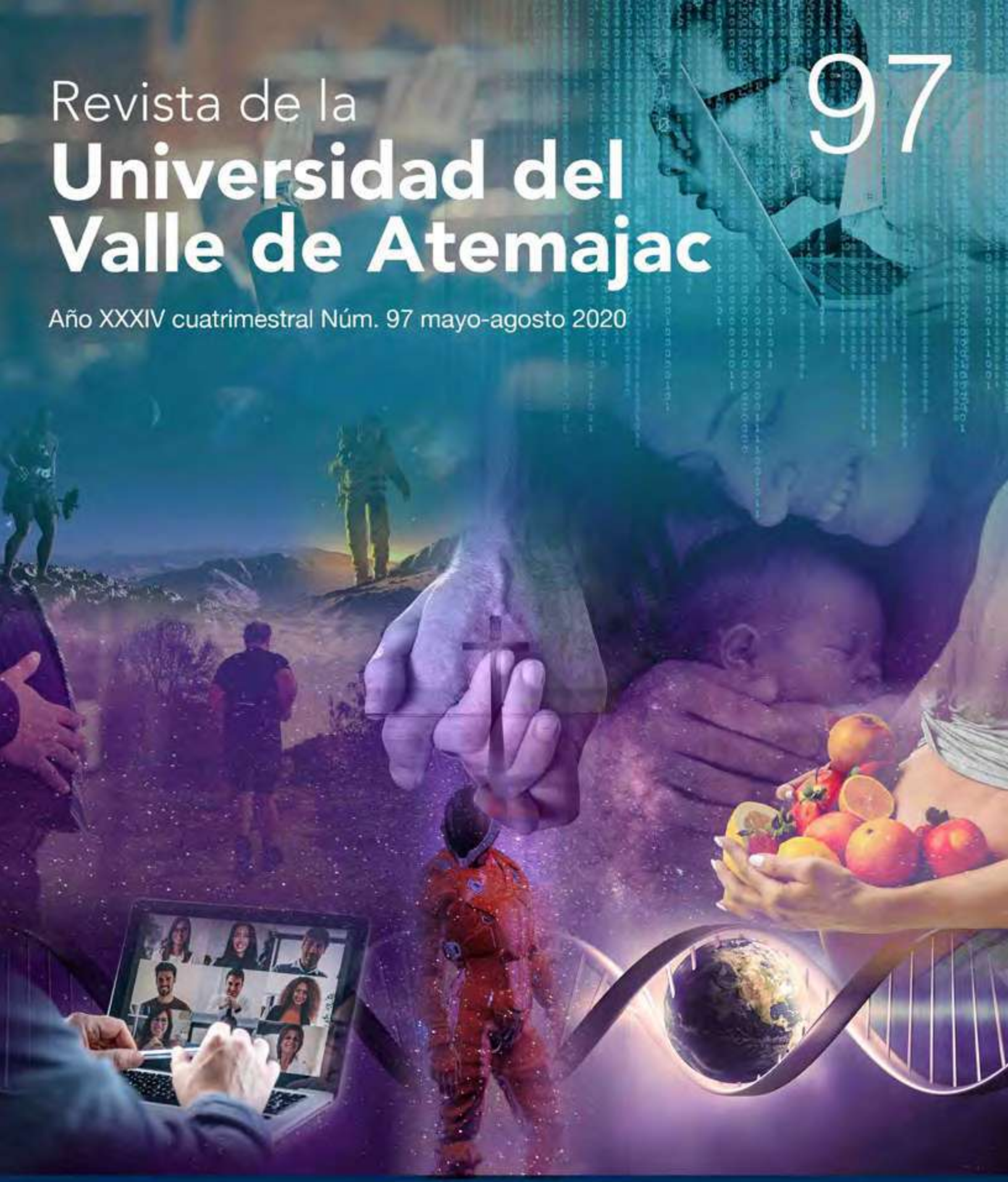


Revista de la

Universidad del Valle de Atemajac

97

Año XXXIV cuatrimestral Núm. 97 mayo-agosto 2020

UNIVA
La Universidad Católica

DIRECTORIO

Año XXXIV, Núm. 97; mayo-agosto 2020

Portada
Coordinación de Imagen Corporativa

Colaboran en esta edición
Ernesto Roque Rodríguez
Susana Romo Wierches
Mauricio Leija Esparza
Alba Gloria Arias Ibáñez
María del Carmen Castro Saldaña
Sergio Ellerbracke Román
Elba Lomelí Mijes
Ana Rocío Castañón Arteaga
Luis Ángel Osorio
Jorge Antonio Llamas Navarro
Miguel Ángel Zamora Vega

ISSN 0187-5981
Publicación cuatrimestral, indizada en CLASE
http://dgb.unam.mx

La Revista de la Universidad del Valle de Atemajac, año XXXIV, no. 97, mayo-agosto 2020, es una publicación cuatrimestral editada por la Universidad del Valle de Atemajac; avenida Tepeyac No. 4800, fraccionamiento Prados Tepeyac; Zapopan, Jalisco, México. C.P. 45050. Tel. (33) 3134 0800, Ext. 1735, www.univa.mx/publicaciones/coleccion.php. Editor responsable: Saúl Raymundo López Cervantes. Reserva de derechos al Uso Exclusivo No. 04 – 2017 – 070311535500 - 102, ISSN. 0187-5981, ambos otorgados por el Instituto Nacional de Derechos de Autor. Licitud de Título y Contenido en trámite, otorgada por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación.

Correo electrónico: saul.lopez@univa.mx **Página Web:** www.univa.mx/publicaciones/coleccion.php.

SUMARIO

El movimiento social hacker Whistleblower: contexto, evolución y coyuntura.

Sergio Ellerbracke Román
Profesor del Centro de Enseñanza Técnica Industrial y egresado del Doctorado en Ciencias del Desarrollo Humano de la Universidad del Valle de Atemajac.

