Facultad de Ciencias Sociales y de la Comunicación

Trabajo de Fin de Grado

Grado en Periodismo

Los susurros encriptados del siglo XXI:
la *deep* web como herramienta para el periodismo de investigación

Alumna: Carla Rivero Pérez

Tutor: Samuel Toledano

Curso académico

2019 - 2020

Resumen

El periodismo de investigación en plena era del *big data* transita por terrenos desconocidos y novedosos para los cuales se ha de transformar rápidamente. El contacto y la comunicación con las fuentes requiere por parte del periodista de una garantía de protección a las mismas. Es entonces cuando se puede establecer una filtración segura. Por ello, el uso de la *deep* web, el espacio no indexado que existe en internet, a través de la red Tor es indispensable para fomentar las herramientas de privacidad tanto para ocultar el rastro de lo buscado, lo encontrado, al usuario y con quien pretende contactar el que lo hace. Plataformas como SecureDrop, aplicaciones al estilo de Signal, o la utilización de la PGP serán de uso obligatorio en un futuro no muy próximo en cualquier parte del mundo. La señal titilante estalló en una cascada el año 2010 cuando la plataforma Wikileaks publicó el Caso *Cablegate*, lo cual supuso la primera gran coordinación entre varios medios internacionales. A partir de entonces, la concreción de la vigilancia masiva y el uso masivo de datos se ha demostrado en otras investigaciones como el Caso Snowden y los Papeles de Panamá. Por lo tanto, el periodista ha de estar preparado para estos retos.

Palabras claves

Deep web, periodismo de investigación, privacidad, seguridad, filtración, fuente, encriptación, Proyecto Tor, Tor Browser, SecureDrop.

Abstract

Investigative journalism in the middle of the big data era travels through unknown and novel terrain for which it must rapidly transform. Contact and communication with sources requires the journalist to guarantee their protection. This is when a safe filtration can be established. Therefore, the use of the deep web, the non-indexed space that exists on the internet, through the Tor network is essential to promote privacy tools both to hide the trace of what is sought, what is found, the user and with whom intends to contact the one who does it. Platforms such as SecureDrop, Signal applications, or the use of PGP will be a must in the near future in any part of the world. The flickering signal exploded in a waterfall in 2010 when Wikileaks published the Cablegate Case, which was the first major coordination between various international media. Since then, the realization of mass surveillance and the massive use of data has been demonstrated in other investigations as the Snowden Case and the Panama Papers. For that reason, journalists must be prepared for these challenges.

Keywords

Deep web, investigative journalism, privacity, security, filtration, source, whistleblower, encryption, Tor Proyect, Tor Browser, SecureDrop.

Los susurros encriptados del siglo XXI

Fuente: Pixabay

Carla Rivero Pérez

A mamá y a papá, por creer en mí.

A Andrea y a Pablo, por convertir la excepción en normalidad.

A mi familia y amistades, en la lejanía y en la proximidad de las escapadas, en los cafés y en las reuniones, por las charlas y los consejos, los silencios y los llantos de risa, gracias por darme las fuerzas para resistir.

A mis niñas, por haberme dejado construir un hogar al que pertenecer.

A Vicky y a Guille, profesoras del IES Cairasco de Figueroa, que con tanto ahínco cuidaron y fomentaron la biblioteca que me dejó encontrar *Nada y así sea* de Oriana Fallaci. Por su paciencia y por creer que merecía la pena aguantar durante el recreo a que eligiese libro, por enseñar que la cultura era también cosa nuestra.

A Samuel Toledano, por decidir apostar por nosotras con gestos como programar el documental *Citizenfour* en el Aguere de La Laguna e invitarnos a ir. Ahí surgió la idea.

ÍNDICE

Introducción……6

Los inicios……8
De camino a la triple W……..9
Los océanos como fuente de vida, y conexión……..10
Un secreto compartido……...12

La ruta de la cebolla……..17
20.000 leguas de viaje submarino……..18
Sumergidos en la *deep* web……...….21
En busca de una SecureDrop……..…...24

El periodismo de investigación (digital)……26
Los cables de Wikileaks…….....28
Snowden vs. NSA……....30
Los Papeles de Panamá, el periodismo es colectivo……33

Una realidad, y varias recomendaciones……...36

Anexo……....40

Hay miles de ojos a la espera de saber qué va a escribir en el teclado de su dispositivo. Hay técnicas para descubrir, según la coordinación de sus dedos, cuáles son las palabras que utiliza para realizar una búsqueda y, cómo no, también hay miles de millones de intereses, que registran, guardan y catalogan la información que dejamos en las telarañas de la red.

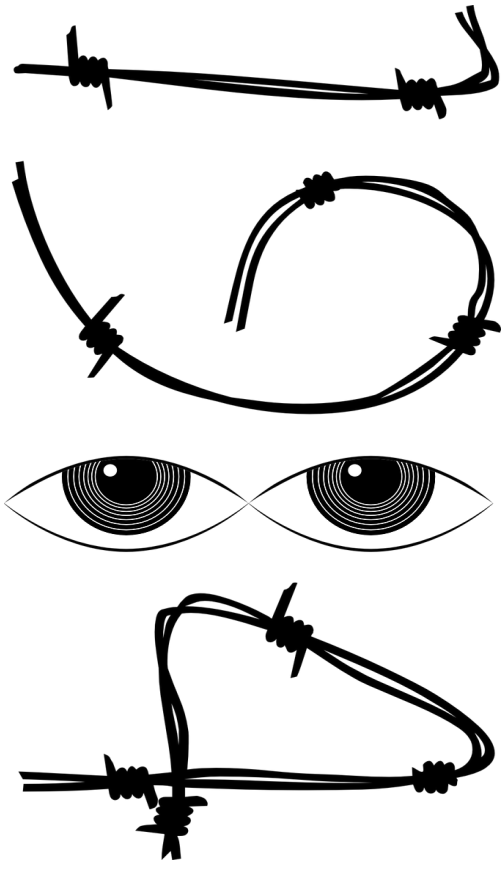
La era de la libertad, vaticinaban, de la libre circulación de información, cultura, transparencia. Esa era la meta. Unos valores que se esgrimían para defender el uso abierto y comunitario de la World Wide Web (WWW) en un mundo aún acostumbrado a rebobinar y soplar el polvo del VHS. Sin embargo, la proyección y el potencial de los nodos que habían ejecutado el avance de las telecomunicaciones supuso, de repente, una amenaza. Un interés. Un control.

No son teorías conspiratorias ni imaginaciones de los activistas que luchan a merced de sus vidas por encontrar una vía de escape a las escuchas y rastreos a los que se les somete en sus países de origen. Tampoco esta esquizofrenia virtual es propiedad de gobiernos dictatoriales, como podría pensar algún ciudadano occidental orgulloso de la libertad que aporta el capitalismo al sistema de bienestar común. Es la realidad común, y el periodista ha descubierto en su ejercicio diario que esto es el principio.

La señal titilante estalló en una cascada el año 2010 en la plataforma Wikileaks. Aunque hay varias revelaciones en etapas sucesivas, una que marcó la agenda política internacional y periodística fue la *Filtración de documentos diplomáticos de los Estados Unidos*. La primera gran colaboración de cinco medios internacionales: The Guardian (Reino Unido), *Le Monde* (Francia), *Der Spiegel* (Alemania), *The New York Times* (Estados Unidos) y *El País* (España).

Este hito llevó al vicepresidente Joe Bidden, mano derecha en el momento de Barack Obama, a decir que Assange era un "terrorista de alta tecnología". ¿Era así? ¿Desvelar los documentos secretos que comprometían el prestigio de las democracias occidentales era un delito? El servicio público y la libertad de prensa y expresión se conjugaban en un auténtico ejercicio deontológico y periodístico por mantener y vislumbrar la verdad.

El *Caso Snowden* y *Los Papeles de Pa-*



namá resultaron dos filtraciones de dos fuentes anónimas pusieron en jaque al sistema y marcaron la década. ¿Qué herramientas emplearon entonces estos profesionales? ¿Cómo se comunicaron estas denunciantes con ellos? ¿De qué manera podían garantizarles su anonimato?

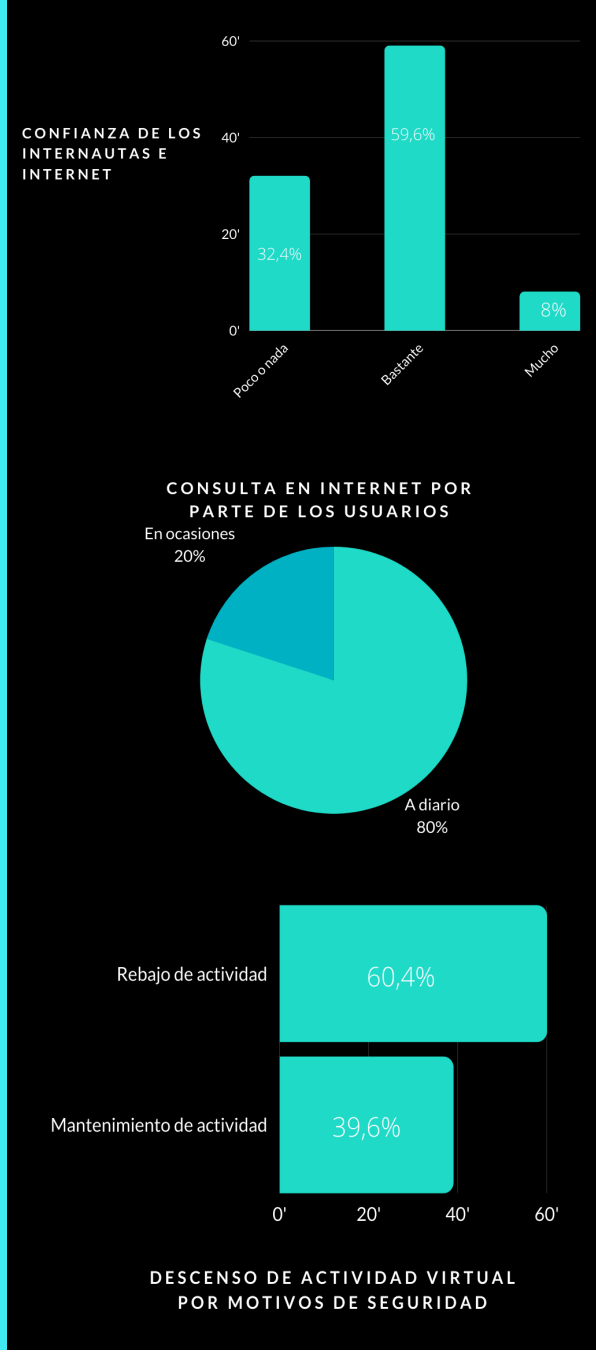
Dentro de ella, como una especie de *matrioska*, está Tor (The Onion Router), un proyecto que se superpone en la red para garantizar la comunicación anónima. El anonimato es un aliciente para los deseen revelar historias o transmitir documentos a los periodistas, aplicando *la ruta de la cebolla* mediante las *secure drop* —una *caída segura*—.

Ahora bien, ¿sabe el usuario a qué se enfrenta?

Las noticias que salen sobre el uso de los datos y sus consecuencias ha hecho que la ciudadanía española, por ejemplo, rebaje su actividad virtual, como indica el último informe del Instituto Nacional de Estadística, y tome precauciones en el uso de la tecnología que hoy día resulta imprescindible.

A nivel global, el portal Tor Metrics cuantifica la cantidad de volumen y navegantes que hay en sus lides en unos 2 millones en un día. En paralelo, el Banco Mundial apunta que en 2017 un 49,7% de la

Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares de 2019, del Instituto Nacional de Estadística (INE)

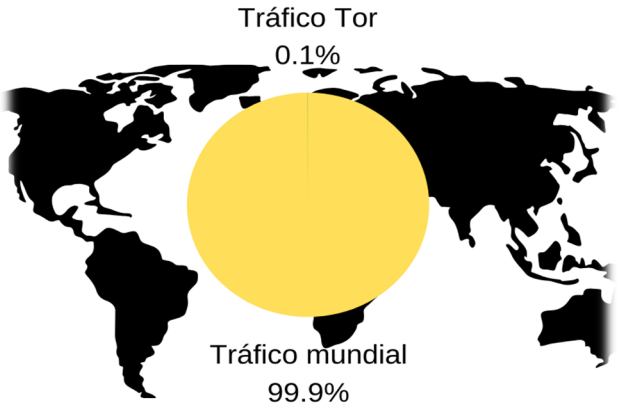


Elaboración propia.

población usaba internet, lo que daría cerca de 3 mil millones de usuarios alrededor del globo. Las cifras en términos porcentuales quedan en un 0,1% para Tor frente al 99,9% total…

Es como si solo Canarias estuviera borrando sus huellas en la arena.

Comparativa entre el tráfico mundial y de la red Tor



Elaboración propia.

Los inicios

La aparición de internet es uno de los puntos álgidos de la historia de la humanidad. Así, la red es un conjunto descentralizado de redes de comunicación enlazados a través de los protocolos TCP/IP, es decir, los pasos para que un contenido se direccione sin interferencias.

1962

En agosto, J.C.R. Licklider, informático estadounidense, previó el nacimiento de la computación interactiva moderna. Trabajaba en el Instituto de Tecnología de Massachusetts (MIT) e inició un proyecto para la Agencia de Investigación de Proyectos Avanzados (ARPA) del Departamento de Defensa de los EE. UU.: Arpanet.

Otros autores como Leonard Kleinrock, científico del MIT, publicaron sus aportaciones a la teoría de conmutación de paquetes, dando la posibilidad de aplicar estos preceptos. Lo que lograron fue que los ordenadores "dialogaran" entre sí. Era una carrera que confluía con las publicaciones de varios grupos de investigación en el mismo período de tiempo.

1969

El 29 de octubre de 1969 se transmitió el primer mensaje de la red de computadoras del sistema Arpanet.

Arpanet experimentó con la tecnología de comunicación de datos por paquetes y propició el intercambio entre la base de datos de los centros de investigación

Este cordel invisible logró la transmisión de información entre los aparatos, pero no la comprensión pues sus programas funcionaban como idiomas diferentes.

