Facultad de Periodismo y Comunicación Social

UNIVERSIDAD NACIONAL DE LA PLATA

"Maten al mensajero"

Un análisis sobre los riesgos en la era de Big data

Autores:

Muguruza, Carlos Sebastián; Legajo 18170/4 – sebamugu@hotmail.com

Natansohn, Agustin Ezequiel; Legajo 18174/8 – agustinnatansohn@gmail.com

Director:

Cristian Secul Giusti

Sede: La Plata

Presentación: Octubre de 2020

Indice

1 – Introducción

Este trabajo surge de la puesta en común de un conjunto de reflexiones provocadas por hechos y situaciones de actualidad. Ambos compartíamos la necesidad de elaborar el TIF de la Licenciatura en orientación periodismo, y coincidíamos en observar con preocupación un nubarrón de fenómenos y situaciones heterogéneas, tanto en el país como en el mundo.

Quisimos elaborar un trabajo que funcionase a modo de aporte ante las problemáticas que observamos. Y en función de eso nos preguntamos, ¿qué sería más necesario, determinar en qué consistió el pasaje de un sistema de vigilancia coercitivo a uno voluntario, o tratar de caracterizar este último dentro de nuestro campo de estudio que es la comunicación? ¿No son demasiado pretenciosas las preguntas?

Sin embargo, la respuesta es clara. Una cosa es imposible sin la otra. Comprender cabalmente la lógica del poder actual implica necesariamente estudiar los procesos históricos que le dieron lugar. Y finalmente, vislumbrar o inclusive aportar a una situación general que contemple caminos paralelos a una visión totalizante de la comunicación, se vuelve necesario y termina siendo nuestro motor motivacional para profundizar en los temas que elegimos.

Por esto mismo, este trabajo es caótico como lo es el mundo que nos toca presenciar. Combina visiones filosóficas, teorías consagradas, vaticinios actuales, historias de personas que corrieron riesgos, procesos intrincados y persecuciones de gobiernos a individuos por el mundo.

Actores jugando

Los hackers y alertadores tienen el enorme mérito de lograr algo que parecía imposible en la actualidad: materializarse en enemigos públicos sin hablar árabe. Mientras el escudo burocrático de fronteras, offshores, sociedades anónimas e instituciones inmunizan la impunidad de la mayor cantidad de concentraciones existentes (de poderes, de riquezas), personas comunes se vuelven los villanos de un momento al otro apenas por publicar cierta información. De esta manera, cobra extrema relevancia la importancia que tiene hoy en día la red como espacio de disputa: si además de ser el principal vehículo de la economía, sirve para manchar nombres, los poderosos tienen un problema.

Nuestro acuerdo sobre que ahí había un tema interesante nos llevó a preguntarnos cómo hacían esas personas para acceder a esas informaciones, cómo hacían para publicarla, cómo los perseguían luego. La historia de Julián Assange es singularmente relevante, tanto para el foco de este trabajo como para lo que nosotros consideramos es el futuro de las comunicaciones tal las conocemos.

A la vez, no dejamos de sentir que los radicales cambios que sufrieron los medios desde que entramos a la facultad, en el año 2008 hasta el presente, debían significar algo y eso debía formar parte del trabajo de alguna manera. No sólo de los medios de comunicación, sino también de algo nuevo que antes no existía, que son las redes sociales, o lo que sería más preciso decir, la informatización de nuestra manera de ser en sociedad.

Por todo ello, este trabajo reúne una fusión de visiones teóricas relativas a la actualidad en clave comunicacional, un repaso de la informatización como proceso relevante de la configuración actual, el estudio de algunos casos particulares de espionaje, filtraciones y disputas en torno a la libertad de la red, en todos los casos con la intención de darle cohesión y coherencia a una multiplicidad de hechos y datos que tienden insistentemente a abrumarnos y sobrepasarnos.

Fundamentación

En tiempos donde parece confuso encontrar la raíz de los problemas, y donde también cada uno ve el problema en algo diferente (lo cual es un problema en sí mismo), es interesante tomar reflexiones analíticas que contemplen de manera amplia nuestro tiempo. Creemos que la única forma de echar claridad ante tanta complejidad es ser paciente, estar abierto a leer ideas nuevas, pero por sobre todo prestar atención a los problemas.

Como primer eje no podemos dejar de analizar lo que solemos entender como el sistema capitalista, a veces entendido como sistema económico, aunque sabemos de sobra que es un ordenamiento global que excede lo meramente económico, como también excede cada vez más una denominación precisa.

La mutación del capitalismo es constante. Ante cada crisis se reinventa. Y no sólo eso. Parece alimentarse de los recursos simbólicos contestatarios, transformando cualquier estética en mercancía. Lo que nunca parece terminar de admitir es la finitud del mundo. El paradigma del

crecimiento, y la medición de bienestar como PIB siguen vigentes, aunque no sabemos por cuánto tiempo más.

Por otro lado, la revolución técnica en lo concerniente a la electrónica, comienza facilitando tareas y termina condicionando y modificando de manera decisiva el devenir humano a nivel planetario, al incidir cada vez más en diversos aspectos hasta configurar lo que Byung Chull-Han llama el psicopoder.

Dentro de este devenir neoliberal, toma extrema relevancia la cuestión de la información, su uso y su manejo. Hoy todo pasa por la tecnología, no sólo la comunicación. El debate por la libertad y el anonimato dentro de la red se convierten así en uno de los temas más necesarios de ser debatidos, junto con el desastre ecológico.

Es por eso que para el abordaje teórico de este trabajo tomamos como terminología relevante la mutación, entendida como concepto que aúna los procesos de cambio, psicopolítica, posverdad y big data.

Alcances y limitaciones

La metodología de este trabajo es cualitativa, y nuestro marco teórico se encuentra en la web y en los libros editados sobre el tema. Como comunicadores que no manipulamos el lenguaje encriptado que manejan los hackers, estamos limitados a conocer sólo los secretos que ellos (Assange y Snowden por ejemplo) han revelado a la comunidad. Sin embargo, es posible realizar una lectura del entramado de poder a partir del material a nuestro alcance.

Por este motivo, nos centraremos en los siguientes ejes: caracterización de las dificultades de quienes han alentado y generado un estímulo en la democratización de la red y su vinculación con el contexto mediante un abordaje teórico.