Elba Lomelí Mijes
Profesor-Investigador del Departamento de Geografía y Ordenación del Territorio, y egresada del Doctorado en Ciencias del Desarrollo Humano de la Universidad del Valle de Atemajac.

La posmodernidad ha influido sobre los movimientos sociales. Por un lado los movimientos sociales tradicionales ahora colaboran mediante la red, y se comunican interna y externamente por medio de redes sociales y, por otro lado han surgido nuevos movimientos sociales, deslocalizados y sin una dirigencia central. En esta nueva categoría de movimientos sociales estarían los movimientos ecologistas, los globalifóbicos, los consumidores indignados (que luchan contra la obsolescencia programada, consecuencia del diseño de productos de baja duración), y los hacktivismos.

Resumen

Un movimiento hacker es un movimiento social que surge de las tecnologías de la computación y que se opone a estrategias perversas de grandes ejércitos, corporaciones y gobiernos. Un hacktivista se enfrenta a una realidad que no acepta, creando un sistema que haga obsoleta dicha realidad. Bajo estas definiciones, en años recientes los autores de este artículo hemos articulado una taxonomía de nueve movimientos sociales hacker: *whistleblower, criptolibertarios, anti RFID, consumidores indignados, anarquistas, libres, wikipedianos, DOAJ y cruncher*. En este trabajo nos centramos especialmente en los whistleblower, movimiento que se relaciona e identifica con la coyuntura generada por la detención de Julian Assange en Londres, la cual tiene como finalidad su extradición a los Estados Unidos. En este trabajo se presenta un análisis de la evolución de los whistleblower y una conclusión con escenarios en que puede derivar del caso de Julian Assange.

Palabras Clave:
Whistleblower | Julian Assange | Hacktivismo | Wikileaks | Chelsea Manning.

The Whistleblower social movement: context, evolution and juncture

Summary

A hacker movement is a social movement that arises from computer technologies and opposes the perverse strategies of large armies, corporations and governments. A hacktivist faces a reality that he/she does not accept, creating a system that makes that reality obsolete. Under these definitions, in recent years the authors of this article have articulated a taxonomy of nine social hacker movements: whistleblower, crypto-liberals, anti-RFID, outraged consumers, anarchists, free, wikipedians, DOAJ, and cruncher. In this paper we focus especially on whistleblowers, a movement that is related and identified with the situation generated by the arrest of Julian Assange in London, which aims at his extradition to the United States. This paper presents an analysis of the evolution of whistleblowers and a conclusion with different scenarios in which the case of Julian Assange can be derived.

Keywords: Whistleblower | Julian Assange | Hacktivism | Wikileaks | Chelsea Manning | Edward Snowden.

Le mouvement social hacker Whistleblower: le contexte, l'évolution et la conjoncture

Résumé

Le mouvement hacker est un mouvement social qui émerge des technologies de l'informatique et qui s'oppose aux stratégies perverses de grands méchants, corporations et gouvernements.
Une hacktiviste est confrontée à une réalité qu'elle n'accepte pas, cette hacktiviste fait un système qui rend obsolète la réalité dont on parle. Selon ces définitions, ces dernières années les auteurs de cet article, nous avons énoncé une taxonomie de neuf mouvements sociaux hacker: le whistleblower,les cripto libertarios, l'anti RFID, les consommateurs indignés, les anarchistes, les libres, les wikipédiafs, le DOAJ et le cruncher. Dans cette étude, nous allons nous concentrer spécialement sur les whistleblower, un mouvement qui s'identifie et est lié à la conjoncture générée par l'arrestation de Julian Assange à Londres, afin de l'extrader vers les États-Unis. Dans ce travail, on présente une analyse sur l'évolution des Whistleblower et une conclusion avec les différents scénarios qui pourrait emmener au cas de Julian Assange.

Mots clés: Whistleblower | Julian Assange | Hacktivismo | Wikileaks | Chelsea Manning | Edward Snowden.

La posmodernidad ha influido sobre los movimientos sociales. Por un lado los movimientos sociales tradicionales ahora colaboran mediante la red, y se comunican interna y externamente por medio de redes sociales y, por otro lado han surgido nuevos movimientos sociales, deslocalizados y sin una dirigencia central. En esta nueva categoría de movimientos sociales estarían los movimientos ecologistas, los globalifóbicos, los consumidores indignados (que luchan contra la obsolescencia programada, consecuencia del diseño de productos de baja duración), y los hacktivismos. Estos movimientos representan la mejor propuesta tanto hacia la dignificación de una política desprestigiada, corrupta e inoperante -la política de los partidos políticos en crisis-, así como en contra de la economía del capitalismo salvaje.

Los autores hemos intentado caracterizar y delimitar una amalgama de movimientos sociales que tienen en común un origen derivado de las tecnologías de la computación, el software y la electrónica, los cuales denominamos movimientos hacker. Estos se oponen a estrategias de ejércitos, corporaciones y gobiernos. Son meritocracias, responden a la ética y trabajan de manera distribuida, en red. Los hacktivistas son luchadores sociales que utilizan la tecnología para enfrentarse a injusticias. Un hacktivista se enfrenta a una realidad que no acepta creando un sistema que haga obsoleta dicha realidad.

De esta forma, hemos aglutinado un conjunto de movimientos sociales hacker: algunos de ellos operando en la legalidad, otros criminalizados. Algunos con una enorme visibilidad mediática, otros apenas conocidos. Algunos cuyos integrantes se definen en términos de su hacktivismo, otros cuyos integrantes no son plenamente conscientes de que forman parte de un movimiento social. Algunos con estructuras administrativas y financieras que garantizan su permanencia y desarrollo, otros que apenas subsisten. Algunos en la escala de los millones o cientos de miles de integrantes, otros en la escala de las decenas o centenares de luchadores sociales. Algunos con enormes avances en su agenda, otros con avance incipiente. Algunos construyen, otros boicotean.