1991

La implantación de la fibra óptica a finales de los ochenta logró agilizar la expansión del cableado para unir los sistemas que se estaban creando. La política estadounidense aprobó en 1991 la *High Perfomance Computing and Communication Act*, conocida como Ley Al Gore debido a que fue su artífice al proponerla como senador en la oposición durante el mandato de George W. Bush padre. En ella, plasmaría la total liberalización del sector. La inversión pública de la administración fue de unos 600 millones de dólares dirigida a la renovación de la infraestructura. Por fin, el desarrollo de una banda ancha iniciaba la globalización de internet con la implicación del sector privado.

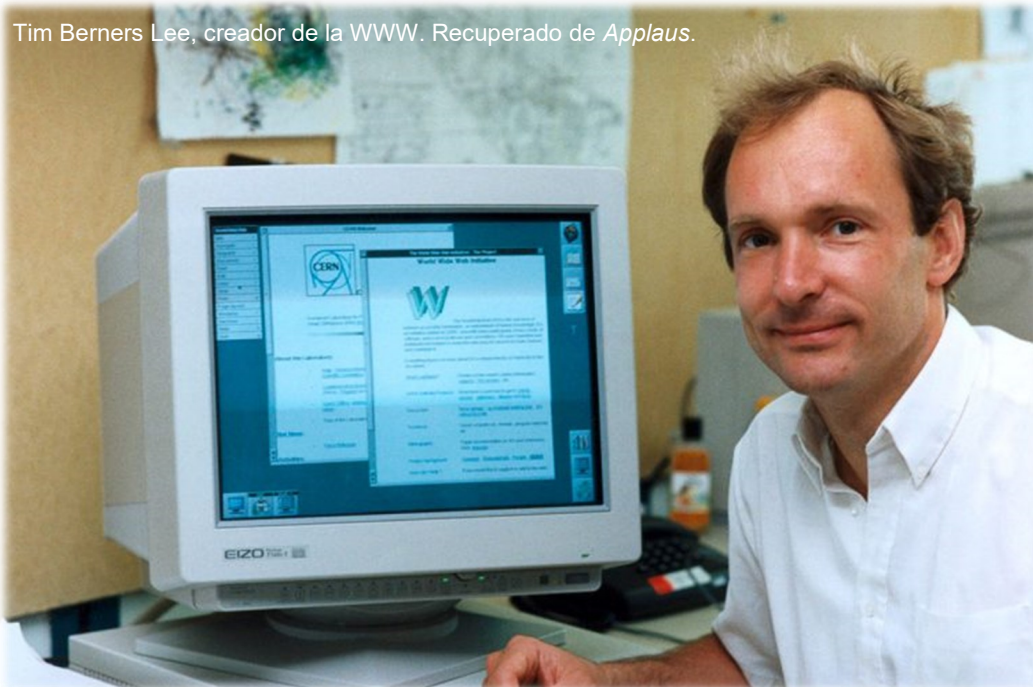
Mientras, España estaba supeditada a la política del marco europeo en el ámbito de las telecomunicaciones, por lo que influyó la desregulación de los Estados Unidos en el sector. La directiva europea optó en 1998 por seguir los preceptos de Martin Bangemann, comisario responsable del estudio *Europa y la sociedad de la información planetaria*, donde destacó la necesidad de crear un marco reglamentario y jurídico para optimizar los recursos de esta nueva industria.

De camino a la triple

Una fecha clave para entender la clase de hiperconectividad es el 6 de agosto de 1991.

Un científico computacional presentó la *World Wide Web*. Tim Berners Lee, el padre de las 3W, consiguió promover la construcción de una arquitectura común gracias a tres ingredientes. Primero, un lenguaje de etiquetas denominado hipertexto (*HyperText Markup Language,* HTML), que es un sistema que ordena la información para ser leída en la pantalla a partir de etiquetas que sugieren y describen el contenido de las páginas web, cuyo contenido se almacena en los servidores web. Seguidamente, el diálogo entre estos servidores y ordenador que accede a las páginas se haría mediante un protocolo de transferencia del hipertexto (*Hypertext Transfer Protocol*, HTTP). Y, por último, cada web poseería una dirección (*Uniform Resourse Locator,* URL) para hallarla. Según el World Wide Web Consortium (W3C), la web es "un espacio informativo donde los ítems de interés, referidos como recursos, están identificados por un identificador global llamado *Uniform Reourse Identifiers* (URI)".

Para que la burbuja virtual opere y sea efectiva es necesario que haya una infraestructura física que la soporte. La ciencia de las telecomunicaciones establece sus principales bazas en los cables submarinos, que suponen cerca de un 95% del tráfico de voz y datos, y los satélites. La plataforma TeleGeography proporciona un mapa detallado del cableado mundial con unos 406 tubos de fibra óptica en constante cambio. El intercambio de grandes volúmenes de información ronda entre las principales potencias, siendo EE. UU. una de las principales acaparadoras del mercado mundial vía el Atlántico y el Pacífico.



Tim Berners Lee, creador de la WWW. Recuperado de *Applaus*.

Los océanos como fuente de vida, y conexión

La construcción de la red BELLA, un cable submarino que conectará Europa y América Latina directamente y cofinanciada por la UE con 25 millones de euros, es una señal para el curso de los datos de ambas regiones. Anunciada en el 2015, la promoción de cables tienen un impacto económico en la distribución de la riqueza y las transacciones extranjeras, dándole una ventaja competitiva a los centros financieros bordeados por la costa.

La apuesta por el despliegue tecnológico es desarrollo. Según el Informe Especial del Tribunal de Cuentas Europeo, un incremento del 10% en conexiones de banda ancha en un estado podría suponer un aumento del PNB per cápita del 1% anual o la mejora de la productividad en un 1,5% en los siguientes cinco años. Por ello, las naciones africanas se sumarán con la construcción de unos 37 mil kilómetros de cable submarino alrededor de su litoral. El capital privado será puesto por Facebook junto las compañías de telecomunicaciones China Mobile International, MTN GlobalConnect, Saudi Telecom Group, Orange, Vodafone y West Indian Ocean Cable Company, para invertir en la industria africana y, por supuesto, en futuros clientes.

Lo físico es tangible y la visualización ayudan a determinar quién o qué controla los canales de información que usa la población para comunicarse. La metáfora tiene cabida en la era digital. El almacenamiento pasó del disco duro a ser remoto y hablar del almacenamiento en la nube o *cloud computing* cuando la sincronización y el acceso a los datos es por medio de internet. No un pendrive,

La instalación de cables submarinos favorece la economía de un país y traza las rutas de comunicación global

sino un servidor externo que puede estar en Alaska y en el que uno confía que mantenga segura y privada su información, al estilo de Google Drive o los servicios de correo electrónico. James Bridle, escritor londinense, habla de la nube como algo que experimentamos sin entender qué es o cómo funciona, a lo que el individuo se ha acostumbrado a confiar sin tener idea de su poder, como recoge la periodista Marta Peirano en su libro *El enemigo conoce el sistema*.

Sería una simple anécdota, salvo por XKeyscore, un sistema informático secreto de la Agencia de Seguridad Nacional de los Estados Unidos (NSA) desvelado por el *Caso Snowden* y publicado en *The Intercept* en 2015. El registro del tráfico internauta que se suministraba por la fibra óptica de los cables submarinos permitía el espionaje de cerca de 700 servidores distribuidos por México, Brasil, Reino Unido, España, Rusia, Nigeria, Somalia, Pakistán, Japón y Australia. El programa interceptaba correos electrónicos, llamadas teléfonicas, servicios *online* que incluían hasta las sesiones de Skype. El resultado eran diez billones de grabaciones recogidas en la base de datos de la NSA.

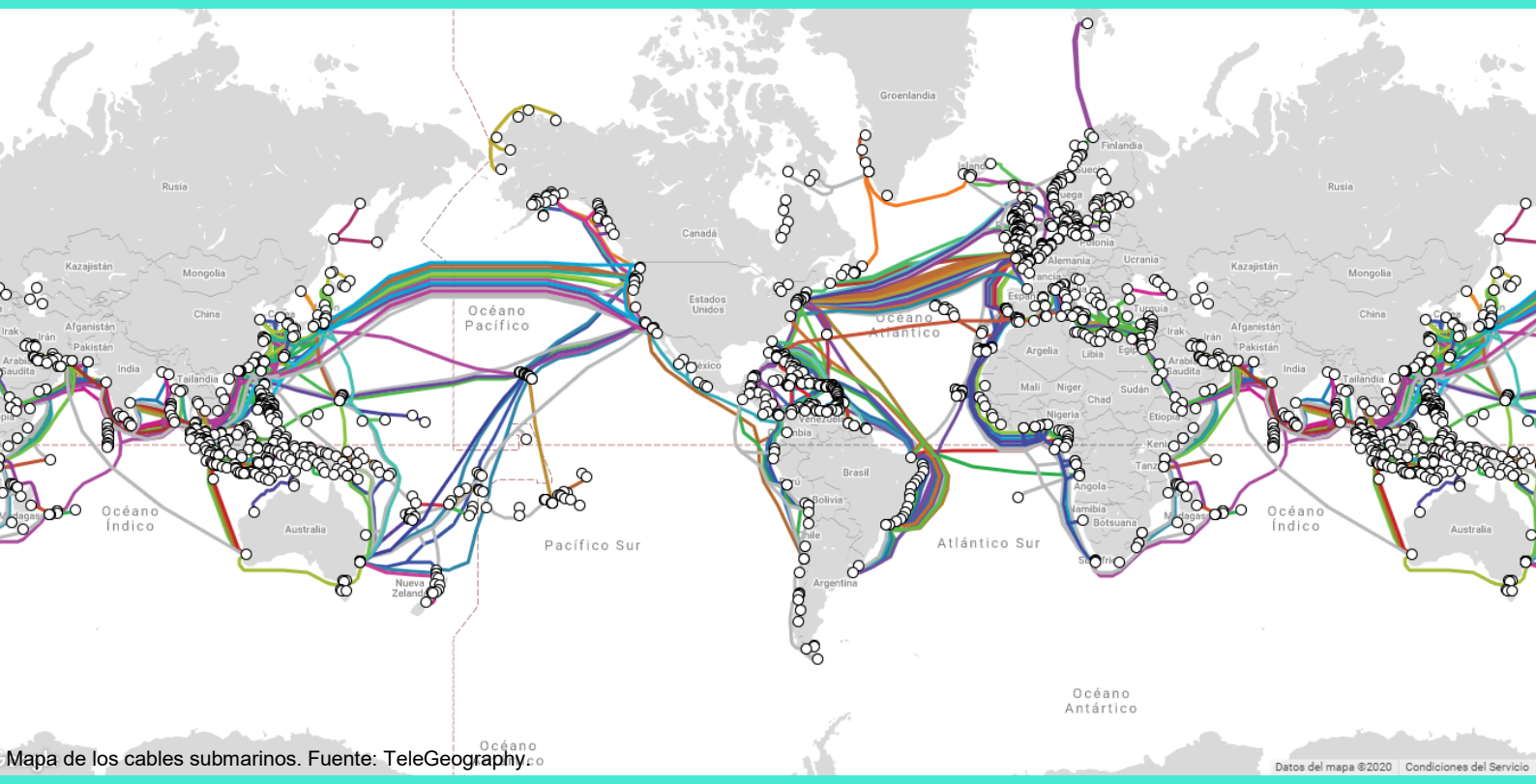
Por tanto, la gestión del tráfico da el poder de leer la información de las cabeceras de los paquetes, para comprobar que cumplen los requisitos del protocolo y, el de regular su itinerario. El pódium de los proveedores mundiales de la nube lo encabezan Amazon Web Service (AWS), Microsoft Azure y Google Cloud Platform. La conexión de estos puntos está íntimamente relacionada con el quehacer diario de quienes encienden un monitor o un teléfono móvil.

Declaración de Independencia del Ciberespacio

"...In China, Germany, France, Russia, Singapore, Italy and the United States, you are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace. These may keep out the contagion for a small time, but they will not work in a world that will soon be blanketed in bit-bearing media..."

John Perry Barlow , fundador de Electronic Frontier Fundation

Davos, 8 de febrero de 1996



Mapa de los cables submarinos. Fuente: TeleGeography.

Un secreto compartido

Vista aérea de la marcha del 8 de diciembre de 2019 por el Día de los Derechos Humanos en el distrito de Causeway Bay en Hong Kong, seis meses después del inicio de las protestas contra el control ejercido por China. Laurel Chor (Reuters).

.

Un manifestante arroja un cóctel molotov en El Cairo en las Revueltas Árabes de 2011. Amr Abdallah Dalsh (Reuters). Recuperado de *El País*.

En la actualidad, hay países como Ecuador, Bolivia o Venezuela que carecen de una ley de protección de datos, y la tendencia de los usuarios en los próximos años va dirigida a usar la tecnología de la nube. La protección es urgente y decisiva para defenderse de los ataques cibernéticos, escriben los investigadores.

La cuestión es acuciante, por lo que en 2016 el Consejo de Derechos Humanos de las Naciones Unidas afirmó y reconoció que las personas gozan de los mismos derechos en internet, reafirmándose así en el artículo 19 de la Declaración Universal de los Derechos Humanos sobre libertad de expresión y del Pacto Internacional de Derechos Civiles y Políticos. A escala europea, la protección está amparada en el Reglamento General de Protección de Datos de la Unión Europea (RGPD), con su aprobación en 2016, y las legislaciones nacionales adaptan y promulgan la seguridad de sus habitantes. Entonces, ¿por qué una ingente cantidad de información confidencial sirve para la *economía de datos*, que mueve billones de dólares, y al espionaje masivo?

La Agencia de Ciberseguridad de la Unión Europea (Enisa) alumbra en el artículo *The value of personal online data* una cifra llamativa. El promedio de ingresos por usuario (ARPU – *Average revenue per user*) en los anuncios publicitarios, principalmente controlados por Google y Facebook, llega a los 59 dólares por persona en 2017. Multiplíquese por los millones de usuarios que utilizan la red. En cuanto al espionaje masivo, la filtración de un informador a *The Guardian* alertó de los 87 millones de perfiles de Facebook que se usaba para las campañas de las elecciones estadounidenses por la entidad Cambridge Analytica. El resto es Trump.

Internet ofrece la posibilidad de participar en debates públicos, hacer activismo, buscar, difundir y programar sin tener que revelar la identidad personal.

Una pantalla muestra al presidente chino Xi Jinping en una calle de Pekín durante una alocución gubernamental. Kevin Frayer (Getty Images). Recuperado de *El País*.