Objetivo general:

Caracterizar el periodismo de riesgo en la actualidad desde un abordaje teórico y conceptual, subrayando sus casos relevantes y las repercusiones que tiene en el discurso de la información.

Objetivos específicos:

- Destacar las implicancias y los riesgos que nos plantea la era de la hipercomunicación, tanto a los comunicadores como a la población en general.

- Recopilar los componentes esenciales del entramado hegemónico de poder planteado a través del desarrollo de las nuevas tecnologías.

- Indagar cuáles son las nuevas armas que un periodista comprometido debe maniobrar en la actualidad, específicamente en lo digital.

2 - Antecedentes

Cada vez hay más estudios académicos sobre la implicancia de la creciente virtualidad en los diversos asuntos sociales. Tanto desde enfoques comunicacionales como humanísticos, la relevancia de la incidencia real de estos nuevos procesos en el devenir humano cobra cada vez más notoriedad, haciendo exponencial el número de tratados tanto en claustros como en ensayos. El enfoque desde el que nosotros abordamos los temas de actualidad es lo bastante singular para comprender que no íbamos a hallar un trabajo de características exactas.

En su artículo "'Fake news' y posverdad en tiempos de populismos: lecciones para periodistas" (2017), escrito para el Festival Internacional de periodismo de Perugia, Patricia Alonso repasa algunos estudios que ya se deciden a prestarle atención a los contenidos que circulan por la web y cada vez compiten con mayor fuerza con el discurso periodístico. Sin arribar a conclusiones cerradas, se limita a establecer una preocupación que requiere permanente atención y preocupación por parte de los comunicadores, no sin hacer notar que "la desinformación ha estado siempre presente, pero lo que ha cambiado es la manera de producir y distribuir las noticias". Para Alonso el rol del comunicador actual es contrarrestar la desinformación, y es a partir de esa noción que la autora elabora su reflexión.

El mismo tema es tratado por Manuel Álvarez Rufs, alumno de la Universidad Nacional de Educación a Distancia de España (UNED), en su trabajo de fin de máster, *Estado del arte: posverdad y fake news* (2018). El estudio es muy extenso y detallado, tanto en la amplitud de definiciones posibles sobre verdad y falsedad, como en la explicación de los procedimientos que emplea para trabajar esas búsquedas, de ahí que en el título haga énfasis en el estado del arte. De esa manera, se puede interpretar la obra de este alumno como una verdadera guía donde se pueden encontrar muchas definiciones de diferentes tenores. Entre ellas destacamos: "En las circunstancias correctas, una mentira puede ser derrotada por el despliegue hábil de los hechos. Pero posverdad es, antes que nada, un fenómeno emocional. Se trata de nuestra actitud hacia la verdad, en lugar de la verdad misma (D´ Ancona, en Álvarez Rufs, 2018, p. 61).

A través de D´Ancona, Álvarez Rufs intenta contextualizar el origen de la atomización de las verdades, tal como nosotros intentamos en nuestro marco teórico con los autores que elegimos.

En la publicación *Papeles secretos, los cables de wikileaks* (2012), Shila Vilker compila ocho trabajos que analizan la implicancia de *Wikileaks* desde diferentes perspectivas: derecho de la comunicación, política internacional y transformación cultural. Cada uno aporta un enfoque particular al mismo tema. Entre sus líneas encontramos convincentes fundamentaciones sobre la vigencia del periodismo, o síntesis muy singulares que merece la pena citar:

> Todas las nuevas redes sociales generan vías de información inmediata pero poco profundas. La superficialidad de las informaciones que se pueden encontrar en la red de redes culmina en la difusión de documentos desclasificados, basados en apreciaciones subjetivas y noticias editoriales. Así como los valores que para Max Weber habían generado la racionalidad se perdieron en el tiempo y en la práctica de siglos, las fuentes de los documentos desclasificados publicados por *Wikileaks* se desdibujan y construyen un sentido común avalado por la principal potencia militar del mundo. (Fiorito, en Vilker, 2012, p. 172).

Así como cada trabajo que hallamos posee su "aurea teórica", elegida ya sea a gusto o conveniencia de cada autor, el nuestro es un trabajo de interpretación donde tomamos como referencia este tipo de obras citadas, pero encarando el tema junto a los autores elegidos para contextualizar, los cuales se enunciarán en el marco teórico.

3 - Marco teórico

Palabras Clave: Psicopolítica, Mutación, Big Data, Posverdad

Desde los primeros encuentros en que discutimos los temas que darían lugar a este trabajo, se nos plantearon una gran cantidad de problematicas que nos obligan a pensar el presente. Tal es así que desde ese primer momento, decidimos indagar tanto en teorías y autores vigentes, que encarasen de algun modo analítico o reflexivo la actualidad, como así también en profundizar sobre la historia de este proceso que en líneas generales puede llamarse informatización.

Hacer esto nos obligó a releer viejos supuestos saberes, encadenar estas nuevas teorías conforme vimos que eran posibles respuestas a nuevos fenómenos, ordenar de alguna manera que resultase legible (aportable?) el enjambre de tópicos y datos, y decantarlo en forma de racconto reflexivo que cumpla las características que demanda la academia.

Convertir justamente un pastiche en algo coherente, hacer que ciertas visiones parciales del mundo, con su nombre específico, tengan provisoriamente un punto de contacto entre sí, fue una tarea para nada sencilla. Hubo que construir puentes de sentidos y esbozar un cuadro situacional que contemplara diversas herramientas conceptuales, dando cuenta que no necesariamente cada autor escribe con las mismas motivaciones ni objetivos.

En muchos casos los estados hallados por estos lentes analíticos fueron desalentadores y lo siguen siendo. Para equilibrar la carga negativa, nos ocupamos también de indagar en la lucha que se está llevando a cabo en la red, lo que nos parece un suceso de gran trascendencia en relación directa con todo lo que analizamos. De los términos manejados por los autores escogidos, el marco teórico lo componen los siguientes cuatro: psicopolítica, mutación, big data y posverdad. Por fuera de esas nociones, hay también diversos temas que son tratados por casi todos los autores que repasaremos: la libertad, el poder, la crisis poítica o de representación. Volveremos sobre cada uno de estos grandes temas una y otra vez, conforme la visión de cada autor nos lleve a reflexionar desde un enfoque distinto la misma problemática.