En esta heterogeneidad de movimientos sociales hacker, presentamos nuestra propuesta de un espectro hacktivista compuesto por *whistleblower, criptolibertarios, anti ubicación, consumidores indignados, anarquistas, libres, wikipedianos, DOAJ y cruncher.*

En el presente trabajo nos concentraremos en el movimiento social whistleblower, uno de los movimientos sociales hacker de mayor cobertura mediática. Pero primero necesitamos una visión de conjunto,

y para ello debemos encuadrar a los whistleblower dentro del espectro hacktivista.

Por lo tanto, nos enfocaremos en la evolución de los hacker whistleblower, dando al final un énfasis en la coyuntura que se abre con la detención de Assange en Londres y su proceso de extradición a Estados Unidos.

El espectro hacktivista

Como un punto de partida, para Manuel Castells (2001, pp. 92-93) -quien trabaja a partir de la definición de Touraine- un movimiento social se caracteriza por la identidad del movimiento, el adversario del movimiento y la visión o modelo social del movimiento.

Comencemos con lo más importante: la identidad. Aplicando la definición de Castells-Touraine, para el caso de los movimientos hacker, se puede observar que obtienen su identidad a partir de tres perspectivas:

En este enfoque la visión de los movimientos hacker es la construcción de software, información o fármacos, públicos y libres, desarrollados mediante redes de personas que colaboran entre sí. Son actores importantes en la construcción de alternativas al estado actual de la globalización

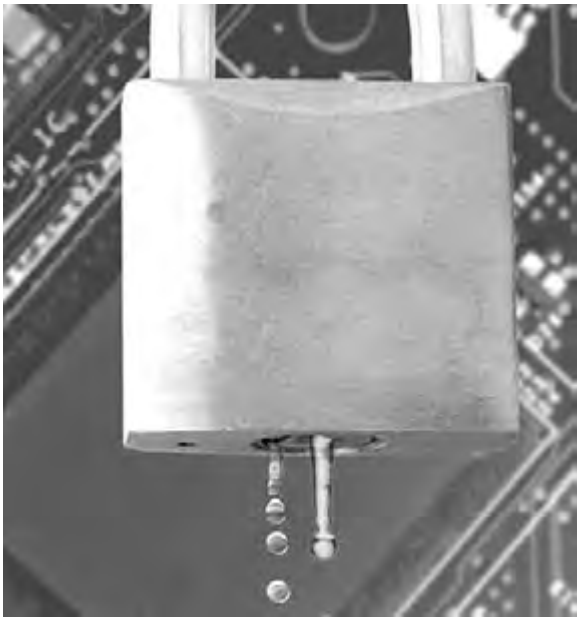
1. En una primera vertiente, algunos movimientos hacker construyen su identidad al concebir al software y a la información como bienes públicos, colocando a sus adversarios en las empresas que afirman su propiedad privada del software o la información, o que han realizado ataques a los bienes públicos. En este enfoque la visión de los movimientos hacker es la construcción de software, información o fármacos, públicos y libres, desarrollados mediante redes de personas que colaboran entre sí. Son actores importantes en la construcción de alternativas al estado actual de la globalización. Aquí entran los libres, wikipedianos, DOAJ, cruncher y anarquistas.
2. En segundo lugar, algunos movimientos hacker van a obtener su identidad de la protección de la privacidad, ante los abusos en la vigilancia del gobierno hacia los ciudadanos. La protección de la privacidad está vinculada permanente con el pacifismo, pero también con los movimientos sociales, con el periodismo libre y con la aplicación de reglas justas en el comercio internacional. La cuestión es que debido al carácter belicoso de Estados Unidos en alianza con Reino Unido, Australia, Canadá y Nueva Zelanda (conocidos como los cinco ojos), ha operado por décadas una red global que intercepta las comunicaciones del planeta. Es la única forma eficiente en que se puede espiar a los *objetivos* (ejércitos y gobiernos) seleccionados. Pero ya hicieron el gasto y ya tienen la información, así que es posible autorizar el acceso a las comunicaciones de cualquier periodista, luchador social o empresa. En la vertiente de protección de la privacidad se encuadran los whistleblower, criptolibertarios, y anti ubicación.
3. Para el caso particular de los consumidores indignados, la identidad se construye ante el reconocimiento del hecho de que en amplias categorías de hardware y software, la innovación tecnológica ha dejado de ser el motor del desarrollo de esos tipos de hardware y software, y la importancia objetiva de dicha innovación tecnológica es residual. El problema es que las corporaciones que fabrican esos hardware y software, han incorporado técnicas de obsolescencia programada que reducen la duración del hardware y software. Los consumidores indignados se integran al movimiento ecologista y al desarrollo, en general, de productos diseñados para su perduración y no para su obsolescencia.

En Ellerbracke y Lomelí (2019), es posible consultar una tabla más amplia de nuestra caracterización de los movimientos sociales hacker.

Los whistleblower (una traducción aceptable sería alertador, aunque también se conocen como filtrador, delator de ilegalidades y revelador de secretos; aquí se usará whistleblower, alertador o filtrador, indistintamente) constituyen el origen de los hacktivismos orientados hacia la protección de la privacidad.

El movimiento hacker whistleblower

Los whistleblower (una traducción aceptable sería *alertador*, aunque también se conocen como filtrador, delator de ilegalidades y revelador de secretos; aquí se usará whistleblower, alertador o filtrador, indistintamente) constituyen el origen de los hacktivismos orientados hacia la protección de la privacidad. Una definición propia de whistleblower sería: una persona que conoce hechos secretos, que: son constitutivos de delitos; representan riesgos para la sociedad; son fraudulentos y decide dar a conocer estos hechos ante la sociedad civil, ante los medios de comunicación o ante organismos públicos.