En consecuencia, el Relator Especial de la Asamblea General de las Naciones Unidas, Frank La Rue, expresó su preocupación por los bloqueos o filtros arbitrarios de los estados que emplean mecanismos de censura en la red como la vigilancia motivada por razones políticas y no de seguridad nacional, la cual puede llevarse de manera arbitraria y encubierta. Medidas como la "respuesta graduada", una serie de avisos al usuario que, infringiendo derechos de propiedad, pueden terminar en la suspensión del servicio de internet —dado en la "ley de los tres avisos" en Francia y la Ley de economía digital de 2010 del Reino Unido— son propuestas que evidencian el intento de un control centralizado del tráfico web. Además, el Relator nombra el triángulo que se ha ido construyendo a lo largo de estas últimas décadas: **Estado, individuo y plataforma**. Esta relación no es baladí. De ahí que haga hincapié el experto europeo en la influencia sin precedentes del sector privado en la vida del individuo y recuerde que el papel de las empresas es motivar y velar la privacidad, no convertirse en un aliado de los estados que desean obtener los nombres y comunicaciones privadas de los usuarios.

La lucha contra la censura fue el adalid del constitucionalismo liberal y permitió que la prohibición previa de publicación frente al Estado fuera abolida. La excusa repetida por los gobiernos es la seguridad nacional y la lucha contra el terrorismo para hacerla prevalecer. Ahora los poderes privados poseen una supervisión del flujo de comunicación muy superior a ninguna acción censora de la gobernanza habida.

Un policía británico saca una foto mientras un transeúnte mira. Mattew Wilkinson (Flockr). Recuperado de *eldiario.es*

Los anuncios de las plataformas se segmentan según los *me gusta*, las páginas visitadas, la geolocalización y demás detalles conforman un perfil minucioso de cada uno. Pone en peligro también la seguridad de los alertadores periodísticos y del profesional.

El estudio *Censura y vigilancia de periodistas: un negocio sin escrúpulos* de Reporteros Sin Fronteras (RSF) analiza el negocio de la vigilancia masiva. China, Irán, Siria o Uzbekistán encabezan la lista de los países más represivos del mundo en libertad de información en la red, pero la permisividad tiene su punto de partida en los estados occidentales. RSF notificó en 2013 que cinco compañías que operaban con sistemas de espionaje de datos se ubicaban en Reino Unido, Alemania, Italia, Francia y Estados Unidos, y destacó al conglomerado Hacking Team, que vendía tecnología "ofensiva" de vigilancia a Marruecos y a los Emiratos Árabes Unidos.

Casualmente, en el año 2015 saltaba a los medios de comunicación españoles que el Centro Nacional de Inteligencia (CNI) compraba material a este equipo para tener acceso a los sistemas operativos que decidiera infectar el cuerpo de inteligencia.

El presidente George W. Bush firma junto a los miembros del Senado la USA Patriot Improvement and Reauthorization Act en 2005, ley motivada por el ataque terrorista del 11-S. Eric Draper. Recuperado de Archivos de la Casa Blanca.

La cobertura periodística a estos niveles recuerda Mercé Molist, periodista especializada en tecnología y autora del libro *Hackstory.es,* que era algo que producía desconcierto entre sus compañeros de redacción en los 90 cuando aprendió cómo se enchufaba un módem a la red. "La seguridad se ha hecho cada vez más fuerte y se ha convertido en un negocio, tan solo tienes que ver las aplicaciones y la conexión que se requiere, en detrimento de la privacidad", anota por teléfono, "el mundo digital es una esfera que lleva la monitorización por defecto, y se pueden saber tantas cosas que me parece hasta normal que la privacidad se haya rebajado tanto con la mejora de estas tecnologías puesto que viene así por defecto". En su actividad diaria utiliza PGP (Pretty Good Privacy), un programa que protege las conexiones vía internet mediante el uso de criptografía de clave pública, o Signal. "También he utilizado Tor para encubrirme a mí misma y evitar dejar mi rastro, o para visitar una web que había bloqueada". Entiende que esto tendría que ser el corpus digital de la redacción: "Los periodistas deberían usar por defecto sistemas como el PGP, por ejemplo, pero tiene que ver mucho con la educación de la sociedad ya que, si el conjunto y tu fuente no las utiliza, tú como periodista tampoco puedes".

¿Qué hacer para despistar el rastro y disipar la huella?

"La seguridad se ha hecho más fuerte en detrimento de la privacidad"

Panorámica del Pentágono, el Departamento de Defensa de los EE.UU. Recuperado de *20minutos.*

La ruta de la cebolla

La *deep web* es lo que escapa a los motores de búsqueda convencionales. Es una gran cantidad de masa de información que está oculta porque no están indizadas. Las cifras que se suelen manejar acerca de su dimensión dan una estimación de unas 400 o 500 veces más cantidad de información que la World Wide Web, además, el escrito del *The journal of electronic publishing* atribuía en 2001 unos 7.500 terabytes a la web profunda con un total de 200 mil sitios apreciados. Dos décadas más tarde, a falta de un análisis similar, se le supone un crecimiento exponencial.

Cuando se habla de esta dimensión se alude a documentos (archivos pdf, imágenes, vídeos, que no constan de protocolos HTML que los indexe); bases de datos de origen académico, empresarial, científico, administrativo; contenido de acceso restringido u oculto a propósito que requiere de programas específicos para intervenir; o de páginas no enlazadas que se ubican fuera de los hiperenlaces.

Poco o nada se habla de las posibilidades que ofrece y los usuarios que publican una ruta de la seda en su interior suelen centrarse en la famosa *dark web*. En realidad, el término corresponde a los servicios fraudulentos y nocivos que le dan mala fama al resto de la burbuja, pero sigue dentro de ella. Para acceder al tráfico ilegal de armas, drogas, pornografía, o al requerimiento de los servicios de *hackers* rusos especializados en ciberataques se ha de utilizar las mismas herramientas que pasan por la web profunda, debido a que estas *madrigueras*, por razones obvias, tampoco quieren ser encontradas.

Cada vez que alguien se conecta a la red, el sistema envía paquetes de datos con la información que esa persona está gestionando. Los paquetes van de un punto a otro reconocible que identifica tanto la puerta de salida del ordenador del usuario como la puerta a la que está tocando el mismo aparato para que se le abra el servicio que requiere. Esas *migajas* que se dejan es la que alimentan a los algoritmos, y hay maneras de evitarlo.

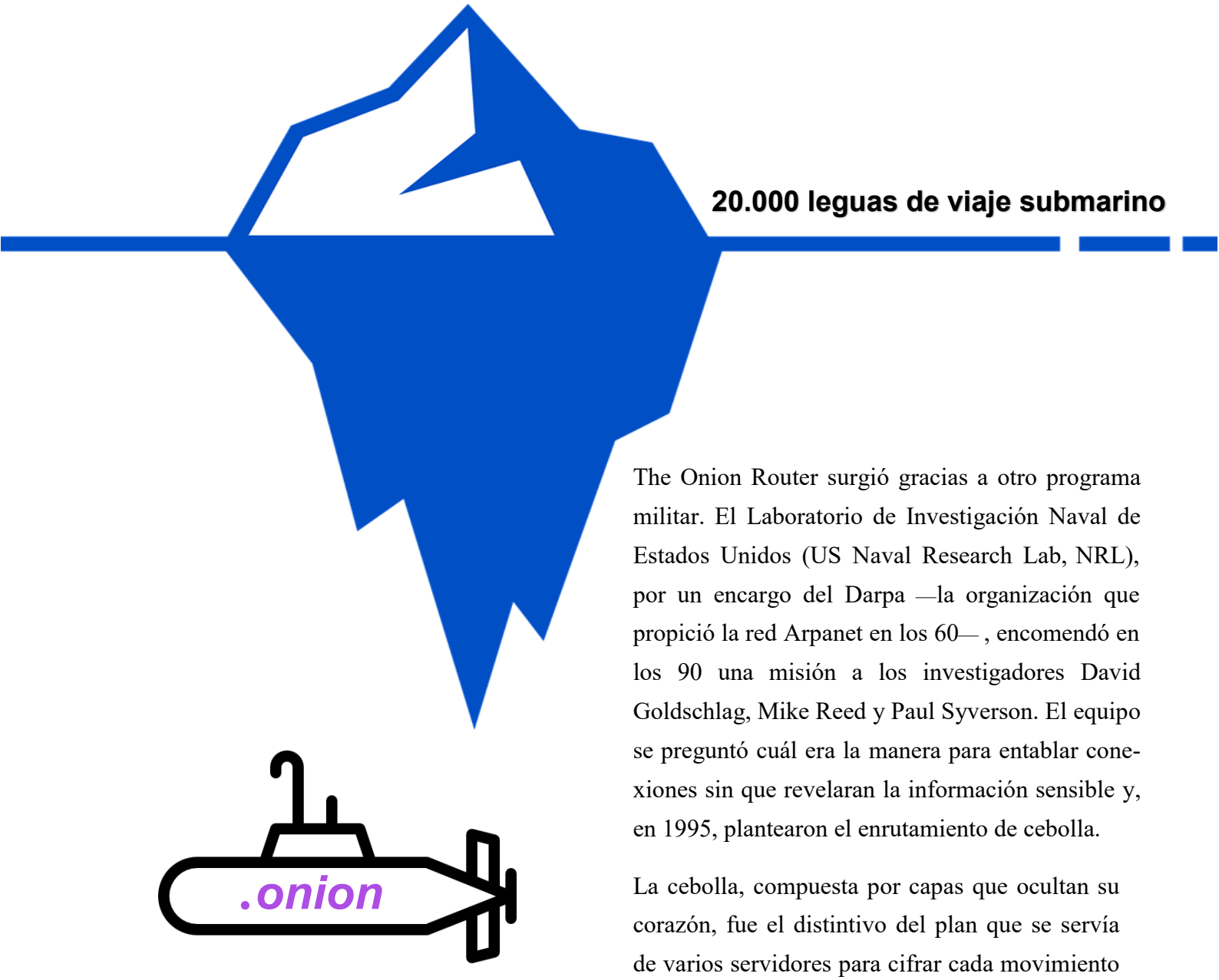
La clave de la inmersión y la supervivencia en un medio, previsiblemente hostil, es la encriptación. Marta Beltrán Pardo, especialista en Arquitectura y Tecnología de Computadores en la Universidad Rey Juan Carlos y cofundadora del Cybersecurity Cluster, comenta vía *email* que no hay "una técnica perfecta". Aclara que, si bien la cripto simétrica es más eficiente y rápida, es difícil resolver el problema del reparto de claves, y una vez comprometida la clave, el sistema está roto; mientras que la cripto asimétrica es poco eficiente y lenta, pero su clave pública se reparte con facilidad. En definitiva, "lo bueno es que cada dominio de aplicación se escoja la más adecuada según las necesidades que se tienen". Los esfuerzos están enfocados en la criptografía cuántica: "Si los computadores pueden romper por fuerza bruta un criptosistema actual en pocos minutos, habrá que repensar todo y, desde el punto de vista de la vida cotidiana, tenemos un reto con las contraseñas y en cómo evitar que los usuarios tengan que recordar 100 diferentes". La educación es fundamental para que los "nativos digitales", dice, entiendan que "una cosa es estar rodeados de tecnología y verla como algo natural, y otra es saber entenderla y usarla de manera segura". Hace un alto en el camino para subrayar que, a pesar de que Snowden dijera que la criptografía es el método infalible, "no es el único factor".

"Si los computadores pueden romper por fuerza bruta un criptosistema actual en pocos minutos, habrá que repensar todo"

Concluye que en la actualidad la seguridad se asienta sobre más pilares debido a que las amenazas son muy variadas y la cripto no nos puede proteger de todas ellas.

Uno de los múltiples acechos que cercan la rutina cibernética es la vulnerabilidad del *software*. La organización europea Enisa publicó en marzo de 2018 el artículo *Is sofware more vulnerable today?*, donde recogía los datos de las agencias National Vulnerability Database (NVD) y la Common Vulnerability and Exposures (CVE). En él, asevera unas 14.500 vulnerabilidades nuevas en 2017 comparadas con las 6.000 registradas en el mismo período del año anterior. Las razones que atiende la Enisa para el considerable crecimiento de estos fallos se debe a la innovación del mercado, así como a la menor madurez de los productos por competir antes en el sector y, también, la inadecuada legislación que no protege al consumidor y desincentiva el compromiso de la industria. Entre las soluciones propuestas remarcan una: la responsabilidad del *software*, una iniciativa recogida en la RGPD europea para comprometer a los promotores.

Toda precaución es poca y es hora de hablar de Tor.



The Onion Router surgió gracias a otro programa militar. El Laboratorio de Investigación Naval de Estados Unidos (US Naval Research Lab, NRL), por un encargo del Darpa —la organización que propició la red Arpanet en los 60— , encomendó en los 90 una misión a los investigadores David Goldschlag, Mike Reed y Paul Syverson. El equipo se preguntó cuál era la manera para entablar conexiones sin que revelaran la información sensible y, en 1995, plantearon el enrutamiento de cebolla.

La cebolla, compuesta por capas que ocultan su corazón, fue el distintivo del plan que se servía de varios servidores para cifrar cada movimiento en el camino. Ahora los paquetes ya no irían de un extremo a otro, sino que conformarían un re-

corrido impredecible de nodo en nodo para llegar al final del camino. El primer servidor de Tor que conecta con la red Tor, o puerta de enlace, sabe quién es el que envía la solicitud, pero no puede conocer su contenido. Cuando el ordenador del usuario toque en el servidor que requiere, este no podrá ver cuál fue la puerta de salida de su visitante. Solo se da a conocer el último nodo de salida o *exit relay* —el horizonte entre Tor y el resto—. Así, la petición llega sin que se sepa el IP, el número de identificación del usuario.