Antes de entrar de lleno en las palabras clave, vamos a hacer uso de las voces de algunos pensadores para hacer un cuadro conceptual o coyuntural que nos sitúe en la tónica de incertidumbre del diálogo posterior.

"Si la libertad ya ha sido conquistada, ¿cómo es posible que la capacidad humana de imaginar un mundo mejor y hacer algo para mejorarlo no haya formado parte de esa victoria?" (Bauman, 2001, p.8). Bauman responde esta pregunta con un interesante análisis, con el propósito de desentramar los motivos de la crisis política que significa encontrarnos inmersos, después de un siglo sangriento y una generación contestataria machacada por dictaduras, en una época de apatía politica o moral, donde reina el desgano o hartazgo generalizado por la política. Con una simplicidad admirable, Bauman nos recuerda la importancia de la política. Al respecto nos dice:

> Tanto la nación como la familia son soluciones colectivas del tormento causado por la mortalidad individual. Ambas transmiten el mismo mensaje: mi vida, por breve que sea, no es en vano ni carente de sentido si, a su modo y en pequeña escala, ha contribuido a la duración de una entidad mayor que yo mismo (o que cualquier otro individuo semejante a mí) y que antecede y sobrevivirá a mi propia vida, dure esta lo que dure. Esa contribución es la que otorga un papel inmortal a una vida mortal (...) en vez de enfrentar mi mortalidad resignadamente, he hecho algo para superarla. He convertido mi propia mortalidad individual en un instrumento para lograr la inmortalidad colectiva. (Bauman, 2001, p. 47).

En la actualidad, son esas totalidades las que sufren un desmoronamiento gradual y constante, las que no ofrecen protección alguna, por no hablar de inmortalidad, y que por eso han perdido su capacidad de conferir sentido (Bauman, 2001).

Visto de este modo, podemos establecer que la crisis de las instituciones que venimos atravesando desde casi el inicio del siglo XX, trae consigo una crisis un poco menos tangible: la crisis de la política, del nivel de participación ciudadano en los aspectos comunes. A medida que el capitalismo mutó de un sistema de alianzas de Estados fuertes, hacia otro más desterritorializado, las instituciones entran en crisis, porque dejan de controlar las certezas que hacían posible su funcionamiento. Las promesas de prosperidad incumplidas hacen estallar ese arquetipo fallido.

Las aspiraciones de encontrar el bienestar se vieron así atomizadas en todo tipo de prácticas, dogmas y causas. El hartazgo a la retórica de política clásica se puede ver reflejado en consignas como "que se vayan todos", o la idea de que son "todos chorros", por sólo citar un suceso a nuestro alcance.

Lo que Bauman aporta aquí es claro. Por más atomizadas que estén las identidades, la única vía posible hacie el bien común es política (o democrática, si se quiere). ¿está preparada la humanidad para un debate global? Slavoj Zizek, filósofo esloveno, se pregunta lo siguiente en relación a esto: "Lo que definimos como nuestro bien común no es algo que simplemente está ahí; por el contrario, tenemos que asumir la responsabilidad de definirlo" (Zizek, 2014, p. 8).

Una valoración muy apropiada respecto a la realidad que nos toca debatir, es el hecho de que no necesariamente debemos encontrarle un sentido. La ruptura de los sentidos monolíticos, únicos y totalizantes, es quizás una condición con la que tenemos que convivir (o de la cual aprender). Sobre eso, Zizek señala que el capitalismo global es necesariamente inconsistente: la libertad de mercado va acompañada del apoyo de los Estados Unidos a sus propios agricultores, “y su prédica de las virtudes de la democracia es simultánea a su apoyo a Arabia Saudí. Esa incoherencia, esta necesidad de romper las propias reglas, abre un espacio a intervenciones políticas genuinas” (Zizek, 2015, p. 195).

En términos similares, el investigador franco-argentino Miguel Benasayag marca un pensamiento muy similar en una entrevista, que refleja ciertas tensiones:

> En Argentina, hay una contradicción entre justicia social y justicia ecológica. Porque la justicia ecológica dice no a los transgénicos o a la minería y justamente de ahí está sacando el gobierno de Cristina Kirchner la plata para pagar los planes sociales. Entonces, al chico que está en una villa miseria con riesgo de morir de malnutrición, la justicia ecológica le puede parecer perfectamente un lujo de ricos y una abstracción. Las dos luchas son coherentes, pero no armónicas (...) no hay solución global en un mundo complejo, no hay síntesis" (Fernández Savater, 2015).

La historia humana no se caracteriza por ser un relato carente de violencia, sometimiento e injusticia. Sin embargo, todos estos pensadores están dando cuenta de algo distinto. El mundo se ha

complejizado, es caótico, y a su vez cada vez más interdependiente. Y mientras la avanzada científica nos sorprende, cabe preguntarnos ¿estamos a la altura de las circunstancias?

Mutación

En medio del pasaje de cierto tradicionalismo a un sistema radicalmente distinto (Bauman diría líquido, mientras que cada autor va a elaborar una explicación diferente), vamos a prestar atención a los aportes de Franco Berardi, que se ocupa no sólo de analizar los efectos de la tecnología en la sociedad, lo cual lo vuelve pertinente a nuestro trabajo, sino también de remitirse a un orden más interno, emparentandolo con lo que vamos a leer en Han.

Berardi percibe la transformación social como algo que ocurre, también, a nivel interno. Y objetiviza la mutación en términos de conjunción-conexión. Resulta interesante tomar nota aquí de qué comprenden esos terminos, y su paralelismo con la disyuntiva biopoder-psicopoder de la cual vamos a hablar después. Para Berardi el sistema conjuntivo que estamos abandonando es aquel en el cual los cuerpos interactúan de maneras inciertas, sin diseños preestablecidos.

En él la producción de sentido se da gracias a una sintonía provisoria y precaria, pero que genera resultados insospechados y diferentes. En el sistema conectivo en cambio cada elemento permanece diferenciado e interactúa únicamente de manera funcional: “Más que una fusión de segmentos, la conexión supone un simple efecto de funcionalidad maquinal¨ (Berardi, 2018, p. 29), la red por ejemplo se expande a partir de la reducción progresiva de un número creciente de elementos a un formato, a un estándar y a un código que compatibiliza los diferentes componentes.