El concepto whistleblowing (de *whistle* (silbato) y *blowing* (soplar)), fue acuñado por Ralph Nader, en 1972, como "Un acto de un hombre o mujer que, creyendo que el interés público anula el interés de la organización a la que sirve, hace sonar el silbato de que la organización está involucrada en actividades corruptas, ilegales, fraudulentas o dañinas" (Nader, 1972, citado en Banisar, 2011). Nader pretendía crear un concepto que no tuviera las connotaciones negativas frecuentemente aplicadas a las personas que hacían pública información secreta, como soplón, informante, delator, chivato o traidor. Nader extendió el sentido de whistleblower, a simplemente ser el de una persona que hacía sonar un silbato, entre ellos los árbitros de diferentes deportes, que suenan el silbato para sancionar una jugada sucia, dado que sólo es permisible el juego limpio (*fair play*).

Por supuesto, la prensa siempre ha estado vinculada con filtraciones y hay una tradición muy importante de proteger las fuentes.

Los hacker whistleblower han sido los personajes por los cuales ahora el conocimiento criptográfico es público, así como se conoce la dimensión del eavesdropping. Si a eso le sumamos las filtraciones de corrupción, es obvio porqué los gobiernos les tienen tanto miedo a los alertadores.

Ahora bien, sólo nos concentraremos en los whistleblower que han sido centrales para el desarrollo del pensamiento hacker. En particular, hasta mediados de los sesenta, los gobiernos y los ejércitos habían sido exitosos para ocultar el conocimiento criptográfico. Además, el gobierno estadounidense y sus aliados (Reino Unido, Canadá, Australia y Nueva Zelanda, conocidos como los *cinco ojos*), habían sido exitosos para ocultar el *eavesdropping* (interceptación y escucha silenciosa de comunicaciones) que realizaban (y siguen realizando) a todo el mundo (incluyendo a sus ciudadanos). Los hacker whistleblower han sido los personajes por los cuales ahora el conocimiento criptográfico es público, así como se conoce la dimensión del *eavesdropping*. Si a eso le sumamos las filtraciones de corrupción, es obvio porqué los gobiernos les tienen tanto miedo a los alertadores. Los whistleblower tienen que formar un binomio con periodistas. En el caso de los hacker whistleblower, los nombres más conocidos son Daniel Ellsberg, Chelsea Manning y Edward Snowden, y los periodistas más relevantes son Neil Sheehan, Ben Bagdikian, David Kahn, James Bamford, Julian Assange y Glenn Greenwald.

Como punto de arranque, en Septiembre de 1960, dos agentes de la Agencia Nacional de Seguridad (NSA), Bernon Mitchell y William Martin, desertaron y se presentaron ante la prensa mundial en la casa de los periodistas, en Moscú.

Los soviéticos organizaron una gran conferencia de prensa. Martin y Mitchell manifestaron que ellos habían decidido viajar a Rusia para decirle al mundo lo que sabían, conscientes de que la organización donde habían trabajado estaba empujando al mundo hacia la Tercera Guerra Mundial. Dijeron que habían trabajado por años en una gigantesca organización estadounidense, una tal *National Security Agency*, que tenía más de dos mil estaciones de interceptación de mensajes electromagnéticos en el mundo, que trabajaba coordinadamente con el británico GCHQ (*Government Communications Headquarters*), que interceptaban comunicaciones de todos lados, y que habían logrado romper las comunicaciones encriptadas de cuarenta naciones.

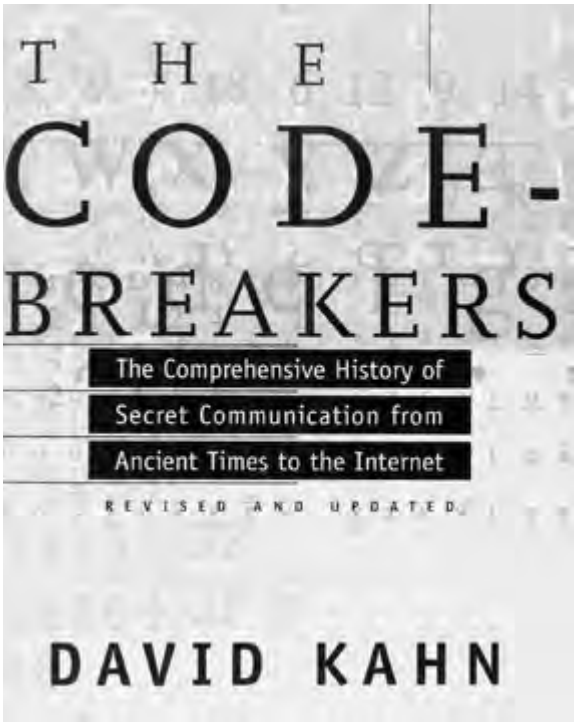
A continuación, Víctor Hamilton, otro agente de la NSA, también desertó hacia Moscú. El reportaje de ocho columnas del periódico *Izvestia* informó que Hamilton trabajaba en el sector de oriente próximo de la NSA, que abarcaba a la U.A.R., Siria, Iraq, Líbano, Jordania, Arabia Saudita, Yemen, Libia, Marruecos, Túnez, Turquía, Irán, Grecia y Etiopía. Hamilton informó que rutinariamente interceptaban, rompían la criptografía y analizaban los mensajes tanto militares como diplomáticos de esas naciones, incluyendo las representaciones diplomáticas de esas naciones en el mundo y de manera especial las comunicaciones de los representantes en la ONU.

A partir de las declaraciones de Martin y Mitchell, David Kahn, un académico/periodista, decidió dedicar los siguientes siete años de su vida a escribir un libro que se convertiría en objeto de culto por los hacker y que lo cambiaría todo: *The Codebreakers*.