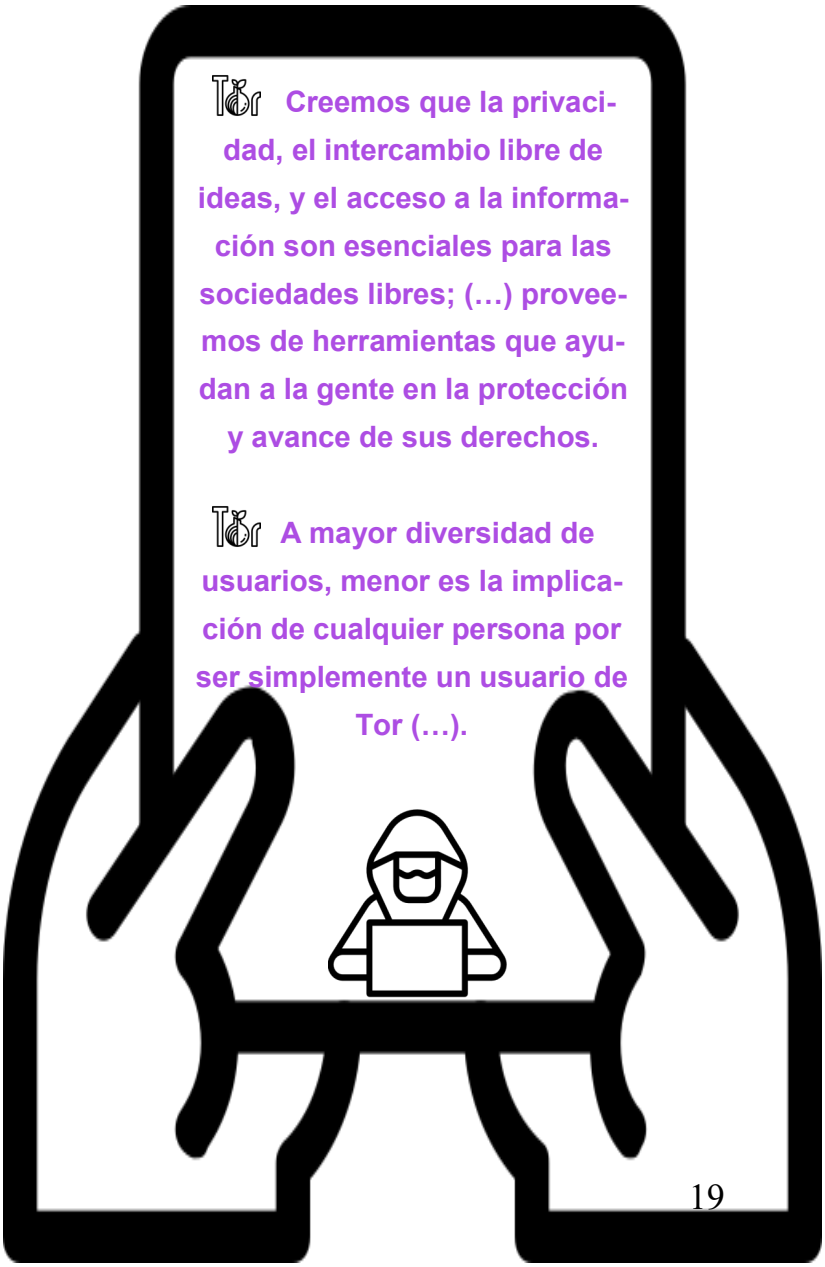
En el 2000, el plan pasó a Roger Dingledine, del MIT, y lo bautizó como Tor. A él se le unió Nick Mathewson y, dos años más tarde, publicaron el código bajo una licencia de *software* libre. El proyecto se había democratizado, y la Electronic Frontier Foundation (EFF) apostó por su financiación en 2004 con la característica URL de dieciséis caracteres con terminación (.onion).

Nick Mathewson se disculpa por la tardanza y envía sus respuestas. Desea concienciar que el mundo tiene la oportunidad de hacer efectivo un *software* al que sea intrínseco la privacidad, donde las garantías que prestaría serían menos vulnerables que las que su propio equipo experimentó en los 90. Con un emoticono sonriente es determinante: "Estoy a favor de la privacidad digital, y creo que todos los argumentos en contra de ella son tonterías —*bunk*—".

Mathewson recuerda que "no tiene sentido hacer un *software* que la gente no use y, personalmente, tengo fe en la humanidad como un conjunto, en vez de cualquier gobierno en particular". Detalla que la paradoja está en cuando los investigadores del NRL se dieron cuenta de que una red privada debía de ser abierta para la sociedad, ya que, si se descubriera la naturaleza de esta se podría, lógicamente, saber quienes eran los implicados.

El informático coincide con la investigadora Beltrán: "Con encriptación regular, como la que usas para visitar una página web segura con tu buscador, solo tu ordenador y la página pueden decir lo que estás diciendo, pero cualquiera en ese mismo internet puede decir con quién estás hablando", añade, "esto no es bueno si el mero hecho de estarte comunicando es sensible". Acerca de quienes aún no se acercan a estas medidas de ocultamiento advierte que, el no utilizarlo, no se puede traducir como una menor preocupación, "creo que el factor de actuación es crítico en cuándo y por qué la gente toma la decisión de seguir con Tor".

Hay dos *contratos sociales* del Proyecto Tor que han logrado la implicación de la comunidad internauta:



A más usuarios, más fácil es cubrir la identidad con los miles de repetidores disponibles. Ellos son quienes transitan por el navegador web Tor Browser, llegado en 2008, el mando que posibilita acceder a la *deep web* sin represalias. Periodistas, activistas, organizaciones por los derechos humanos, plataformas como WikiLeaks, ciudadanos de países en los que imperan medidas restrictivas buscan a través de esta infraestructura cibernética información y libertad de circulación.

El principio de neutralidad en la red establece que tanto los proveedores de servicios de internet como los gobiernos deben establecer que el tráfico que transite será en igualdad de condiciones. Significa no incrementar ni instaurar tarifas adicionales por visitar alojamientos de mayor peso, carga, contenido, etc. La evolución del debate en la Federal Communications Commission de EE.UU., que aprobó en la Telecommunications Act de 1996, demostró su compromiso a partir de una serie de principios que ofrecen libertad al consumidor en materia de elección del contenido, uso de aplicaciones y servicios, elección de conectarse a través de las máquinas que decida y la competencia entre proveedores.

Sin embargo, las injerencias continúan.

La NSA intentó aunar esfuerzos para tumbar la red Tor a través de técnicas como la EgotisticalGiraffe, la cual se colaba por los fallos de los ordenadores. Pero no lo consiguió, como revelaron los documentos de Snowden en *The Guardian*. Mathewson es optimista: "Lo más importante para la supervivencia de Tor es que es *software* abierto que cualquier pueda utilizar. Incluso si los que trabajan en Tor pararan, sería posible continuar para otros". Indica que el término común es hacer crecer el número de programadores y, en un futuro que no se atreve a predecir, "mi esperanza es que las ideas de Tor se vuelvan tan ubicuas como la TLS —*Transport Layer Security*—, e internet sea privada por defecto".

Edward Snowden escribe en su biografía: "Tor era incluso más neutral que Suiza. A mí, Tor me cambió la vida, (…) al permitirme saborear ligeramente la libertad de no sentirme observado".

El programador estadounidense no había leído los avances en una red cuántica que promete en los próximos cinco años lanzar mensajes de un servidor a otro sin que se pueda *hacker* su contenido. Un equipo de investigación dirigido por la Universidad Tecnológica de Delft Stephanie Wehner, y en colaboración la Alianza de Internet Cuántico y la Universidad de Ciencia y Tecnología de China dibuja la utopía de una seguridad total.

Existen otras vías por las que acceder a la *deep web*, bien por Invisible Internet Project (I2P) o Freenet. La periodista Marta Peirano concluye en *El pequeño libro rojo del activista en la red* que esas redes, diseñadas para la descargada de archivos y fundamentados en el sistema P2P -donde los ordenadores funcionan como pares cuyos nodos alternan la función de cliente y servidor- se sirven de Java y carecen de tantos servidores de salida. Por lo que su efectividad es menor.

La popularización de la red Tor y los peligros que acechan a los periodistas de investigación convencieron a los grandes medios para apostar por técnicas seguras y eficaces para que sus fuentes, los *whistleblower*, se comuniquen de manera segura con ellos. Son las conocidas como *secure drop*. Arriba, en rojo, dice, *pero ¡qué haces, no activas Tor y la búsqueda no es segura!*

Vamos a cambiar.

"Mi esperanza es que las ideas de Tor se vuelvan tan ubicuas como la TLS , e internet sea privada por defecto"

La profesora Juliana Freire, de la Universidad de Utah, trabajando en la DeepPeep. Jeffrey D. Allred para *The New York Times*.

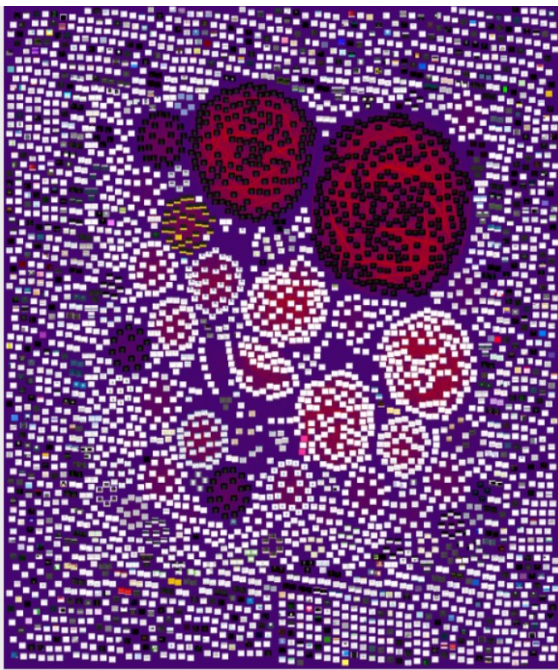
Sumergidos en la *deep* web

Descargarse Tor Browser es sencillo. Desde Proyecto Tor se puede obtener el buscador de la cebolla. Este se instalará en apenas unos minutos y la primera pantalla que aparecerá será, tras la ejecución, la ventana de la configuración de la Red Tor. Da dos opciones: conectar y configurar. La segunda está dispuesta para los países en los que se prohíbe la plataforma, como Egipto, China o Turquía, donde bloquean los proveedores de servicios de internet (ISP). La plataforma se amolda a las circunstancias para evitar la censura e instalarla con éxito.

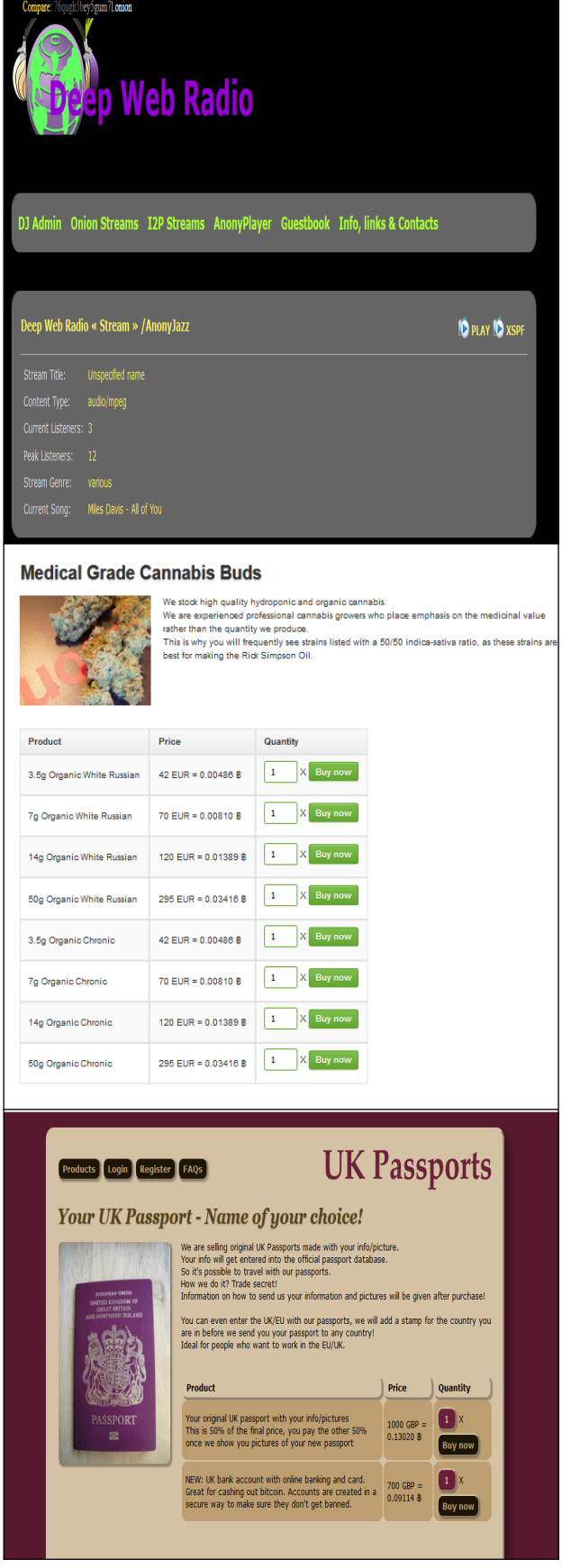
Al entrar por primera vez da como motor de búsqueda predeterminado DuckDuckGo. El nivel de seguridad que ofrece es el estándar, el cual puede modificar el internauta. Tor recomienda evitar los elementos que contengan el plugin Flash Player, los que utilicen el lenguaje de programación JavaScript porque puede habilitar ataques a la seguridad, y, en definitiva, desaconseja la instalación de complementos adicionales que afectarían a la seguridad del sistema.

Hay numerosas investigaciones universitarias que intentan indexar el contenido de la *deep* web para lograr unir las millones de bases de datos que pululan en el vacío. Un reportaje de *The New York Times* se hacía eco del estudio de la DeepPeep, una apuesta de la Universidad de Utah por establecer patrones de búsqueda semántica en el subsuelo. Alcanzó unas 13.000 direcciones hasta que el proyecto quedó cancelado. Otro camino.

En julio de 2018 un grupo de analistas que se autodenominan frikis, "pero somos, como, *cool* frikis", conformaron el Hyperion Gray y aglutinaron cerca de 6.600 webs accesibles usando Tor. Antes de hincarle el diente al mapa, piden aceptar un consentimiento. La mejora de las pesquisas ha dado pie a tres versiones del mapeo y, como escriben, decidieron ocultar los últimos cuatro caracteres del enlace (.onion) para preservar la privacidad y, a su vez, designar fondos blancos para no herir la sensibilidad del navegante.



Mapa de la deep web hecho por el grupo Hyperion Gray.