Berardi considera que este cambio es una mutación antropológica, una transición de la predominancia de un modo conjuntivo a la de un modo conectivo en la esfera de la comunicación humana:

> Desde un punto de vista antropológico este cambio tecnocultural está centrado en el desplazamiento de la conjunción hacia la conexión en los paradigmas de intercambio de los organismos conscientes; un cambio cuyo factor predominante es la insersión de segmentos

> electrónicos en el continuum orgánico, la proliferación de dispositivos digitales en el universo orgánico de la comunicación y en el cuerpo mismo (Berardi, 2018, p. 29).

Berardi no es el único que se atrevió a analizar este fenómeno. Miguel Benasayag, cuya singular historia lo lleva desde la lucha con Montoneros en los 70 a una prestigiosa carrera como neurocientífico en Francia, ha publicado estudios detallados que dan cuenta de esta mutación: "Se está produciendo una reorganización del cerebro humano. ¿cómo? se está transformando en un aparato de procesar información, pero de una manera especial: esa información en ningún momento hace mella, no esculpe, no marca. Simplemente es flujo, pasa". (Revista Mu, 2014).

El estudio de Benasayag es eminentemente más "científico". Berardi en cambio se atrevió a especular de manera filosófica sobre algo que es visto con preocupación: "Las respuestas a muchos de mis interrogantes políticos y culturales se hallaban en este desplazamiento de la conjunción hacia la conexión." (Berardi, 2018, p. 13). La conexión fluye por un orden preestablecido: genera mensajes que sólo pueden ser interpretados por agentes que comparten el mismo código, lo cual da cuenta de una extrema limitación en sus posibilidades, respecto al modo conjuntivo. En otras palabras, recaemos en una suerte de estandarización, algo que está muy emparentado con la preponderancia del carácter mercantilista de la cultura. A modo de síntesis, Berardi explica en este párrafo la transformación política que posibilitó la mutación.

> Como se ha señalado, en el contexto de la historia la acción política era dirigida por la voluntad, el entendimiento racional y la predicción (...) en la era que comenzó con Maquiavelo y terminó con Lenin, la voluntad política (el príncipe, el Estado, la patria) era capaz de reinar en la infinita variación caótica de eventos y proyectos, y de someter los intereses y pasiones individuales a los objetos comunes de orden social, crecimiento económico y progreso civil. Ahora, las transformaciones técnicas que hemos presenciado en las últimas décadas del siglo XX y la infinita proliferación de fuentes y flujos de información desatada por la aceleración de la tecnología de redes han hecho imposible la elaboración consciente de la información por parte de la mente individual y la coordinación consciente de agentes individuales intencionales. Como resultado, la falta de efectividad en la acción política se debe esencialmente a un cambio en la temporalidad: en las codiciones de aceleración y complejización de la infoesfera, la razón

> y la voluntad (esas características cruciales de la acción política) ya no pueden procesar ni decidir en el tiempo (Berardi, 2018, p. 35).

El flujo electrónico es demasiado rápido para una examinación crítica. El análisis es acertado y ayuda a comprender, al menos en parte, la crisis de las certezas. El panorama planteado por Berardi es bastante desolador, y los problemas se suceden unos con otros, por lo cual llega un momento en que tenemos que hacer un racconto de hasta dónde podemos permitir que nos innunde el pesimismo en relación a los procesos que, involuntariamente, forman parte de nuestra cotidianeidad. La teoría de la mutación parece acertada, nuestros mecanismos de construcción de sentidos están más automatizados que antes, resultan más estandarizados y predecibles.

En el libro Data Trash (datos basura), Arthur Kroker y Michael Weinstein escriben que, en el ámbito de la aceleración digital, más información implica menos significado, porque el significado ralentiza la circulación de la información. En la esfera de la economía digital, mientras más rapido circula la información, más rapido se acumula el valor. Pero el significado ralentiza este proceso, ya que necsita tiempo para ser producido, elaborado y compredido. Así, la aceleración de los flujos de información supone la eliminación del significado.

> En las décadas inauguradas por Thatcher y Reagan, el conocimiento fue puesto a trabajar en condiciones de absoluta dependencia respecto del capital. La ciencia se había incorporado a los automatismos de la tecnología, desprovista de la posibilidad de cambiar las finalidades que guiaron su operatividad funcional. La aplicación intensiva del conocimiento en la producción condujo a la creación de la tecnoesfera digital, la cual generó efectos de un potencial extraordinario. Pero este potencial fue sometido a los automatismos técnicos en los que se halla encarnado el poder. La tecnología, constreñida por las categorías de beneficio económico, incrementó la productividad del trabajo multiplicando, simultaneamente, la miseria, la subordinación de los seres humanos al trabajo asalariado, la precariedad, el desempleo y nuevas formas de alienación (Berardi, 2018, p. 211).

Para sintetizar el devenir neoliberal y su tendencia informatizante, Berardi acuña el término semiocapitalismo, incluso también el de absolutismo capitalista. Producto de las desregulaciones y las crisis de los Estados-Nación frente a la transnacionalización del poder, esta nueva versión de capitalismo encuentra menos obstrucciones y limitaciones para operar. Es más flexible y resiliente. Parte de esa transformación es la que da cuenta de que, los bienes de mayor cotizacion dejan de ser materiales, para ser virtuales.

> Solo aquellos acontecimientos y cuerpos que no son ni muy grandes ni muy pequeños, ni muy rápidos ni muy lentos para la comprensión humana, pueden ser objeto de la acción histórica y de la voluntad política. Aquello que es demasiado grande o pequeño, rápido o lento como para ser visible, perceptible y manejable, pertenece a la esfera de la evolución, no a la de la historia. El pensamiento científico y el cambio tecnológico les han dado a los humanos la posibilidad de abordar aquellas dimensiones espacio-temporales que no pueden ser examinadas a simple vista y que no pueden ser verificadas y sometidas a la discusión racional y a la decisión crítica. Por esta razón, estamos saliendo de la dimensión histórica, y nuestras acciones deben abordarse cada vez más desde una apreciación evolutiva (Berardi, 2018, p. 296).

De alguna manera Berardi nos dice que las decisiones se nos están yendo de las manos. Están dejando de ser controlables, en términos políticos o inclusive simplemente humanos.