The Codebreakers, publicado en 1967, es una historia de la criptografía, desde la antigüedad hasta el nivel alcanzado en ese momento. Es un libro académico, pero bien escrito, tanto como para ser nominado al

premio Pullitzer (Kahn, 2008). Aunque no lo escribió un ingeniero, sino un historiador, tuvo rigor científico y estilo periodístico, de manera que un ingeniero podía programar criptografía robusta a partir de la sola lectura del libro, y eso, en 1967, era revolucionario.

The Codebreakers aportó un capítulo completo sobre la *National Security Agency*. Este capítulo fue el primer trabajo serio sobre la NSA. La NSA fue creada en 1952, y se ubicó en un terreno de 82 acres. En esas instalaciones laboraban entre diez mil y catorce mil personas. Por lo menos otro millar de agentes de la NSA trabajaban en instalaciones fuera de los Estados Unidos (Kahn, 1973: 375-380). En la NSA existían más de dos mil estaciones de interceptación de comunicaciones electrónicas, la mayoría de ellas en bases militares estadounidenses, pero también a bordo de aviones y barcos (Kahn, 1973: 388).



El siguiente hito provino de Daniel Ellsberg, quien era un funcionario de muy alto nivel del Departamento de Defensa, que coordinó un estudio acerca de la toma de decisiones del gobierno de los Estados Unidos sobre Vietnam, abarcando el período de principios de los cuarenta hasta marzo de 1968 (Trzop, 2007: 9-10).

Ellsberg luego comentó que "al ver siete mil páginas de evidencia documentada de mentiras, por cuatro presidentes en 23 años, concibiendo planes y acciones de asesinatos masivos, decidí que debía detener el ocultamiento de esto, lo debía hacer de alguna manera" (Trzop, 2007: 10), y entregó una copia a Neil Sheehan, corresponsal del *New York Times*, y otra copia a Ben Bagdikian, del *Washington Post*, periódicos que publicaron sus reportajes. Aunque el gobierno de Nixon le prohibió a los periódicos la continuación de publicaciones, la corte suprema decidió en favor de ellos, privilegiando la primera enmienda (Trzop, 2007: 10-11). Los Pentagon Papers demostraban que la administración Johnson había mentido sistemáticamente, no sólo al pueblo estadounidense, sino al congreso. También dejaban mal paradas a las administraciones Kennedy y Nixon.

Los Pentagon Papers demostraban que la administración Johnson había mentido sistemáticamente, no sólo al pueblo estadounidense, sino al congreso. También dejaban mal paradas a las administraciones Kennedy y Nixon.

Posteriormente Perry Fellwock, un analista de la NSA en Estambul y en Vietnam, publicó una entrevista en la revista *Ramparts*. Tal vez estas revelaciones hayan sido un factor de primera importancia en evitar la tercera guerra mundial. De ese tamaño la hipérbole. Lo que afirmó fue: que la NSA rompía con facilidad todos los códigos de criptografía rusos; que habían replicado por completo el sistema de radares ruso, de manera que Estados Unidos contaba con pantallas que mostraban exactamente la misma información que veían los rusos a través de sus radares; que la NSA había logrado conocer y tener actualizada la ubicación y dirección de cada nave militar rusa, independientemente de que fuera avión, barco o submarino, información que se actualizaba las veinticuatro horas del día; que la mayoría de veces conocían las claves de cada avión, e incluso los nombres de cada piloto; que los barcos y submarinos rusos se movían en patrones predecibles, de manera que era posible encontrarlos incluso cuando se movían sin transmitir comunicaciones; que en la práctica el ejército soviético estaba totalmente orientado al aspecto defensivo y que carecía de capacidad ofensiva; que la embajada estadounidense en Moscú contaba con equipamiento para interceptar las comunicaciones electrónicas de dicha ciudad; y que las posiciones de barcos, avio-

"All the News That's Fit to Print"

The New York Times

LATE CITY EDITION

VOL. CXXII ... No. 42,312 NEW YORK, SATURDAY, MAY 13, 1972 15 CENTS

PENTAGON PAPERS CHARGES ARE DISMISSED; JUDGE BYRNE FREES ELLSBERG AND RUSSO, ASSAILS 'IMPROPER GOVERNMENT CONDUCT'

White House Says Attacks Will Continue in Cambodia

By BERNARD GWERTZMAN

GRAY CALL TO NIXON

Said to Inform Inquiry It Came 3 Weeks After Watergate

By ANTHONY RIPLEY

NEW TRIAL BARRED

But Decision Does Not Solve Constitutional Issues in Case

By MARTIN ARNOLD

Air of Expectancy, Then Tears, Shouts, Embraces

nes y submarinos rusos se calculaban al instante, con cualquier comunicación que emitieran dichas naves, mediante RDF (*Radio Direction Finding*) (Horowitz, 1972). Además, afirmaba que la NSA monitoreaba las llamadas telefónicas que los estadounidenses realizaban al exterior. Esta era la primera vez que se acusaba a la NSA de invadir la privacidad de los estadounidenses. Ya no se trataba de espionaje militar o diplomático, sino de una violación ilegal a la privacidad de cualquier estadounidense.

A partir de que la NSA estuviera violando la Constitución estadounidense y espiando a los estadounidenses, se conformaron tres comisiones del Senado: Church dirigió el Comité de Inteligencia del Senado, Abzug coordinó el Subcomité de Información Gubernamental y Derechos Individuales, y Pike encabezó el Comité Especial sobre Inteligencia. Los tres comités trabajaron simultáneamente, entre 1975 y 1976. La NSA fue obligada a dar audiencias, y los informes, hechos públicos -a pesar de la oposición del presidente Ford-, fueron muy críticos hacia la NSA.

A partir de entonces, James Bamford, doctor en derecho y periodista del *New York Times*, ha dedicado su vida al estudio de la NSA. De hecho, ha escrito cuatro libros. Más de 2000 páginas. Pero *The Puzzle Palace* (1983) se cuece aparte. Simplemente fue el primer libro de la NSA y el único por más de una década.