El servicio de Tor reconduce la navegación web por los servidores de distintos países. La cebolla dibuja un trazado, aleatorio, que contempla Francia, Alemania, Rumanía y más

Hay un camino tradicional: la HiddenWiki. Si pulsa en el símbolo de candado de la URL, el Tor Browser le notifica qué circuito está tomando en esos momentos. Haciendo una búsqueda rápida, toma el camino de Francia, Alemania, Rumanía y, finalmente, la HiddenWiki, y ofrece establecer un trazado para volver al mismo lugar y despistar.

Un *bazar persa* se despliega ante los dedos del explorador. El cartel principal está plagado de direcciones que están categorizadas en varios apartados. En primer lugar, servicios de ocultamiento (*hidden service*) y de motores de búsqueda que contemplan DuckDuckGo, Anonet Webproxy, Gateway to Freenet y otras. Deslizando el ratón, hay un mercado financiero que apunta a servicios de *bitcoins*, la moneda digital, y otros de *paypal* por si a uno le entran ganas de comprar en esos submundos. Algunos gustos populares parecen ser las armas, la tecnología marina, pasaportes, móviles y hasta un Amazon. Siempre hay que ir a la última.

Una de las millas doradas de la *deep* web es la relacionada con la compraventa de drogas. El cierre de Silk Road en 2013 fue ampliamente comentado y uno de los argumentos esgrimidos para el cese de la red Tor por *cubrir* el comercio de los estupefacientes. Dicen que donde hubo fuego queda cenizas, y se demuestra en los servicios que ofrecen algunas páginas de venta de gramos de LSD con un comentario en la cabecera bastante alentador: “Todos los productos están testados por nosotros y mezclados en nuestro laboratorio, tratamos siempre de ofrecer la mejor calidad al mejor precio”. El cliente es lo primero.

El siguiente apartado es de alojamiento, *hosting*, y da a entender la libertad del usuario a subir contenido sin prejuicio. Un tema que entronca con esta

permisividad es el reportaje publicado por Maite Garrido en *eldiario.es* acerca de un *hacker* que intentó indexar más de cien mil webs de este entorno para encontrar aquellas que publicaban y difundían material pornográfico infantil. Al mandarle un directorio de las piezas al Grupo de Delitos Telemáticos de la Guardia Civil (GDT) sufrió un registro de su propiedad, a pesar de las explicaciones que daba. El Código Penal recoge en el artículo 197/3 con relación al acceso de sistemas que "el que por cualquier medio o procedimiento, y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años". No se especifica en ningún caso la legitimidad, finalidad o servicio que podría constituir tal intromisión y los resultados que se extraigan de ella. Al final, el *hacker* no fue detenido, aunque ya se había llevado el susto.

La expresión artística tiene cabida, y por eso el apartado de blogs muestra opciones variopintas que van desde un portal de Deep Web Radio hasta una enciclopedia o algo de cienciología para variar la conversación. A continuación, los foros y chats se conjugan con los enlaces de email y mensajería. En ocasiones, se pide un usuario y contraseña para entrar en el paraje virtual, asegurándose de la pertenencia del individuo a la comunidad que forma parte de ella.

De repente, un mensaje aparece en el fondo blanco: "This site has been seized; by the FBI, (…)", el enlace deep.dot.web fue cerrado por fuerza mayor. El carácter político de la red es inmanente a ella y ofrece recursos, entre los que se encuentra WikiLeaks. Como si de una llamada complementaria se tratara está la sección del *hacking* con alquileres de servicios que van desde la instalación de troyanos hasta medidas urgentes que suponen unos 200 euros.

Las bibliotecas y la música son populares en la *deep* web gracias a un largo catálogo de descargas que está disponible antes de pasar al contenido para mayores de edad. La pornografía y los enlaces eróticos son las últimas aportaciones.

Páginas web encontradas en la dirección HiddenWiki. La URL está omitida por motivos de seguridad.

En busca de una SecureDrop

Una persona común, anónima, que posee información sensible que delata las malas prácticas de la organización en la que está contratada tiene el imperativo de denunciarlo. El hecho de comunicarse es, por sí mismo, peligroso.

La difusión y habilitación de las *secure drop* en los medios de comunicación -y que sus lectores sean conscientes de ello- es de una importancia extrema. Después de las denuncias hechas por WikiLeaks o Snowden, los periódicos anglosajones tomaron la iniciativa para la protección de sus fuentes informativas. La cuestión reside en recibir la documentación que compromete y motiva la investigación periodística. Luego, el ejercicio de contrastar y verificar los datos recibidos dará cuenta de si esa filtración es cierta y necesaria, o no.

La SecureDrop es una plataforma de *software* de código abierto que fue diseñado y desarrollado por Aaron Swartz y Kevin Poulsen en el año 2011. A la muerte de Swartz, la revista estadounidense *New Yorker* fue la primera en lanzar su versión en 2013 con el nombre de Strongbox y, ante el refuerzo de su uso, la Freedom of the Press Foundation decidió hacerse cargo del desarrollo y cambiar la denominación de DeadDrop a SecureDrop. Al estilo de Tor, que es el único medio por el que se puede abrir, configura una serie de servidores privados para mantener la fiabilidad de la mensajería que se establecerá.

En cualquier caso, la página securedrop.org da un listado de treinta medios que tiene, cada uno, su dirección (**.onion**) para favorecer la comunicación con los *whistleblower*. El usuario decide en quien confiar, selecciona y se redirige a la URL aportada por el medio y encuentra dos opciones: empezar o acceder al usuario. Mientras que el *New York Times* solo da la opción en inglés, *The Intercept* amplía al portugués y *The Guardian* atiende a la diversidad incluyendo idiomas como el inglés, chino, japonés, francés, turco, portugués, alemán y español.

La sede da la bienvenida y asegura que no rastrea a los usuarios. Automáticamente, el sistema asigna un nombre clave para las futuras visitas. Abajo, una observación: “Compartir documentos confidenciales puede ponerlo en peligro, incluso si lo hace a través de Tor y SecureDrop”. El *nick* es de cuarenta y un caracteres que conforman siete palabras. La precaución recomienda que se escriba el nombre en soporte físico y se guarde en un lugar seguro y, si no queda otra, se memorice. Son palabras escogidas al azar, y el algoritmo ahora aporta las siguientes: *atrophy jitters tibia endocrine aching*…

El ratón presiona la casilla *enviar documentos*.

Un recuadro está dispuesto a que se suban los documentos con un tamaño máximo de 500 MB. La SecureDrop advierte que los archivos son cifrados, aunque no estaría de más si, de estar acostumbrado a usar las técnicas de GPG, la persona cifrara ella misma el mensaje con la llave pública que el medio dispone a su informante.

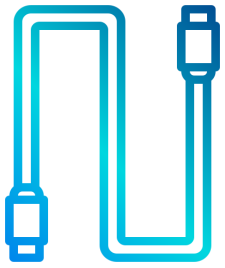
Desde ese momento, en que deja el sobre en el buzón, queda la espera hasta que se reciba un mensaje del periodista de investigación que acepte y desee continuar el diálogo para adquirir más información.

En España, la SecureDrop brilla por su ausencia. Los parques y las llamadas por teléfono son las viejas costumbres de los periodistas de raza. Canarias no tiene habilitada ninguna de estas funciones y, en general, los medios locales de las provincias tampoco. Las grandes cabeceras como *El País*, *El Mundo* o *El Confidencial* carecen de este dispositivo y, como excepción a la regla, nació Fíltrala en abril de 2014, propulsada por la Associated Whistle-Blowing Press y conformada por *eldiario.es*, *Mongolia*, *Civio*, porCausa, Ecologistas en acción, Greenpeace, Facua y la Plataforma en defensa de la libertad de información (PDLI).

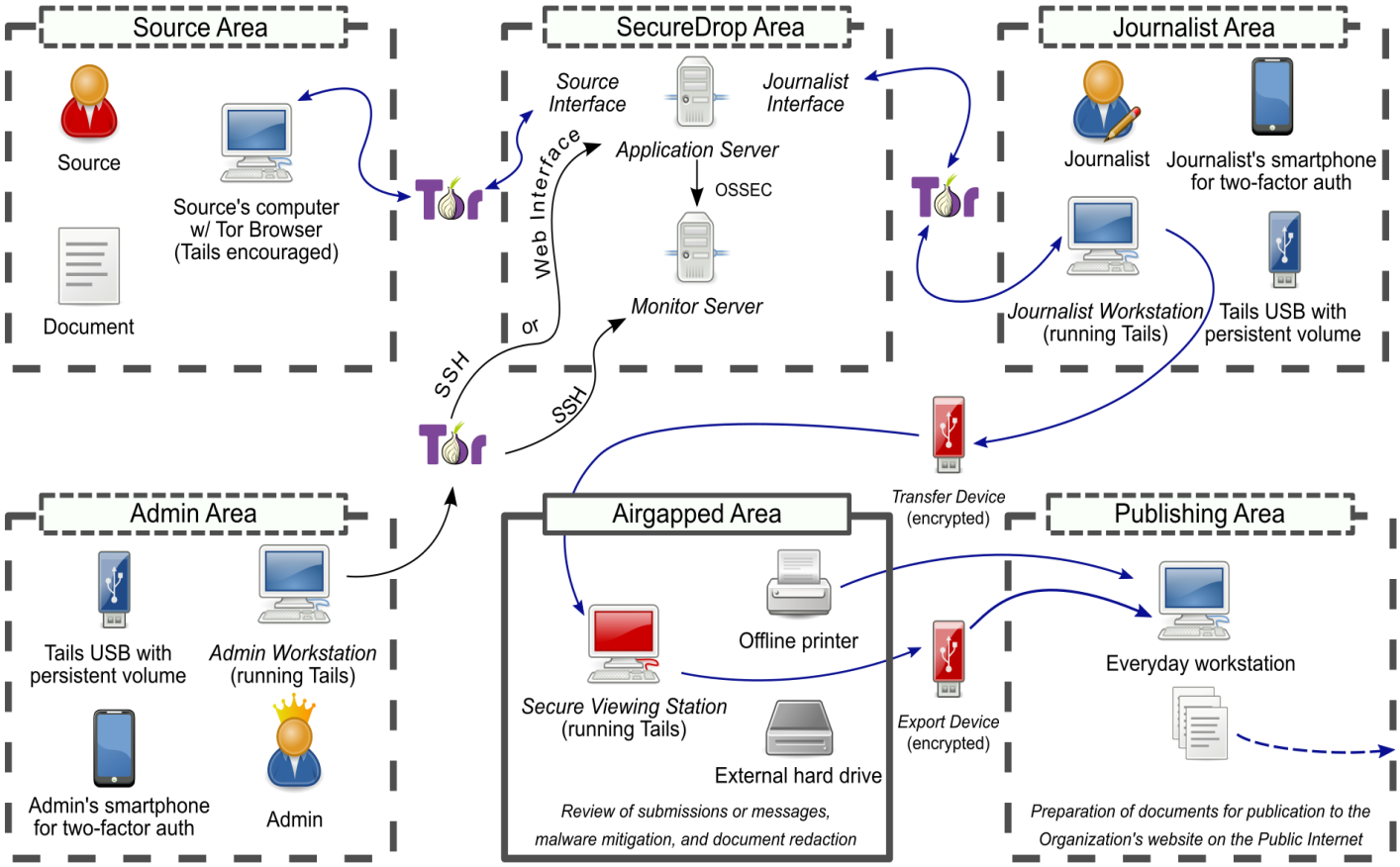
Glyn Moody, autor de *Rebel Code* y periodista especializado en el campo tecnológico, argumenta en una videollamada desde Londres que el uso del código abierto es la esencia de la libertad y la privacidad. "Cualquier medio de comunicación serio debe tener una SecureDrop puesto que, si tienes aplicaciones defectuosas, el sistema será inseguro, por lo tanto, conocer los códigos de fuente abierta es importante y, repito, cualquier medio serio deberá tenerla", afirma.

La formación del periodista es indispensable para conocer estos detalles, "uno de los problemas es que la tecnología es muy complicada y los periodistas generalistas no son tan buenos para explicarla porque intentan resumirlo y dar una aproximación sin meterse en los detalles". Reniega de ello: "Con la tecnología tienes que preocuparte por los detalles". La exigencia diferenciará el compromiso de la empresa y la decisión o no de aceptar tener recursos acordes con los tiempos.

La privacidad viene dada por una serie de factores que se encadenan unos a otros para devenir en las grandes exclusivas de la última década que han cambiado por completo el devenir de la historia del periodismo de investigación.



Infografía del grupo Securedrop.org acerca del funcionamiento del sistema.



EL PERIODISMO DE INVESTIGACIÓN (DIGITAL)

Fotograma de la película Spotlight (McCarthy, 2015).

pISTA

pESQUISA NÓICACILBUp

El catedrático José Manuel de Pablos Coello de la Universidad de La Laguna hablaba de las 5P en el periodismo de investigación que se dan cuando el profesional decide indagar en algo que está oculto o que es *ocultado*. La razón última es el beneficio para los intereses informativos de los lectores y, ampliamente, de la opinión pública. El *watchdog*, en su papel de observador del poder y defensor del sistema democrático, intentará revelar y agitar de tal manera el debate público que transformará la agenda mediática.

La disciplina periodística recapacita, contrasta, verifica y cuestiona las "verdades" promulgadas por los distintos actores de la sociedad.