Psicopoder

Una de las teorías más recordadas en nuestra facultad es el panóptico de Bentham, junto con la espiral del silencio de Noelle-Neumann. Además de ser una teoría muy gráfica, el panóptico es un ejemplo de cómo opera el poder en las instituciones (esas cuya decrepitud anunciamos al inicio de este capítulo). Bentham había diseñado una cárcel con una torre desde la cual se podía observar a todas las celdas. El poder que vigila, todo lo ve. Foucault es quien retoma el concepto del panóptico en su descripción del poder de las instituciones, y acuña el término biopoder, como analogía de un gran organismo que controla las partes que lo componen.

Cuando uno lee a Byul Chun Han se da cuenta de que el poder actual es mucho más que la capacidad de vigilar (y actuar en consecuencia): las transformaciones que estamos vivenciando modifican constantemente la fisonomía del poder.

Hay varios intelectuales y lectores que toman con pinzas las teorías de Han, por considerarlas apresuradas o carentes de un sustento adecuado. Sobre todo, porque parecería querer quitarle la razón a Foucault, algo que resulta absurdo ya que este último analizó una sociedad al menos algo diferente a la actual. Amén de eso, es interesante observar su punto de vista. Son pocos los análisis que intentan estudiar las implicancias del surgimiento de los macrodatos o big data, y su consecuente usufructuo por parte de empresas y gobiernos. Ello sin dudas representa una situación mucho más compleja que el poder ejercido desde la coerción y la vigilancia óptica de los cuerpos, como ocurrió y se estudió a mediados del siglo XX. De hecho, la directriz de este poder ya no opera en el plano físico, sino desde lo interno, lo cual lo vuelve mucho más complejo.

"La libertad ha sido un episodio", empieza Han uno de sus ensayos, “Psicopolítica” (2014). Caracterizar nuestra contemporaneidad como una era neoliberal, donde preponderan las llibertades individuales por sobre las colectivas, es una buena forma de comenzar.

El episodio que Han considera concluido tiene que ver con las decisiones que estamos vedados de considerar, lo cual hace acordar mucho a lo que acabamos de ver con Berardi y nuestro devenir como seres conectivos. El concepto más interesante de su ensayo da cuenta de las decisiones a nivel prereflexivo que realizamos, mediante una manipulación intencionada que los grupos de poder pueden efectuar (y lo hacen) mediante un preciso y complejo análisis de la información que -voluntariamente- les proveemos.

> El neoliberalismo como una nueva forma de evolución, incluso como una forma de mutación del capitalismo, no se ocupa primeramente de lo `biológico, somático, corporal´. Por el contrario, descubre la psique como fuerza productiva. Este giro a la psique, y con ello a la psicopolítica, está relacionado con la forma de producción del capitalismo actual, puesto que este último está determinado por formas de producción inmateriales e incorpóreas (Han, 2014, p. 41-42).

Para objetivar la dominación Han habla a su vez del sujeto neoliberal. En el siguiente pasaje se da cuenta de a qué se refiere, y cómo el poder opera desde lo interno en él.

> El sujeto neoliberal como empresario de sí mismo no es capaz de establecer con las otras relaciones que sean libres de cualquier finalidad (Han, 2014, p. 13). ¨El neoliberalismo es un sistema muy eficiente, incluso inteligente, para explotar la libertad. Se explota todo aquello que pertenece a prácticas y formas de libertad, como la emoción, el juego y la comunicación. No es

> eficiente explotar a alguien contra su voluntad. (...) Solo la explotación de la libertad genera el mayor rendimiento (Han, 2014, p. 14).

Esa singular inteligencia de la que habla Han nos hace sentirnos responsables a nosotros mismos cuando nuestro rendimiento no es el esperado: "Quien fracasa en la sociedad neoliberal del rendimiento se hace a sí mismo responsable y se averguenza, en lugar de poner en duda a la sociedad o al sistema" (Han, 2014, p. 18).

El psicopoder es inteligente porque oculta la dominiación. En un régimen de autoexplotación, donde a diferencia de un régimen represivo, uno dirige la agresión hacia uno mismo. La autoagresividad, continúa Han, "no convierte al explotado en revolucionario, sino en depresivo" (Han, 2014, p. 18)

A propósito de lo mismo es válido este comentario de Miguel Benasayag:

> El neoliberalismo -digamos, la gestión empresarial de la vida- es una lógica global, pero que se dispersa en el infinito de las situaciones (por ejemplo, la escuela, la salud o la naturaleza son gestionadas como empresas). El todo está en cada una de las partes, diríamos filosóficamente. Uno no encuentra al neoliberalismo más que bajo sus diversos modos de existencia. Es decir, el neoliberalismo está compuesto de prácticas cotidiantas, de relaciones sociales y nosotros mismos participamos en esta explotación a la que estamos sometidos¨ (Fernández Savater, 2015).

Así, podríamos decir que el psicopoder es una de las formas que tiene el neoliberalismo para desarrollarse. Vale aclarar que existen un sinfín de culturas y subculturas distintas a lo ancho del planeta que no se encuentran inmersas en esa vorágine, si se quiere, occidental. Pero entendemos que a lo que apunta Han con su crítica es a esas inmensas mayorías de sujetos urbanos, que no sólo representan una mayoría demográfica, sino que además encarnan de alguna manera el futuro del devenir social. La mayoría de las culturas del mundo cada vez se parecen más a una única cultura, y es este arquetipo el que Han estudia cuando habla de "sujeto".

Big data

La herramienta infalible sobre la cual se basa este giro hacia la dominación sutil es el empleo de los macro datos. La big data podría describirse como una herramienta novedosa que surge de una compleja evolución en las formas de circulación de la información, que al ingresar a su etapa digital encuentra formas de almacenar y procesar cantidades hasta hace pocos años inimaginables de datos. Datos que ya no son sólo la textualidad del discurso, sino también la metadata del mismo: dónde y cómo circula, quiénes y cuántos acuden a ellos, por qué canales. Toda esa información en grandes cantidades se vuelve valiosa. Los smartphones son máquinas de generar metadatos, a través de sus diversos sensores: GPS, cámaras, procesadores que son computadoras en sí mismas.

La utilización de la big data para analizar y sacar provecho de las tendencias sociales es el eje central de la psicopolítica, y es también el salto crucial entre la noción foucaultiana de biopoder y la tesis de Han: ¨Para incrementar la productividad, no se superan resistencias corporales, sino que se optimizan procesos psíquicos y mentales." (Han, 2018, p. 42).