Lo primero es que la NSA surge en el más absoluto secreto, el 5 de noviembre de 1952, con un memorándum firmado por Truman el 24 de octubre de 1952, con diez mil empleados (Bamford, 1983, 15-17), en 1969 tenía 95,000 (Bamford: 108-109) y en 1978 tenía 68,203 empleados (Bamford: 17).

En las instalaciones había una *multitud de extrañas antenas*, entre ellos múltiples platos de microondas y antenas parabólicas, pero también antenas de otros tipos. Destacaban dos *radomos enormes*, uno parecía una pelota gigante de golf, y otro una pelota gigante de ping pong. (Bamford: 1983).

Ahora bien, antes de que la NSA pueda atacar un código o leer un mensaje, primero debe ser capaz de capturar y registrar la señal. Pero eso no lo hace directamente la NSA, sino el CSS Central Security Service, una organización tan secreta como la NSA, con presupuesto e instalaciones independientes. Son las estaciones de interceptación de comunicaciones. Hay muchas fotografías en internet de estas instalaciones: algunas con múltiples radomos (como enormes pelotas de ping pong). Son protecciones para que no se vean las antenas que hay dentro de ellas. El plan de la NSA, de mediados de los cincuenta (*Intercept Deployment Plan (IDP)*), tenía el objetivo de instalar 4,120 estaciones de escucha, por todo el mundo (Bamford: 204-210).

Adicionalmente al CSS, en 1961, la Agencia Central de Inteligencia (CIA) y la Fuerza Aérea crearon una oficina para ejecutar el programa espía de satélites. Es la NRO *National Reconnaissance Office,* otra agencia negra, cuya sola existencia debía ser negada por el gobierno (*Bamford*: 243).

Con respecto a los telegramas, operaba el programa SHAMROCK. La RCA (*Radio Corporation of America*), en Nueva York, a partir de 1963, le entregaba diario a la NSA cintas magnéticas con la totalidad de telegramas del día anterior. Cada día se buscaban "ciertas palabras, frases, nombres, localidades, remitentes o direcciones, o cualquier combinación de estos elementos" y se imprimían los telegramas que tenían coincidencias con las palabras de búsqueda. El programa operaba antes de 1963, pero a partir de este año se automatizó totalmente (*Bamford*: 312-313).

Otro programa ilegal era MINARET, que tenía el propósito de reportar las comunicaciones de individuos u organizaciones involucradas en disturbios civiles, movimientos pacifistas o desertores militares involucrados en movimientos pacifistas (*Bamford*: 324).

Después de los comités del congreso, donde quedó clara la ilegalidad en la que operaba la NSA, lo que se ha visto es una serie de burlas a la ley en Estados Unidos. Así, mientras Carter, en 1978, en público, limitaba las atribuciones de la NSA para grabar indiscriminadamente las comunicaciones de los estadounidenses, cuatro años después Reagan, en privado, le permitió a la NSA volver a las anteriores prácticas (*Bamford*: 471). Y luego llegaron las órdenes FISA (*Foreign Intelligence Surveillance Act*), autorizadas por el congreso y el presidente Carter en 1978, otorgadas por una corte federal súper secreta (*Bamford*: 462-463), que en la práctica legalizaban lo ilegal, pero violando el espíritu de la ley.

La relevancia de la aportación de Julian Assange

Desde 1996 existe *cryptome* (https://cryptome.org/), pero esta organización no tiene las funciones de análisis y verificación de documentos, previos a su liberación. Simplemente recibe documentos y si se ha pagado una aportación de cien dólares, se tiene la clave para desencriptar cualquier documento del depósito.

Wikileaks, que comenzó a operar en 1996, fue la primera plataforma mediática que permitía un anonimato absoluto al momento de enviar una filtración. Anteriormente, el whistleblower debía ponerse en contacto con el periodista, y eso podía implicar un riesgo importante si era parte de una organización que vigilara permanentemente a sus integrantes o si el periodista era vigilado.

Wikileaks, que comenzó a operar en 1996, fue la primera plataforma mediática que permitía un anonimato absoluto al momento de enviar una filtración. Anteriormente, el whistleblower debía ponerse en contacto con el periodista, y eso podía implicar un riesgo importante si era parte de una organización que vigilara permanentemente a sus integrantes o si el periodista era vigilado.

Además, Wikileaks tuvo desde el principio la capacidad de *limpiar* los documentos digitales, para

proteger a la fuente (hay una variedad de controles de seguridad, como números de serie, puntos digitales o marcas de agua invisibles) que tienen el propósito de *marcar* un documento con metadatos del usuario responsable. El servidor de Wikileaks opera en la *Deep Web*, así que es inmune a ataques propios del Internet. Lo que se puede observar en https://wikileaks.org/, es simplemente uno de muchos espejos que tiene en internet el sitio de la *Deep Web*.

Los primeros *leaks* publicados nos dan una idea de lo heterogéneos que son los aludidos: un coronel somalí terrorista, un banquero suizo, un presidente keniano, la prisión de Guantánamo, la Cienciología y la lista de miembros de un grupo inglés de extrema derecha. El último *leak* es del 12 de noviembre de 2019, y son documentos de corrupción de una pesquera al gobierno de Namibia. Hay documentos que afectan lo mismo la inteligencia rusa que la alemana o a corporaciones como Amazon o Sony. En total, hay alrededor de 67 directorios de archivos. Sin duda el blanco más atacado es la CIA, ya que 27 de los directorios corresponden a la agencia, la mayor parte de ellos corresponden a las herramientas de hackeo de la CIA, publicados en 2017.