El equipo se esfuerza por demostrar la autenticidad de la filtración. De otra forma, sería solo un rumor. Las generaciones pasadas vieron *Todos los hombres del presidente* (Pakula, 1976), y ahora, sin perder de vista *Spotlight* (McCarthy, 2015), la realidad se acerca a *Citizenfour* (Poitras, 2014), donde las llaves son cantidades pesadas de datos virtuales y quien las porta un objetivo localizado.

pRESIÓN

pRISIÓN

El informe *Protecting Journalism Sources in the Digital Age* de la UNESCO de 2017 da un amplio abanico de perspectivas mediante diversos estudios. El del Pew Research Certer da que un 64% de los periodistas de investigación encuestados creen que el gobierno estadounidense recogió datos de sus comunicaciones. Los efectos directos de las apreciaciones son la pérdida de confianza de las fuentes, unido al hecho de que es más difícil entablar canales de comunicación seguros con ellas. El texto achaca la desactualización tecnológica de los periodistas como una costosa mella en las posibles alianzas. Con ello, la legislación torna hacia otros caminos para definir qué proteger y qué no (periodismo ciudadano,

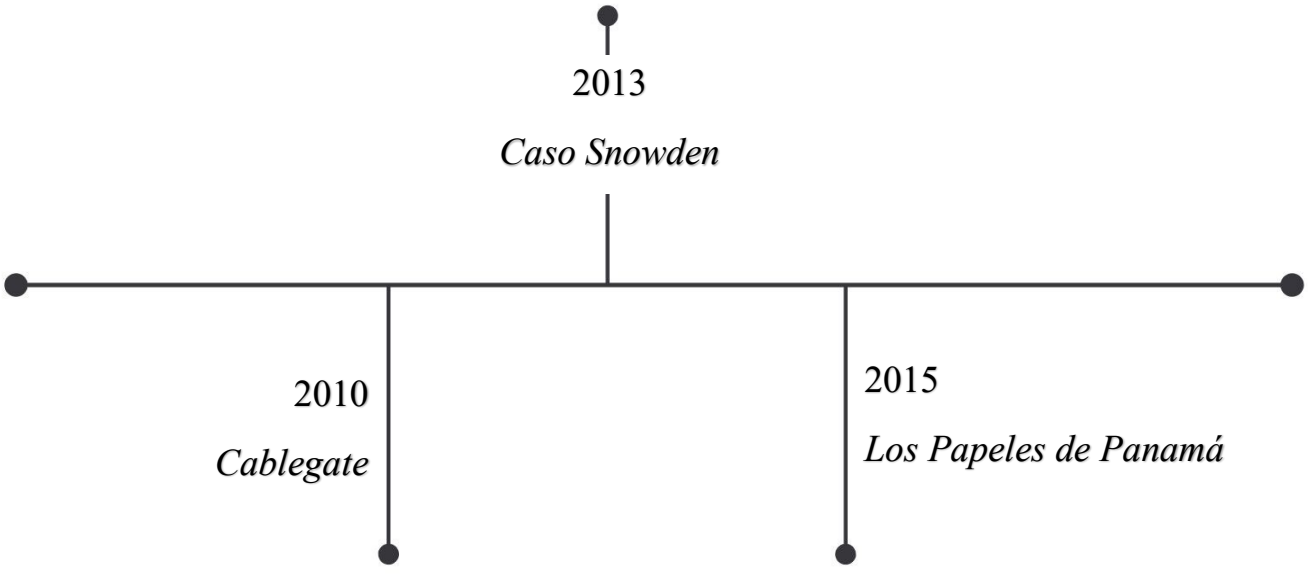
ciudadanía que hace sus alegatos en redes sociales, informáticos, activistas, periodistas…), y el estudio apunta hacia *los actos de periodismo* en vez del título académico. Lo que no da lugar a discusión es que la confidencialidad de las fuentes periodísticas en la era digital es determinante.

La distopía más plausible. Por ello, la formación y la capacitación de los periodistas es cada vez más acuciante para demostrar que, gracias a la *deep* web, la criptografía y los recursos disponibles en seguridad y privacidad digital forman un armazón resistente para los tiempos venideros.

Hay tres casos que demuestran que el periodismo de investigación es una de las mayores contribuciones al bienestar colectivo y que las medidas para combatir la vigilancia masiva son solo el principio de una larga lucha cibernética.

"Internet, nuestra mayor herramienta de emancipación, se ha transformado en la facilitadora más peligrosa del totalitarismo jamás vista. Internet es una amenaza para la civilización humana (…)"

Julian Assange, *Cypherpunks* (2012)



Los cables de WikiLeaks

28 de noviembre de 2010. *The New York Times*, *The Guardian*, *Der Spiegel*, *Le Monde* y *El País* publican simultáneamente los *Papeles del Departamento de Estado* (*Cablegate*). Wikileaks filtró más de 250.000 documentos que comprometían las relaciones diplomáticas de Washington con el resto del mundo. Misiones, despropósitos, amenazas e influencias son descubiertas y la cabeza de turco es el programador, activista y periodista Julian Assange, editor y portavoz de Wikileaks. Los archivos abarcan el lapso desde diciembre de 1966 hasta febrero de 2010.

Wikileaks fue fundada en 2007 y, bajo el lema *We open gobernments*, dio el golpe con la publicación de las estrategias militares en Irak, y luego, con el foco encima, salió a la luz el vídeo que reflejaba el asesinato de 12 personas en Bagdad desde dos helicópteros estadounidenses AH-64-Apache. El siguiente paso consistió en dos filtraciones masivas de 76.607 informes de la guerra de Afganistán en julio y de 391.832 documentos de Irak en octubre de 2010. El *Cablegate* se distinguió por darle a los medios la información previa.

El agujero del sistema por el que se había colado WikiLeaks era Siprnet (Secret Internet Protocol Router Network), una red interna del Ejército norteamericano puesta tras el 11-S. Según detallaban los informes, unas 180 embajadas estadounidenses hacían uso de ese protocolo al que accedían unos 3 millones de empleados, lo cual provocaba serias deficiencias de seguridad.

De repente, en un momento marcado aún por la crisis de 2008 que sometía a la ciudadanía a una crudeza sin precedentes, se ponía en tela de juicio la fiabilidad y reputación de las relaciones diplomáticas. Ninguna autoridad puso en duda la veracidad de estos documentos. Hillary Clinton, como secretaria de Estado de la administración Obama, declaró que esas revelaciones eran un ataque a la comunidad internacional. Los implicados salieron de forma virulenta y acalorada a tachar de desleales a quienes difundieran el material, incluida la prensa. La coordinación entre las cabeceras internacionales y la confianza depositada desde Wikileaks en ellas puso de manifiesto la labor de selección y depuración periodística, obviando aquellos textos en los que peligraran vidas.

Perfil de Julian Assange. Recuperado de *El mundo del abogado*.

The New York Times DER SPIEGEL The Guardian

EL PAÍS Le Monde

Los daños colaterales no se hicieron esperar. La web sin ánimo de lucro estaba financiada por donaciones y, desde ese instante, hubo tal campaña de desprestigio que Bank of America, VISA, Mastercard, PayPal y Western Union le cancelaron sus cuentas. En contrapartida, Anonymous organizó un ataque cibernético contra las entidades.

La otra cara visible es la de Chelsea Manning. Una de las filtradoras de los *Cables*, la soldado y analista de inteligencia, entabló la comunicación mediante las herramientas de la plataforma. Al ser descubierta, estuvo tres años en prisión provisional hasta que el Pentágono la acusó formalmente. La condena dictó, en 2013, pena de 35 años y expulsión del cuerpo por deshonor. Más tarde, Obama conmutaría el resto de su condena. Sin embargo, al negarse a declarar en el juicio de Wikileaks, volvió a prisión en 2019, con intento de suicidio incluido. Una informadora sentenciada.

Como Assange. El ciberactivista permaneció desde 2012 hasta el año pasado en la embajada de Ecuador en Londres en calidad de asilo político para no ser extraditado a EE.UU., al tiempo que era acusado de delitos sexuales en Suecia. La Primera Enmienda de la Constitución de los Estados Unidos está en entredicho. Barton Gellman, periodista que lideró la cobertura del *Caso Snowden* en el *Washington Post*, en una entrevista a *The Guardian* mostraba su preocupación por el precedente que supondría en la jurisprudencia norteamericana de sentar a Assange en el banquillo. Al fin y al cabo, como él describe, el informático es acusado por preguntar, recibir y publicar información, a lo que Gellman se dedica y por lo que no ha sido perseguido. Son más de veinte cargos los que imputan a Assange y su extradición de Londres a Estados Unidos —que en el momento en que se escribe este texto aún no ha ocurrido— supone, para su abogado Baltasar Garzón, en una tribuna de *El País*, el sacrificio de la transparencia en aras de la seguridad nacional, dejando a la prensa en una honda crisis que socavaría su papel como fiscalizador del poder.

Por su parte, el mencionado periodista Glyn Moody critica la exposición indiscriminada que Wikileaks hizo de otros cables, como los correos de Hillary Clinton que afectaron a la campaña presidencial contra Donald Trump, “estaban tan emocionados por difundirlos sin pensar cuál serían las consecuencias, no dieron un paso atrás, hablando con periodistas; al contrario que sí hizo Snowden, que tenía en cuenta las consecuencias personales y totales”. La balanza del periodista es la diferencia, insiste.

En plena tormenta, un análisis de Javier Moreno, director de *El País* en ese momento, rezaba así: “Los periódicos tenemos muchas obligaciones en una sociedad democrática: la responsabilidad, la veracidad, el equilibrio y el compromiso con los ciudadanos. Entre ellas no se encuentra la de proteger a los Gobiernos, y al poder en general, de revelaciones embarazosas”.

Las consecuencias legales aún están en el aire.

Chelsea Manning en una charla. EFE. Recuperado de *El Periódico*.

Snowden vs. NSA

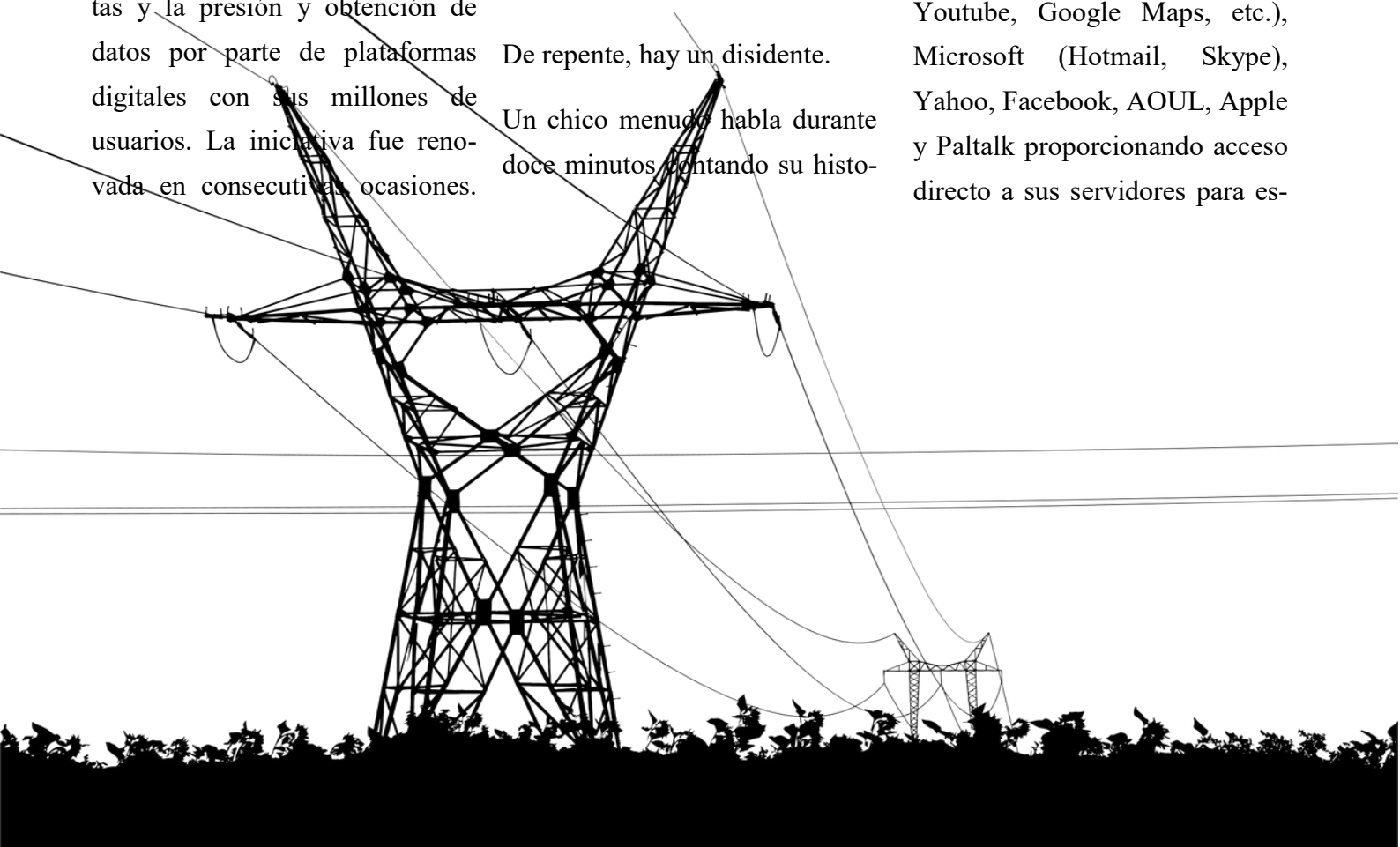
El 11-S es sinónimo de conmoción. El atentado propulsó la entrada de leyes restrictivas y amenazantes para la integridad de la privacidad, cuyo ejemplo más debatido es la *USA Patriot Act*. La ley fue aprobada el 26 de octubre de 2001 como un escudo al que el miedo y el odio ya habían partido por la mitad.

En ella, se aprobaban las prácticas de espionaje masivo de la NSA. Un *hackeo* indiscriminado en pos de información que comprometiera las estrategias terroristas y la presión y obtención de datos por parte de plataformas digitales con sus millones de usuarios. La iniciativa fue renovada en consecutivas ocasiones. Ahora está en el aire, esperando a una nueva prórroga en el Capitolio. A la saga de legislaciones represivas se sumaron la *Intelligence Service Act* de Alemania, la *Investigatory Powers Act* del Reino Unido, la cual fue condenada por el Tribunal Europeo de DDHH por violación de los derechos humanos, y la *Assistance and Access Act* de Australia. El denominador común de los textos jurídicos está en el respaldo al escrutinio de los canales de comunicación. Todas ellas firmadas después del escándalo Snowden.

Un detalle: la *Patriot Act* prohíbe a todo individuo u organización revelar que ha entregado datos al Gobierno federal.

De repente, hay un disidente.