Una definición de Big Data: "La sociedad crea datos y más datos y cada vez existen más dispositivos y más eficientes para almacenarlos. Los datos son vistos como una infraestructura o un capital en sí mismos para la organización ya sea pública o privada que disponga de ellos (…) estas grandes cantidades de datos se están convirtiendo en factores de producción esenciales dentro de cada sector productivo." (Getino, 2015). En su tesis de la Universidad de Barcelona, Antonio Getino expone algunos datos que grafican muy bien la era de los datos: "El 90 por ciento de los datos del mundo ha sido creado en los últimos dos años. Un disco duro que contiene toda la música del mundo sólo vale unos 500€ " (Getino, 2015).

En este estudio, Getino explica de qué forma empiezan a usarse esos datos para desarrollos científicos, de transporte, de logística y de producción. Menciona los puntos oscuros, sus posibles usos con fines de control social, pero se limita a enumerarlos, tanto unos como otros. En un trabajo sobre la Big Data de Saif Shahin para la universidad de Bowling Green State, EEUU, afirma que dentro de las manipulaciones posibles del uso de datos ya ha habido casos de racismo. También en su trabajo deja ver que el análisis de la Big Data corre por vías paralelas: "los esfuerzos por comprenderla y capitalizarla, y los esfuerzos por contornear sus lados oscuros. La Big data ha empoderado a gobiernos y empresas al darles un mayor control sobre nuestras vidas" (Shahin,

2012).

Posverdad

La modernidad nos encuentra ante una situación de mutación, de reconfiguración del poder, de cambios en nuestra sensibilidad y nuestros hábitos. Gracias a los aportes teóricos de autores como Han, Berardi y Benasayag, se pudo merodear estas nociones bajo supuestos, teorías y visiones diferentes pero que coinciden en resaltar la predominancia de la informatización como factor decisivo en el devenir sociopolítico. Es el momento de remitirnos ahora a un aspecto problemático más específico que opera dentro del universo comunicacional, que al fin y al cabo cada vez nos es más propio y cotidiano.

Provenimos de una facultad donde nos enseñan a valorar el uso responsable de la información, a ser mediadores conscientes. Pero todo lo que publicamos se mezcla hoy en un océano virtual en el cual conviven una multuplicidad de -no ya discursos- sino contenidos.

Nuestra cotidianeidad se ha transformado en un continuum de consumo de contenidos. A cada rato estamos viendo memes, chats más o menos privados, noticias de portales que ya no sabemos de dónde son ni desde cuando existen, noticias de procedencia incierta, publicaciones republicadas, tweets retwiteados, emails reenviados, fotos, audios de watsap. Toda esa maraña informativa nos llega por el mismo dispositivo, el celular.

La virtualidad es hoy uno de los principales ejes de la economía mundial. En nuestra era, ya no resulta tan obvio de donde surgen las riquezas. La informatización de la economía es un riesgo en sí mismo y que sea evidente, pero a la vez inevitable puede ser uno de los aspectos más desoladores. Así como los grandes cracks económicos de la historia fueron producto de especulaciones financieras, es decir, de abstracciones en las relaciones entre valores y usos reales, la excesiva falta de correlación entre los actuales motores de la economía y los bienes reales, tarde o temprano llegará a un punto crítico.

Hoy la puja económica y de poder que se cierne en torno a lo digital es enorme. Alcanza dimensiones inusitadas, como por ejemplo la de nuestro tiempo de atención.

A esta lógica que nos lleva a permanecer cada vez más tiempo conectados, parecería no interesarle la calidad de los contenidos en sí, ni su significancia literal o retórica. Quienes gestionan el andamiaje de la circulación, es decir, quienes mejor se aprovechan de esta coyuntura en términos económicos, saben que lo importante es crear los marcos (dispositivos y aplicaciones). En ellos, los contenidos luego circulan.

> El medio digital es un medio de presencia. Su temporalidad es el presente inmediato. La comunicación digital se distingue por el hecho de que las informaciones se producen, envían y reciben sin mediación de los intermediarios. No son dirigidas y filtradas por mediadores. La instancia intermedia que interviene es eliminada siempre. La mediación y la representación se interpretan como intransigencia e ineficiencia, como congestión del tiempo y de la información (Han, 2018, p. 33).

En esta desleal maraña competitiva, los medios de comunicación tradicionales, ya sea en sus soportes tradicionales como en sus versiones web, pierden definitivamente el monopolio de la circulación de mensajes, además de perder las verdades sobre las que se sostenían.

Daniel Mazzone dice que el término posverdad “pretende caracterizar a la situación en la cual mentiras flagrantes se viralizaron a partir de las posibilidades inéditas de las redes reticulares, para finalmente declararse como falsedades. Obviamente, el daño que hizo en unas pocas horas la mentira viral, es infinitamente mayor que el modesto desmentido, tardío, ineficaz” (Mazzone, 2018, p.16).

Tenemos aquí, una definición formal. Sobre esta base, el autor relexiona: ¨Llámese posverdad, fake news o guerra híbrida, lo cierto es que estamos en problemas en un plano en el que no solíamos tenerlos. La humanidad -y Occidente en particular- tiene una prolongada experiencia en materia de circulación de textos con ambición de permanencia en la consideración colectiva. Desde el surgimiento de la escritura, se escribieron textos que aspiraban a decir, comunicar, informar e influir¨ (Mazzone, 2018, p. 33).

Es evidente que la circulación y consumo de contenidos rompe con esa tradición de fiabilidad del discurso informativo. De hecho, ese es el problema central: la nueva camada de discursos no tiene esa pretensión de permanencia en el tiempo. Su carácter efímero y predominantemente visual lo

convierten en un proceso más complejo, donde lo que importa no es tanto el contenido, sino el proceso todo en el que éste circula.

La equiparación en términos de exposición de ambos valores (el contenido y el discurso informativo) en los mismos formatos, en una cotidianeidad que ya no puede distinguir entre el consumo de ambos, es el problema central de la posverdad. Según Maingueneau y Charaudeau, el término de contrato de comunicación "es empleado por semióticos, psicosociólogos del lenguaje y analistas del discurso para designar aquello por lo que un acto de comunicación será reconocido como válido desde el punto de vista del sentido¨ (2005). De acuerdo con Mazzone, y en conformidad con el desarrollo que venimos sosteniendo, también según nosotros, desde hace una década, data el período de transición en que "el viejo contrato industrial viene dando crecientes muestras de agotamiento. En ese marco, en 2016, se legitimó el término 'posverdad', cada vez más utilizado socialmente. Y en 2017, el concepto 'fake news'. Ambos constituyen formas imperfectas, quizá apresuradas, de reconocer que algo había ocurrido¨ (Mazzone, 2018, p. 41).