Las filtraciones de Chelsea Manning corresponden a los directorios *Iraq War Logs, Afghan War Logs, Collateral Murder,* y *Public Library of US Diplomacy*. La importancia de la filtración de Chelsea Manning simplemente no se puede regatear. Puso a trabajar frenéticamente a equipos de *The Guardian, The New York Times* y *Der Spiegel* por cinco meses y a equipos de *El País* y *Le Monde* por dos semanas. Nada más los periodistas de *The Guardian*, redactaron más de 160 artículos. La primera plana del *The Guardian* era: "Filtración cables embajadas Estados Unidos hace estallar crisis diplomática mundial". El ministro de relaciones italiano dijo: "Será el 11S de la diplomacia mundial". "Hablaban de ello en la Casa Blanca, el Kremlin, el Elíseo, habla Berlusconi y Naciones Unidas, Chávez, en Canberra, en todas las capitales del mundo … toda esta gente, estas personas increíblemente poderosas, las más poderosas del mundo, acudían a toda prisa a reuniones del comité de crisis" (Leigh, 2011: 221-224). Además, un mes después de la publicación de los cables, y por referencia a cables de corrupción tunecina, comenzó la Primavera Árabe (Leigh, 2011: 250).

Aparentemente, el resto de whistleblower que han enviado sus filtraciones a Wikileaks, permanecen en el anonimato. La plataforma funciona.

Y además, aunque Wikileaks llegara a desaparecer, ya existen otras plataformas mediáticas que garantizan un anonimato absoluto. Bajo la iniciativa

El periodismo independiente y los filtradores van a seguir funcionando. Además, a partir de la filtración de Edward Snowden, se originó The Intercept. Este sitio es tanto una revista electrónica con un flujo continuo de reportajes, como un depósito de documentos secretos, que publica nuevos documentos varias veces cada semana.

de *PubLeaks*, ya están en operación PubLeaks NL (The Netherlands), *MexicoLeaks*, *Leaks.ng* (Nigeria) e *Indonesialeaks*. El periodismo independiente y los filtradores van a seguir funcionando. Además, a partir de la filtración de Edward Snowden, se originó *The Intercept*. Este sitio es tanto una revista electrónica con un flujo continuo de reportajes, como un depósito de documentos secretos, que publica nuevos documentos varias veces cada semana.

La gran filtración: Edward Snowden

La filtración de Edward Snowden es la mayor de la historia. Snowden fue un agente que trabajó tanto para la NSA como para la CIA (y en las instalaciones de Microsoft) (Greenwald, 2014: 65, 143). Snowden se fue contra la yugular del imperio: había que asfixiar a la NSA. El jueves 6 de junio de 2013, el titular de *The Guardian* decía "La NSA obtiene a diario registros telefónicos de millones de clientes de Verizon", con un enlace a la orden FISA correspondiente. Era la primera vez que se veía una orden FISA. Los medios estadounidenses no hablaban de otra cosa. También era la nota en la prensa del mundo. El titular del viernes 7 de junio era: "El programa PRISM de la NSA accede a datos de usuarios de Apple, Google y otros". También fue la primera plana del *Washington Post*. Era la recogida mundial de datos de los usuarios del internet, los correos electrónicos, las búsquedas…, por *Microsoft (Hotmail…,), Google (Gmail…,), Yahoo, Facebook, PalTalk, YouTube, Skype, AOL y Apple*. La NSA y el gobierno estadounidense, acorralados. Las empresas, aterrorizadas. Los usuarios, traicionados, enojados al ver los logotipos de sus proveedores de servicios en un documento TOP SECRET//SI//ORCON//NOFORN. El siguiente titular de *The Guardian* fue mediáticamente el menos abordado (comparado con los titulares del día precedente y del día posterior), pero es de interés tanto para la comunidad de la seguridad informática como para los militares. El titular era: "Obama ordena preparar una lista global para ciberataques", e indicaba cómo se pueden desarrollar futuras guerras en las que Estados Unidos esté involucrado, mediante OCEO (*Offensive Cyber Effects Operations*), donde los ciberataques buscarán "el uso de electromagnetismo o de energía dirigida a controlar el espectro electromagnético para atacar al enemigo".

El cuarto titular era "Informante sin límites", donde "se describían los métodos según los cuales la NSA recogía, analizaba y almacenaba miles de millones de llamadas telefónicas y correos electrónicos enviados a través de la infraestructura de comunicaciones norteamericana". El último titular de *The Guardian* apareció el domingo 9 de junio: "Edward Snowden: el denunciante tras las revelaciones de vigilancia de la NSA", acompañado por un video de doce minutos, elaborado por Laura Poitras (Greenwald, 2014: 91-107, 137).

Conclusiones

A partir de la filtración de Manning, la mayor desde Ellsberg, cambió dramáticamente la diplomacia mundial. Si le quitas a un diplomático la decencia ¿Qué le queda? ¿Cómo es posible la diplomacia *post Manning*? También es más difícil que militares disparen sus ametralladoras contra automóviles con periodistas y civiles, una vez que cualquiera puede ver *collateral murder*. El poder absoluto corrompe absolutamente. Son indispensables los contrapesos.

Pero, el *eavesdropping* es un problema que va en aumento, ya que no sólo proviene de la NSA/cinco ojos, sino que muchos gobiernos nacionales espían a sus ciudadanos. El mercado mundial de la ciberseguridad fue de 75,000 millones de dólares en 2015 y la estimación para el 2020 es de 170,000 millones de dólares (IEI, 2017), una gran parte de ese presupuesto lo gastan los gobiernos.