Un chico menudo habla durante doce minutos contando su historia en *The Guardian*. Él es quien ha puesto toda la carne del asador en manos de los periodistas Glenn Greenwald, Ewen MacAskill y la documentalista Laura Poitras. Era el 5 de junio de 2013 y Edward Snowden desveló la mayor filtración acaecida hasta entonces: el programa PRISM había sido utilizado por la NSA para espiar los teléfonos de millones de americanos. Ya no se trataba de los países extranjeros, a quienes la *Foreign Intelligence Surveillance* permite vigilar, sino de sus propios vecinos, amigos, familiares, comunidad. A la traición se sumó el descubrimiento de la cooperación de Google (Gmail, G+, Youtube, Google Maps, etc.), Microsoft (Hotmail, Skype), Yahoo, Facebook, AOUL, Apple y Paltalk proporcionando acceso directo a sus servidores para es-



Edward Snowden junto a los periodistas Glenn Greenwald y Ewen MacAskill durante sus reuniones. Imagen perteneciente al documental *Citizenfour* de Laura Poitras, grabado *in situ* durante los primeros estadios de la investigación periodística.

piar a los usuarios en tiempo real. El montante ascendió a 3.000 millones de documentos en solo un mes alrededor del globo. Y todo se hubiera ido al traste porque un periodista no quería encriptar sus correos.

Glenn Greenwald contaba que al recibir el primer día de diciembre de 2012 una nota de alguien anónimo pidiéndole su clave pública de PGP para mantener una conversación, declinó la propuesta. Esto era lo que le pedía Snowden. El informático siguió insistiéndole al periodista enviándole una especie de tutoría para que aprendiera mientras escribía los correos en mitad de la noche, sirviéndose del wifi de desconocidos para no ser interceptado. Volvió a ignorarlo, y la fuente, ante el silencio, decidió optar por comunicarse con Laura Poitras, quien había aprendido estas técnicas de seguridad digital desde que fue marcada como SSSS (Secondary Security Screening Selection) por el gobierno estadounidense al grabar unas imágenes en Bagdad durante el rodaje de una de sus últimos largometrajes.

Las escuchas masivas de la NSA recopilaban cualquier información de ciudadanía extranjera y estadounidense

Los algoritmos que codificaron su diálogo con Poitras fueron de 4.096 y 8.192 *bits*, es decir, el nivel de dificultad para desentrañar el contenido de los mensajes era superlativo y hubiera hecho falta, con la tecnología de entonces, billones de años en desmantelar la clave.

Durante aquellas incursiones, Snowden mantuvo el anonimato en la red con la conexión a internet ajena. Optó por instalarse la función TAILS en un ordenador, que burlaba la MAC y ocultaba su rastro con el añadido de la disponibilidad de la red Tor.

Las razones que llevaron a Snowden a convertirse en un filtrador las fundamenta en su biografía haciendo una comparación entre el Gran Cortafuegos de China y la infraestructura de telecomunicaciones del país al que solía servir. Era imposible que su gobierno obtuviese tanta información sin que hubiera hecho lo mismo que las restrictivas medidas de la nación asiática, el principio tecnológico de “si algo puede hacerse, probablemente se hará y seguramente ya se haya hecho” reverberaba en su cabeza. El

gigante asiático constriñe la libertad de su ciudadanía entre los muros que ha alzado en las últimas dos décadas con el conocido como *cortafuegos chino*, y Snowden concebía la vigilancia estadounidense como una especie de infraestructura accesible, sin bloqueos ni filtros, donde las restricciones de cada individuo dependieran de sus países de residencia y de las empresas, es decir, aquellos que se hubieran convertido en objetivos de vigilancia por haber hecho mala *praxis* virtual como consultar páginas web de fabricación de bombas yihadistas.

Los documentos clasificados como ECI (*Exceptionally Controlled Information*) que encontró en su trabajo en la NSA por casualidad demostraban lo contrario. Decidió sacar la información de allí. El duplicado, comprimido, encriptado y traslado a un lugar seguro fue hecho en tarjetas SD (Secure Digital) mini y micro, las de las cámaras fotográficas. El exanalista de inteligencia ha pedido una prórroga de tres años en Rusia, país en el que reside desde la filtración, acusado por delito es espionaje y por el que le podría caer cadena perpetua.

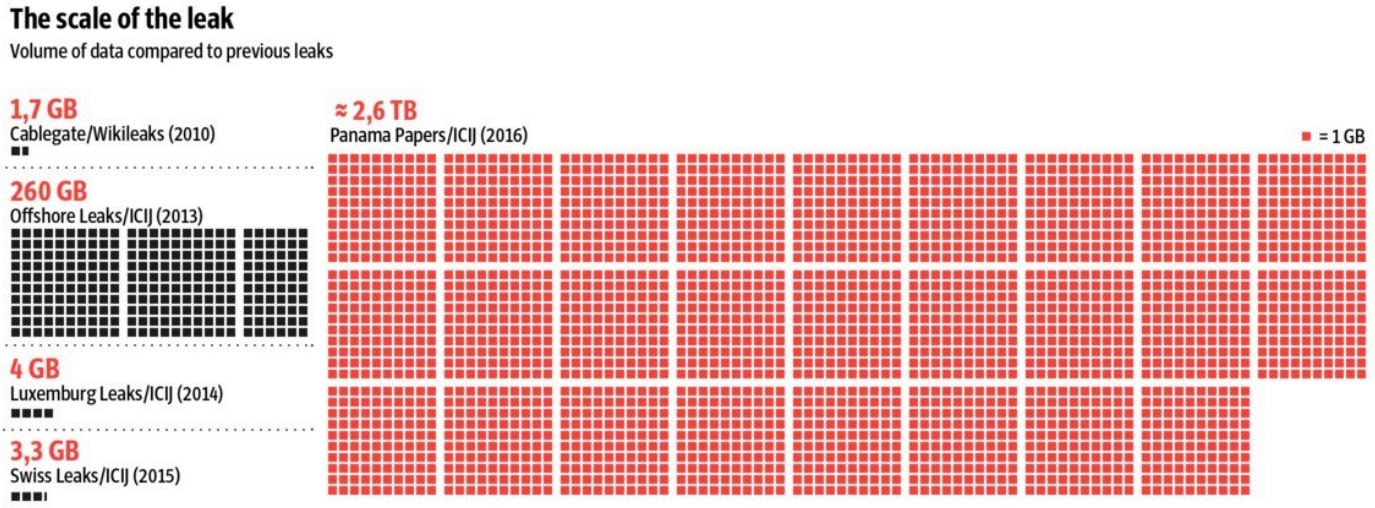
El Parlamento europeo aprobó en mayo de 2019 una ley para la protección de las fuentes y dio como margen de dos años su adaptación en sus estados miembros. En este caso, España es el primer país que lo propuso un mes más tarde gracias a Xnet, miembro de la WIN (Whistleblowing International Network), con la proposición de Ley de Protección Integral de Alertadores.

La función de los periodistas de investigación en este caso ha sido señalar y enfocar las contradicciones de un supuesto sistema benévolo para la población, haciendo rendir cuentas a los implicados.

Snowden decidió desvelar su identidad, podría no haberlo hecho, como John Doe.

> "El informado es una persona que, tras pasar por una dura experiencia, ha llegado a la conclusión de que su vida dentro de una institución se ha hecho incompatible con los principios desarrollados en el conjunto de la sociedad que está fuera de ella, y con la lealtad debida a dicha sociedad, cuestión por la que esa institución debería rendir cuenta; la persona es consciente de que no puede permanecer en la institución, y sabe además que la institución no se puede desmantelar, o que no va a hacerse tal cosa. Sin embargo, considera que la institución sí podría reformarse, así que da el soplo y revela la información pertinente para incorporar el factor de la presión pública"
>
> Edward Snowden,
> *Vigilancia permanente*, 2019.

Los Papeles de Panamá, el periodismo es colectivo



Cantidad de datos manejados durante la investigación de los Papeles de Panamá. Fuente: ICIJ

Parecía que no quedaba más motivos para sorprenderse, y es cuando la International Consortium of Investigative Journalists (ICIJ), una plataforma que reúne a más de 370 periodistas de unos 80 países, hace uso de la tecnología de encriptación para trabajar durante meses en los cables dados por una fuente anónima. Son los *Papeles de Panamá*. El mayor *cable* de la historia del periodismo pesaba 2,6 TB.

En julio de 2015 una serie de reportajes fueron publicándose acerca de los más de 11,5 millones de documentos internos del despacho de abogados panameño Mossack Fonseca, empresa en el top cinco de sociedades *offshore.* A los papeles tuvieron acceso los reporteros Bastian Obermayer y Frederik Obermaier del periódico alemán *Süddeustche Zeitung*. En las filas del ICIJ estaban los medios españoles *El Confidencial* y *La Sexta.*

Correos electrónicos, cuentas bancarias, bases de datos, pasaportes y registros de clientes del despacho, cientos de piezas que revelaron 214.488 paraísos *offshore* en alrededor de 200 países. La firma era conocida por la evasión de impuestos y blanqueo de dinero e implicaba a políticos, celebridades, traficantes de armas, miembros de la élite global y del mundo de los negocios. La investigación del ICIJ supuso un año entero de análisis. Costoso, a nivel empresarial y personal, la inversión se tradujo, entre otras cosas, en un equipo de ingenieros que habilitó una intranet para el trabajo simultáneo de los periodistas implicados en la distancia. Con esa cantidad de gente implicada, el secreto y el compromiso por mantenerlo fue la única salvaguarda de la misión.

Un mensaje:

Hello. This is John Doe. Interested in data?

Bastian Obermayer, del *Süddeustche Zeitung*, fue el periodista que lo recibió. Después de cinco años, la pandemia mundial de la Covid-19 acampa y en pleno confinamiento las coberturas que cubrir se multiplican, pero podrá sacar algunos minutos. “Nadie estaba preparado para una fuga masiva como este caso, pero tuvimos a unos fantásticos periodistas de datos que nos ayudaron a darle sentido a esta montaña de da-

Bastian Obermayer, periodista del *Süddeutsche Zeitung*. Fuente: NCBJ

tos", afirma.

"Al comunicarse vía *online* no puedes asumir el mismo nivel de confianza con la fuente, y su ventaja es, probablemente, la seguridad"

John Doe no ha revelado su identidad y transmitió el tesoro que portaba de manera segura. La fiabilidad de los informadores digitales se basa en la confianza y, por supuesto, en la verificación: "No hay como conocerse en persona, pero, cuando la fuente contactó conmigo, no nos encontramos, no hablamos, solo nos comunicábamos vía *online*", asume, "así que es posible y, a veces, es la mejor opción. No obstante, generalmente, no es lo que preferimos debido a que, entre las desventajas, no puedes asumir el mismo nivel de confianza y su ventaja es, probablemente, la seguridad". Él, ella, quién sabe.

Asimismo, el director del ICIJ Gerard Riley, en una entrevista a *Wired,* ponía distancias con Wikileaks al decir que no iban a exponer de manera indiscriminada los datos, "estamos intentando demostrar que el periodismo se puede hacer con responsabilidad".

La ICIJ reserva un apartado especial para el contacto de las fuentes en su página web y da diferentes recursos: la SecureDrop, el email encriptado con llaves PGP -las que Greenwald tanto le había costado asimilar-, la aplicación móvil Signal, la mensajería de WhatsApp, la alternativa Wire, Telegram, el Keybase para transmitir documentación y que asegura el anonimato en los servidores y, a falta de una opción mejor, el código postal. Obermayer asume que la facilitación de una vía anónima y segura es responsabilidad del periodista, quien ha de proporcionar el canal como lo que comenta acerca de la SecureDrop, "it's the state of the art", es decir, *lo último*.

Mar Cabra, periodista implicada durante la investigación, reflexionó en la charla TEDxSanFrancisco *Our democracy depends on what and how we archive and share data* el vertiginoso cambio de los roles en los medios de comunicación. La exclusiva, la competencia entre cabeceras, la reserva de compartir determinados datos o sucesos son cuestiones que quedan relegadas ante la magnitud del evento. La imparable corriente de información diaria que sirve para ampliar y sobreexplotar los horizontes de la investigación son un obstáculo con el que tiene que lidiar el periodista. Esa razón, a las que se une la lentitud debido a los horarios, requerimientos, cuestiones de última hora, hace que el periodismo de investigación asuma la organización colectiva para buscar una solución a la minería de datos.

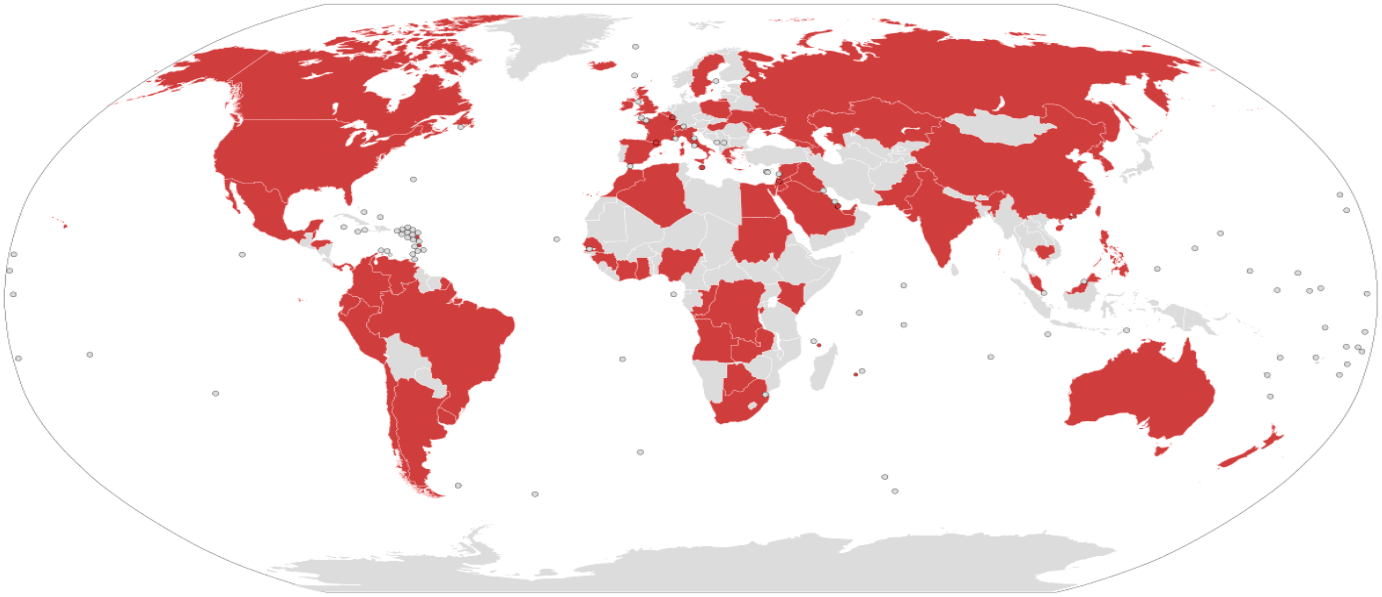
Obermayer se muestra cauto si hablamos de era *dorada* del periodismo de investigación. Depende. "Si los medios gestionan el sustento de su apoyo financiero y mantienen las respectivas publicaciones vivas, estoy de acuerdo. Hay mucho que ganar ahí afuera, y en la época digital es mucho más fácil. También, la colaboración internacional ayuda mucho. Pero si la crisis financiera echa abajo demasiadas publicaciones, pues me temo que queda un som-

Edificio en el que se encuentra el despacho Mossack Fonseca. Recuperado de *El Confidencial*.

brío futuro por delante". Un consejo para las futuras generaciones de periodistas: "Como siempre, mantenerse crítico y escéptico".

