Asegura tu cuenta de Twitter.
- Controla tu información privada en Facebook cuando compartes un contenido.

Vuelve segura tu navegación:

Agrega las siguientes funcionalidades a Firefox y Chrome usando plugins:

- https everywhere: para verificar en cada sitio web si existe una versión https (cifrada) y evitar el phishing (usurpación de identidad).
- No script: para controlar los scripts javascript lanzados en los sitios web que visitas.
- Privacy Badger: para bloquear los rastreadores (trackers) utilizados por los sitios web.
- Certificate Patrol: para verificar los certificados presentados por los sitios en “https”.
- Instala una VPN (red virtual privada) para codificar tus conexiones a Internet.
- Instala el navegador “Tor Browser”, que permite navegar de manera anónima.

Telefonía móvil:

- Crea y usa un sistema codificado para comunicarte con tus fuentes y otros contactos. Por ejemplo, «Bipea» a tus contactos (al llamar, deja sonar una o dos veces el teléfono y cuelga enseguida, para indicar a tu contacto que llegaste bien a un lugar o que todo va bien).

- No emplees los verdaderos nombres de tus contactos en tu agenda telefónica, regístralos con números o seudónimos. Así, si las fuerzas de seguridad te quitan el teléfono o la tarjeta SIM, no podrán conocer toda tu red de contactos.

- En las manifestaciones, lleva tarjetas SIM de prepago si crees que podrían confiscarte el teléfono. Es muy importante que lleves un teléfono móvil que funcione. Si tienes que deshacerte de tu tarjeta SIM, intenta destruirla físicamente.

- Si es posible, bloquea tu teléfono con una contraseña. Todas las tarjetas SIM tienen un código de acceso. Cámbialo y protege tu tarjeta SIM con este código. Cada vez que quieras utilizar tu teléfono te pedirá esa contraseña (tu código de acceso).

- Si crees que una manifestación puede concluir con una fuerte represión de las fuerzas de seguridad, activa el modo avión de tu teléfono. Aunque no podrás hacer ni recibir llamadas, podrás tomar fotos y videos, y después subirlos a Internet. Esta táctica es útil si las fuerzas de seguridad toman como blanco a las personas que llevaban teléfono móvil durante la manifestación, pues después, el gobierno puede pedir registros de las llamadas, los SMS o los datos telefónicos de quienes se encontraban en el lugar en ese momento, con el fin realizar detenciones masivas.

- Desactiva las funciones de geolocalización de tus aplicaciones, a menos que uses esta función como activista, para etiquetar (poner tags) a ciertos medios durante el acontecimiento. Si utilizas tu teléfono móvil para difundir un video en streaming live, desactiva la función de GPS y de geolocalización.

- Si tu teléfono funciona con el sistema Android, puedes usar numerosas herramientas para codificar tu navegación en Internet, chats, SMS y mensajes vocales con las herramientas creadas por Guardian Project y Whispersys. Si usas tu teléfono móvil para acceder a la Web utiliza el HTTPS en la medida de lo posible.

Luchar contra la censura:

Algunas de las herramientas que presentamos anteriormente permiten evadir la censura impuesta por las autoridades (volver anónima la conexión, VPN, etc.). Si deseas conocer más:

- Consulta el sitio web "Collateral Freedom" de Reporteros sin Fronteras. Para evadir la censura tecnológica impuesta por Estados que no respetan los derechos humanos, RSF empleó un original dispositivo basado en procedimientos técnicos de mirroring, que consiste en duplicar los sitios censurados y albergar las copias virtuales en servidores de gigantes de la Web, como Amazon, Microsoft o Google.

- Visita el sitio web "Circumvention Central", creado por GreatFire (organización que concibió la iniciativa Collateral Freedom) para saber más sobre las VPN.

- Consulta el sitio web "Security in-a-box» de Tactical Tech y los artículos de la Electronic Frontier Foundation para evadir mejor la censura en línea y preservar tu anonimato.

Lanzado en 2011, la página «Collateral Freedom» permite hacer accesibles sitios web que han sido censurados →

©RSF

REPORTEROS SIN FRONTERAS promueve y defiende la libertad de informar y de ser informado en todo el mundo. La organización con sede en París posee diez oficinas internacionales (Berlin, Ginebra, Madrid, New York, Túnez, Estocolmo, Turin, Viena, Washington DC, Rio de Janeiro), así como una red de 150 corresponsales repartidos en los cinco continentes.

Secretario general: CHRISTOPHE DELOIRE
Jefa de redacción de RSF: VIRGINIE DANGLES

SECRETARÍA INTERNATIONAL
CS 90247
75083 Paris Cedex 02
Tel. +33 1 44 83 84 84
Web : www.rsf.org

REPORTEROS SIN FRONTERAS
POR LA LIBERTAD DE INFORMACIÓN