Según *Pew Research* (2015), 87% de los estadounidenses están conscientes de los programas de vigilancia electrónica de la NSA. Aplicaron una encuesta en 43 países (excluyendo Estados Unidos) y encontraron una amplia oposición a este tipo de programas, tanto para los ciudadanos del país (81% contra 12%), sus líderes (73% contra 20%), como para ciudadanos estadounidenses (62% contra 31%). Sin embargo, en Estados Unidos la perspectiva fue diferente. Los partidarios de los demócratas estaban 48% en desacuerdo contra 47% de acuerdo, mientras que los partidarios de los republicanos estaban 56% en desacuerdo contra 41% de acuerdo. Y 52% de los estadounidenses estaban de acuerdo con espiar a líderes de otros países, contra un 43% en contra. Aún más, 93% de los estadounidenses quería tener control de su información personal, pero

sólo 9% tenía un buen control de su información. En síntesis, saben de la NSA, medio la toleran, pero no les gusta que tenga su información personal, aunque para una ligera mayoría no está mal que espíen a otros gobiernos.

¿Cómo logró la NSA ser relativamente aceptada por los estadounidenses? Por el uso del miedo. El terror es el miedo en su grado extremo y el discurso es que están en guerra contra el terrorismo.

Al Gore, ex vice presidente de los Estados Unidos, explica con claridad que los nuevos conocimientos neurológicos nos indican que la capacidad de sentir miedo está predeterminada en el cerebro, mientras que la razón está en una zona del cerebro de evolución más reciente: "Cuando el miedo es muy fuerte, basta para paralizar por completo nuestro proceso de razonamiento" (Gore, 2007: 41). Es perverso, pero tiene base científica y funciona.

Julian Assange está acusado por Estados Unidos de conspirar para recibir información de Defensa Nacional, siete cargos por obtener esa información, nueve cargos por revelar esta información y un cargo por conspirar para acceder a una computadora (BBC NEWS, 2019). Por esos cargos, Assange podría ser condenado a 175 años (MILENIO, 2019).

Julian Assange está acusado por Estados Unidos de conspirar para recibir información de Defensa Nacional, siete cargos por obtener esa información, nueve cargos por revelar esta información y un cargo por conspirar para acceder a una computadora (BBC NEWS, 2019). Por esos cargos, Assange podría ser condenado a 175 años (MILENIO, 2019).

Así que en el próximo juicio de Julian Assange en los Estados Unidos, podemos asistir a una intersección de posibles escenarios:

1. Como Assange tiene la razón jurídica de su lado, al haber tratado de proteger a su fuente, como cualquier periodista lo debe hacer, y protegido por las enmiendas constitucionales de libertad de expresión y libertad de prensa, Assange logre no ser declarado culpable y no purgar sentencias en cárceles estadounidenses.
2. Que el gobierno de Estados Unidos logre un juicio relativamente opaco y que el juicio no sea parte de las principales discusiones públicas, de forma que logre condenarlo penalmente en varios cargos y Assange permanezca preso en Estados Unidos, con un nivel de protesta que sea soportable para el gobierno.

3. Que el juicio de Julian Assange se le revierta al gobierno de los Estados Unidos, que se integre en la discusión pública estadounidense, y termine siendo un catalizador que promueva la protección a la privacidad.
4. Que la salud de Julian Assange se siga deteriorando dadas las condiciones en que permaneció en la embajada de Ecuador en Londres y su posterior confinamiento penal, al punto de la muerte de Assange.

Bibliografía

Bamford, J. (1983). The Puzzle Palace. From the Korean Airlines Incident to the Iran-Contra Affair to the Gulf War – New details of the NSA's secret role. New York: Penguin Books.

Banisar, D. (2011). Whistleblowing International Standards and Developments. En: Sandoval, I.E. (Ed.). (2011). Corruption and transparency: debating the frontiers between state, market and society. Washington: World Bank-Institute for Social Research UNAM. Disponible en: https://www.researchgate.net/publication/228124587_Whistleblowing_International_Standards_and_Developments.

BBC NEWS. (24 de mayo de 2019). Julian Assange: Estados Unidos acusa de 17 nuevos delitos al fundador de WikiLeaks. Disponible en https://www.bbc.com/mundo/noticias-internacional-48391860, el 16 de noviembre de 2019.

Castells, M. (2001). La Era de la Información. Vol. II: El poder de la identidad. México, Distrito Federal: Siglo XXI Editores.

Ellerbracke, S.A.; Lomelí-Mijes, E. (2019). Movimientos sociales hacker: contrapoder de la industria farmacéutica. Revista Científica Guillermo de Ockham 17(1), Universidad de San Buenaventura, Colombia. Disponible en: https://revistas.usb.edu.co/index.php/GuillermoOckham/article/view/4013, DOI: https://doi.org/10.21500/22563202.4013.

Gore, A. (2007). El ataque contra la razón. Como la política del miedo, el secretismo y la fe ciega erosionan la democracia y ponen en peligro a Estados Unidos y al mundo. Ciudad de México: Random House Mondadori.

Greenwald, G. (2014). Snowden. Sin un lugar donde esconderse. Ciudad de México: Ediciones B.

Horowitz, D. (1972). U.S. Electronic Espionage: A Memoir. Ramparts 11(2):35-50. Disponible en https://wikileaks.org/wiki/Perry_Fellwock.

IEI. (2017). Israel's Cyber Security. Sector Overview. Israel Export Institute. Disponible en: https://www.export.gov.il/files/cyber/CyberPresentation.pdf.

Kahn, D. (1973). The codebreakers. The story of secret writing. Chicago: New American Library.

Kahn, D. (2008). David Kahn. Official website. Disponible en http://david-kahn.com/david-kahn-biography.htm.

Leigh, D. y Harding. L. (2011). Wikileaks y Assange. Un relato trepidante sobre cómo se fraguó la mayor filtración de la historia. Ciudad de México: Deusto.

MILENIO. (21 de octubre de 2019). Julian Assange comparece ante tribunal en Londres. Disponible en: https://www.milenio.com/internacional/europa/julian-assange-comparece-ante-la-justicia-britanica, el 16 de noviembre de 2019.

Trzop, A. (2007). Beacon Press and The Pentagon Papers. Boston: Beacon Press. Disponible en: https://www.beacon.org/Assets/PDFs/pentagon_35.pdf.