En mayo de 2016, John Doe, la fuente anónima, emitió un comunicado tras las repercusiones acaecidas en la fiscalidad global. Reafirmó su independencia y mostró su compromiso ético al entender las injusticias descritas en los papeles que estaban en su poder. A pesar de todo, la nefasta cobertura legislativa que existe en la actualidad para la protección de informadores que desvelan secretos por la mejora de la sociedad no tiene fin. Doe no es más que un ciudadano, una ciudadana, que busca justicia, y termina:

"La próxima revolución será digitalizada. O quizás esa revolución acaba de empezar"



Infografía con la cantidad de países afectados, por ahora, por la investigación de los Papeles de Panamá. Fuente: ICIJ

Una redacción del siglo XX. Recuperado de *Jot Down Magazine*.

La alianza entre medios es indispensable desde el punto de vista investigativo para ser capaces y resolutivos en la confrontación de la magnitud de datos que se maneja gracias al *big data* y, y el uso de herramientas que garanticen la privacidad de los informantes y la operación de los periodistas es un imperativo.

El experto internacional en materia de libertad de expresión y regulación de medios Joan Barata habla desde Barcelona, está confinado, y eso no le impide vestir una camisa desde primera hora de la mañana. “Hay una cierta visión utópica de internet como un espacio transnacional, en el que no hay fronteras. Es al contrario, cada vez más estamos en un proceso de homogeneización y renacionalización de la regulación de la libertad de expresión”, observa. La legislación de cada estado afecta tanto a sus habitantes como a las empresas digitales que exploten sus recursos, “poco puede hacer estas plataformas globales para resistirse a las órdenes de un gobierno, como el de Turquía, que le dice a Facebook que tiene dos opciones: o quitar un contenido o que le cierre la conexión a internet, por lo que los turcos dejarán de tener acceso a su página”. Entiende que en España hay una cierta inadaptación a las nuevas formas de hacer periodismo y entender sus implicaciones tecnológicas, “por ejemplo, en *The Guardian* hace un curso de capacitación de comunicación sin riesgos con informantes”.

La línea que separa mundo virtual y mundo real es inexistente. “Lo que es legal *offline* lo es también *online*, y viceversa, no hagamos distinciones extrañas”, añade Barata, “es verdad que hay realidades que hasta ahora no estaban contempladas por la legislación, como las redes sociales, pero internet no es un medio de comunicación. Internet es una plataforma donde la vida sucede”, y amplifica las

acciones. “Desde el punto de vista político y regulatorio lo importante es el principio de neutralidad tecnológica, es el servicio que se emplea lo que se regula”.

Los tres grandes hitos del periodismo de investigación mencionados demuestran el alcance de la vigilancia masiva y las oportunidades y riesgos que supone la época digital tanto para el tratamiento como difusión de datos. Oportunidades y dificultades muestran una era conflictiva, tal vez como cualquier etapa anterior, pero los derechos sociales, económicos y políticos adquiridos hasta la fecha no son comparables a ningún otro período histórico y la difusión y alcance del conocimiento están a un solo clic de distancia. El periodista alemán Bastian Obermayer comenta que es difícil, en retrospectiva, hacer un análisis de lo acaecido desde la publicación de los Papeles de Panamá: “Al fin y al cabo, somos una sociedad que está mejor informada sobre qué es lo que pasa detrás de las escenas, y esto es una cuestión buena y realmente importante. ¿Somos mejor sociedad por ello? No creo que ninguna investigación pueda cambiar la naturaleza humana…”.

Berners-Lee, en una entrevista a *Vanify Fair,* anunció la construcción de Solid, cuya meta es descentralizar la red, “estoy resentido del control corporativo sobre la gente y en sus vidas, odio la sociedad de la vigilancia que accidentalmente pusimos sobre nosotros”. Sin embargo, las propuestas de los sectores críticos basadas en el *suicidio digital* o la *ofuscación* no son posibles en términos globales debido a que la sociedad depende por evolución y extensión de los recursos internautas, sea la comunicación vía redes sociales, aplicaciones, procesos administrativos, políticos y económicos, que permuta el control y el espionaje de las grandes tecnológicas y de los gobiernos. El cambio será estructural y paulatino mientras el periodismo siga buscando la verdad.

Impelidos a sumergirnos en la esfera digital, unos principios para aquellos periodistas que en la práctica deseen ser parte activa, y oculta.

“Internet es una plataforma donde la vida sucede”

Redacción renovada de *El País*.

Lee, aprende y fórmate

La UNESCO, Reporteros Sin Fronteras, el Citizen Lab de la Universidad de Toronto, el National Whistleblower Center, el Knight Center, Restor Privacy y miles de asociaciones dan soporte gratuito y *online* para obtener recursos educativos en materia de seguridad digital para el ejercicio periodístico.

Borra tu huella digital

Historiales, contraseñas guardadas en el navegador, memorias, cookies… Que quede vacío. Por ello, la navegación segura a través de Tor Browser o de la instalación de una VPN son esenciales.

Encripta

La seguridad en las conversaciones con tus fuentes anónimas son tu responsabilidad. Aplicaciones como Signal, Wire, el uso de PGP, de Https Everywhere y las SecureDrop, entre otras, ofrecen una fuerte encriptación.

Convence

Los medios de comunicación y las redacciones son parte esencial del cambio tecnológico de la profesión, por ello, explicar y mostrar los beneficios de la preocupación digital es esencial para la mejora conjunta.

Lucha por el interés público

La legislación mundial es un campo amplio donde la libertad de prensa y expresión y la evolución tecnológica están íntimamente relacionadas. Informarse y conocer las diatribas de estas cuestiones es responsabilidad del periodista, que ha de trasladar con suma claridad y exactitud la información a sus lectores. La obtención de una sociedad bien informada radica en el compromiso de su periodismo.

El periodismo del siglo XXI tratará de cómo escapar a la vigilancia masiva

Anexo

Bibliografía:

- Assange, J. (2012). *Cypherpunks. La libertad y el futuro de internet*. Deusto.
- Caminos, J. (1997). Periodismo de filtración, periodismo de investigación. *Revista de Estudios de Comunicación*, 2 (2). Recuperado de: https://www.ehu.eus/ojs/index.php/Zer/article/view/17303/15097
- Comisión Europea. (2014). La política y la gobernanza de Internet. El papel de Europa en la configuración de la gobernanza de Internet, Comunicación de la comisión al Parlamento europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones. Recuperado de: file:///C:/Users/acer/Documents/1.%20UNIVERSIDAD/4%C2%BA/1.%20TFG/BIBLIOGRAF%C3%8DA/CELEX_52014DC0072R(01)_ES_TXT.pdf
- Contreras, F. (2001). Internet: la red en España. *Revista Latina de Comunicación Social*, 37. Recuperado de: https://mdc.ulpgc.es/digital/document/content/rldcs_335
- Cotino, L. (editor). (2011). *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, PUV (Publicaciones de la Universidad de Valencia): Valencia. Recuperado de: file:///C:/Users/acer/Documents/1.%20UNIVERSIDAD/4%C2%BA/1.%20TFG/BIBLIOGRAF%C3%8DA/ART%C3%8DCULOS%20Y%20LIBROS/elibertades2010.pdf
- Ball, J., Schneier, B., Greenwald, G. (2013, 4, octubre). NSA and GCHQ target Tor network that protects anonymity of web users, *The Guardian*. Recuperado de: https://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption
- Eichengreen, B., Lafarguette, R., Mehl, A. (2016). Cables sharks and servers. Technology and the geography of the foreign exchange market, *EU Publications*, nº 1889. Recuperado de: https://op.europa.eu/en/publication-detail/-/publication/82b44372-0dcc-11e6-ba9a-01aa75ed71a1/language-en/format-PDF/source-130202467
- El Confidencial. (2016, 6, mayo). Habla la fuente de los papeles de Panamá: por qué filtré la información, *El Confidencial*. Recuperado de: https://www.elconfidencial.com/economia/papeles-panama/2016-05-06/papeles-panama-papers-fuente-anonima-denunciante-filtrador-john-doe_1195990/
- García, M. J. (2013). La prohibición de la censura en la era digital. *Teoría y realidad constitucional*, 31, pp. 237-276. Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=4263213
- Henrichsen, J., Betz, M., Lisosku, J. (2016). *Cómo desarrollar la seguridad digital para el periodismo*, UNESCO. Recuperado de: file:///C:/Users/acer/Documents/1.%20UNIVERSIDAD/4%C2%BA/1.%20TFG/BIBLIOGRAF%C3%8DA/C%C3%B3mo%20desarrollar%20la%20seguridad%20digital%20para%20los%20periodistas%20-UNESCO.pdf
- Hyperion Gray. (2020) [Página web]. Recuperado de: https://www.hyperiongray.com/dark-web-map/
- Index: coommunity/policies Tor. (2020) [Página web]. Disponible en: https://gitweb.torproject.org/community/policies.git/tree/statement_of_values.txt
- Instituto Nacional de Estadística. (2019). Encuesta sobre equipamiento y uso de tecnologías de información y comunicación en los hogares, Instito Nacional de Estadística. Recuperado de: https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735976608

- Is software more vulnerable today? (12 de marzo de 2018). En *European Union Agency for Cybersecurity*. Recuperado de: https://www.enisa.europa.eu/publications/info-notes/is-software-more-vulnerable-today
- Ivanova, I. (2018). *Informe especial, La banda ancha en los Estados miembros de la UE: pese a los avances, no se cumplirán todos los objetivos de la Estrategia Europa 2020*. Recuperado de: https://www.eca.europa.eu/Lists/ECADocuments/SR18_12/SR_BROADBAND_ES.pdf
- Klein, D. (2001). El papel del periodismo de investigación en la sociedad democrática. *Razón y palabra*, 29 (2). Recuperado de: http://www.razonypalabra.org.mx/anteriores/n22/22_dklein.html
- La Rue, F. (2011). *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*. Recuperado de: file:///C:/Users/acer/Documents/1.%20UNIVERSIDAD/4%C2%BA/1.%20TFG/BIBLIOGRAF%C3%8DA/Relator%20sobre%20el%20control%20en%20internet.pdf
- Mayorga, T., García, M., Duret, J., Carrión, J., Yarad, P. (2019) Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos. *Dominio de las ciencias*, 5 (1), pp. 518-537. Recuperado de: file:///C:/Users/acer/Downloads/Dialnet-HistoriaDeLaNormativaReguladoraDeLaProteccionDeDat-6869937.pdf
- Moreno, J. (2010, 19, diciembre). Lo que de verdad ocultan los Gobiernos, *El País*. Recuperado de: https://elpais.com/internacional/2010/12/18/actualidad/1292626823_850215.html
- Pablos Coello, J. (1998). Periodismo de investigación: las cinco fases P. *Revista Latina de Comunicación Social*, 9. Recuperado de: http://www.ull.es/publicaciones/latina/a/475fp.htm
- Peirano, M. (2019). *El enemigo conoce el Sistema: manipulación de ideas, personas e influencias después de la economía de la atención*. Barcelona: Debate.
- Peirano, M. (2015). *El pequeño libro rojo del activista en la red*. Eldiario.es. Recuperado de: http://index-of.es/Deep%20Web/Cybermedios/manual-antispy-pequeno-libro-rojo-del-activista-marta-peirano.pdf
- Posetti, J. (2017). *Protecting Journalism Sources in the Digital Age,* UNESCO. Recuperado de: file:///C:/Users/acer/Downloads/UN_Protecting_sources_in_the_digital_age_book%20(1).pdf
- Reporteros sin fronteras. (2011). *Censura y vigilancia de periodistas: un negocio sin escrúpulos*. Recuperado de: file:///C:/Users/acer/Downloads/rapport_cs_es_.pdf
- Salazar, Idoia. (2005, 16, octubre). El Inmenso Océano Del Internet Profundo, *El País.* Recuperado de: https://elpais.com/diario/2005/10/20/ciberpais/1129772426_850215.html
- Sarabia, D. (2018, 13, septiembre). Reino Unido violó los derechos humanos con sus programas de vigilancia masiva, *eldiario.es*. Recuperado de: https://www.eldiario.es/tecnologia/privacidad/Reino-Unido-derechos-programas-vigilancia_0_814018994.html
- Secure Drop (2020) [Página web]. Disponible en: https://securedrop.org/
- Suárez, S. (2019). *Big data, poder y libertad. Sobre el impacto social y político de la vigilancia masiva*. Universitat Pompeu Fabra. Recuperado de: https://www.tdx.cat/handle/10803/668235#page=217
- Snowden, E. (2019). *Vigilancia permanente*. Planeta.
- Sumbarine Cable Map (2020) [Página web]. Disponible en: https://www.submarinecablemap.com/

- Tedx Talks [Tedx Talks]. (31 de octubre de 2017). Our democracy depends on what and how we archive and share data. Mar Cabra. TEDxSanFrancisco. Recuperado de: https://www.youtube.com/watch?v=r1kjgoC_o4M
- The Hidden Wiki. (2019) [Página web]. Disponible en: https://thehiddenwiki.org/
- The Journal of electronic publishing. (2001). White paper: the deep web: surfacing hidden value. *Taking License*, 7 (1). Recuperado de: https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main#fn14-ptr1
- The value of personal online data. (23 de abril de 2018). En *European Union Agency for Cybersecurity*. Recuperado de: https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data/
- The World Wide Web Consortium (W3C) (2020) [Página web]. Disponible en: https://www.w3.org/Consortium/
- Tor Project. (2020) [Página web]. Disponible en: https://blog.torproject.org/
- Tor Metrics. (2020) [Página web]. Disponible en: https://metrics.torproject.org/