Pese a esto, la ya declarada muerte del periodismo (citar libro de lavaca) al estilo Fukuyama no es todavía un hecho definitivo. (en un capítulo siguiente se analizarán los motivos por los cuales el periodismo aún conserva vigencia).

Para el filósofo y divulgador Darío Sztajnszrajber la posverdad no es más que una readaptación contemporánea del histórico dilema de la verdad. Pero a la vez agrega algo más. La posverdad sería una herramienta para reafirmar certezas previas, pese a ser un llamado de atención de la realidad. Algo así como un autoengaño. Así, también, obliga a asumir que la dicotomía verdad/falsedad debe ser superada (algo que, de una manera u otra, termina siendo recurrente).

La pertinencia de incluír este concepto es que permite replantearnos no sólo cuales son las verdades que han muerto, sino también dejar el camino abierto a futuros consensos. Hoy la coyuntura parece obstinada a no otorgarnos certezas. Pero como esas nunca fueron más que construcciones de sentido, es cuestión de construir una nueva.

4 - Método de trabajo

Las conversaciones que dieron lugar a este trabajo tuvieron lugar cuando Julian Assange estaba siendo hostigado por la justicia sueca, refugiado en la embajada de Ecuador en Londres, pretendido por las altas esferas de EEUU.

Mientras aún no sabíamos bien bajo qué lineamientos conduciríamos el TIF, iniciamos un proceso de búsqueda e investigación sobre comunicadores en riesgo, que derivó en informaciones y situaciones muy diferentes.

Para engrosar nuestros conocimientos sobre Assange y todo el mundillo informático del cual forma parte, tuvimos que comprar una buena cantidad de libros cuyo contenido, paradójicamente, no está disponible en la web. Existen muchos libros sobre *Wikileaks*. Le dimos prioridad a los escritos por sus integrantes, aunque también nos ganó la curiosidad por ver qué decían algunos detractores sobre Assange, como Daniel Estulin, que parece ser un experto en conspiraciones, pero sus análisis poco sirvieron para este trabajo.

Cuando comenzamos a reunirnos con nuestro director, Cristian Secul Giusti, nos recomendó algunos autores para abordar el marco teórico. En particular a Bifo Berardi, quien nos aportó una perspectiva de actualidad muy singular, que hizo falta repensar en innumerables charlas hasta que nos resultara lo suficientemente pertinente y congruente para los propósitos del TIF.

Por otro lado, existen teorías y visiones filosóficas que forman parte de nuestro agrado y quisimos agregarlas, ponerlas a jugar con los textos recomendados por Cristian, para que formaran parte de los conceptos teóricos desarrollados, no sólo como marco teórico, sino como guía para nosotros mismos, en la tarea de encontrarle sentido a los fenómenos que fuimos investigando.

Al tratarse de un TIF de investigación, decidimos concentrar las búsquedas principalmente hacia fuentes bibliográficas. Para esto, se tuvo en cuenta una metodología cualitativa, a fin de tomar la recopilación de datos como un diagnóstico de lectura y contexto, con una búsqueda orientada al proceso (Palazzolo y Vidarte Asorey, 2012). Esta perspectiva sirvió para acercarse a los materiales y comprenderlos de la manera más integral posible. La conformación de referencias se realizó a partir de clasificaciones de unidades de sentido, las identificaciones de las disyunciones fundamentales y el rastreo de las asociaciones (Charaudeau, 2004).

Pese a ser un tema de actualidad, ya existe gran cantidad de trabajos sobre coyuntura político social, virtualidad y comunicación global. Podríamos diferenciar tres grandes tipos de material de texto: aquellos que se referían a un tema específico, como los ya mencionados libros sobre *Wikileaks*, los ensayos de autores, como el caso de Berardi, Han, o Zizek, claves para cohesionar y contextualizar, y por último los textos del ámbito comunicacional, que fueron los más esclarecedores en tanto su riqueza interpretativa, y sus enfoques nos sirvieron para ordenar finalmente nuestra investigación. De este tipo destacan las obras de Mazzone, sobre Fake news, y la compilación de Vira Shilker (Eudeba) sobre las implicancias de *Wikileaks* en el ámbito periodístico.

Dentro de esta categoría también hallamos trabajos académicos de casas de estudio de todo el globo que ya empiezan a estudiar fenómenos como la posverdad, el impacto de las redes en la esfera comunicacional, etc.

La mayor parte del trabajo estuvo originado en nuestra interpretación de estos tres tipos de textos. Las consultas a especialistas se redujeron a cuestiones puntuales, dado que los temas que tratamos en el trabajo son tan diversos, que el único punto en común es el orden particular bajo el cual hacemos congruente todas las problemáticas.

En alguna fase primaria del trabajo nos habíamos propuesto indagar, mediante entrevistas o consultas por email, a algunas personalidades o especialistas en seguridad informática. Pero al notar que lo que debíamos incluir estaba ya contenido en los textos, y que nos obligaba a reformular o ampliar aún más el espectro de temas tratados, decidimos limitarnos a interpretar la información que recopilamos con los textos que elegimos. Dentro del cúmulo de datos que también usamos se hallan una gran cantidad de artículos periodísticos, noticias sobre la suerte de algunos alertadores, videos de actualidad o coyunturales, manuales, sitios web, revistas virtuales, etc.

El capítulo sobre el abordaje histórico de las telecomunicaciones fue el único que nos hizo salir de la metodología que proponíamos, obligándonos a realizar una búsqueda de datos que fue posible a través de Internet. Gracias a trabajos de distintas universidades, logramos hallar datos claves acerca de la conformación de la infraestructura comunicacional, vital para interpretar y comprender lo que tratamos en los capítulos siguientes.

Para llevar adelante el trabajo creímos pertinente hacer una división de tareas, si bien los libros que fuimos adquiriendo los leímos los dos. Una vez divididas las tareas cada uno se encargó de un

capítulo diferente, sumándole varias reuniones a lo largo de un año, donde intercambiamos datos, pareceres y puntos de vista, generando una dinámica de trabajo que nos permitió aunar conceptos y consensuar la orientación que fueron tomando los resultados a los que arribamos.

5 - Abordaje histórico de la informatización de la comunicación

En este capítulo vamos a hacer un repaso histórico por algunos hechos que, lentamente, fueron conformando la compleja trama de infraestructura informacional que tenemos en la actualidad. Consideramos necesario realizar una revisión de cómo fue concebida la comunicación a larga distancia y qué prácticas fue despertando a nivel humano. La finalidad de este capítulo es entender cómo llegamos a este mundo globalizado, qué invenciones nos depositaron en la era de la inmediatez y la conexión casi total, y así poder comprender cómo cambiaron las armas, las estrategias y los riesgos en la esfera comunicacional de hoy.

¿Al servicio del Estado?

Los primeros antecedentes de lo que es hoy la Red, pudieron haber sido esas comunicaciones a larga distancia en que el mensajero hizo llegar su recado sin trasladarse físicamente. Las técnicas de luces, toques de tambores o señales de humo a la hora de enviar señales forman parte de la historia de la comunicación, sin embargo, no forman parte de la historia de la Red. Esta tiene sus raíces en la modernidad y es inevitablemente una construcción del Estado: “Cualquier sistema de telecomunicación estable necesita de una infraestructura y unos gastos que sólo pueden ser sufragados por una entidad poderosa. Por ello los primeros sistemas de telecomunicación eran siempre por y para el servicio del Estado” (Estepa, 2004).

Este es un dato no menor, ya que hoy día la actitud de los alertadores y sus prácticas están juzgadas de “poner en riesgo” la seguridad nacional y muchos son considerados, por esto, como “enemigos del Estado”. La Red, lejos de ser libre y gratuita, nace bajo esta condición a fines del siglo XVIII y la mantiene hasta el día de hoy.

La realidad es que tanto Internet como las comunicaciones a larga distancia fueron, primero que nada, experimentos que llevaron a cabo los grupos más poderosos del planeta, desarrollando tecnologías que primeramente estuvieron al servicio del ejercicio militar.

Como expone Estepa, las primeras redes de telecomunicación propiamente dichas surgen con la aparición de la telegrafía óptica en Francia y datan justamente de la revolución francesa. La red óptica-mecánica fue ideada por Claude Chappe y en una década comenzó a expandirse por Europa.

Los costos de infraestructura y mantenimiento excedían lo que ciertos Estados podían solventar, como lo fue el caso de España que consolidar su red telegráfica nacional le llevó unos diez años, cuando pudieron al fin pagar los costos a las empresas inglesas encargadas de desarrollar este tipo de tecnología.

Cable transatlántico

En 1844 es llevada adelante la primera transmisión telegráfica en Estados Unidos. El invento generó un gran asombro en su generación y forjó un gran paso en las telecomunicaciones: "Hacia 1863 el mapa telegráfico tenía ya una cierta complejidad con 7 líneas radiales y una red periférica que cubría costas y fronteras" (Estepa, 2004). El gran impulsor de este invento fue el estadounidense Samuel Morse.

Eran tiempos de grandes progresos industriales. La gutapercha fue fundamental para lograr un aislamiento perfecto de los cables conductores, entonces podía pensarse en la conexión telegráfica incluso a través del agua. Fue en 1851 cuando se coloca con éxito el primer cable que cruza El Canal de la Mancha, conectando a Inglaterra con toda Europa. La gran potencia quedó unida al continente para siempre.

Incluso permitió pensar en establecer comunicación directa entre territorios separados por el Océano Atlántico, y fue así como en "…1866 se instaló el primer cable trasatlántico que unía América con Europa, permitiendo así la interconexión de ambas redes telegráficas. La telegrafía eléctrica se había impuesto ya por esta época en otros países de Europa desarrollada al amparo del ferrocarril, donde las compañías tenían su propia red que coincidía con el trazado de la línea." (Estepa, 2004).

La proeza se logró en 1866, sin embargo, fue en 1857 cuando se realizó el primer intento de conectar Europa con América. Para esto Cyrus W. Field, un ambicioso empresario estadounidense, se encargó de viabilizar el proyecto negociando con los comerciantes más ricos de Inglaterra y con

diferentes empresas para el logro del objetivo: creó la Atlantic Telegraph Company y generó contratos con Gutta Percha Company, Glass, Elliot and Co. y R.S. Newall and Co.

> Las fábricas tejen día y noche, se gastan montañas de hierro y cobre en la fabricación del cable, y por él han de sangrar bosques enteros para elaborar la goma del revestimiento de glutapercha. Nada revela mejor las proporciones de la empresa que el hecho de que en un solo cable tengan que entretejerse más de seiscientos mil kilómetros de diferentes hilos, catorce veces más de lo que bastaría para abarcar el mundo y suficiente para unir la Tierra con la Luna (Miranda, 2010).

Es evidente que una hazaña de tal magnitud sólo es posible lograr cuando las voluntades económicas y políticas están del mismo lado. Y no hubiese sido posible la colocación del cable sin la utilización de buques que permitan transportar tanta cantidad de hierro y cobre en sus cubiertas:

> Hacen falta dos buques que, a su vez, deben ir acompañados por otros que han de prestar ayuda. El gobierno inglés pone a disposición de la empresa uno de sus buques de guerra más grande, el HMS Agamemnon, y el gobierno norteamericano presta el USS Niágara, la fragata de mayor desplazamiento de la época (cinco mil toneladas). Pero es necesario reformar completamente los dos buques para poder emplazar en cada uno de ellos la mitad del inmenso cable (Miranda, 2010).

Finalmente, tras varios intentos fallidos, pérdidas de miles de libras esterlinas, con otros buques nuevamente puestos a disposición por los gobiernos inglés y estadounidense y casi diez años después, el cable transoceánico es colocado con éxito. Esto marcó un antes y un después en materia de telecomunicaciones. El cable colocado en 1866 tuvo un uso de casi cien años y fue el precedente de otros cables transoceánicos como el Columbus II, colocado en 1994, y el UNITY Cable cuya instalación comenzó en 2008.

Durante el siglo XIX estos tipos de tecnologías, aún incipientes, eran utilizados y desarrollados únicamente por Estados. Sólo ellos podían pensar en una inversión para el perfeccionamiento y la evolución de las mismas. El énfasis desde un comienzo estuvo puesto en el desarrollo militar y la conexión estratégica en pos de reforzar los Estados. Era, hasta el momento, imposible pensar en la noción de boicot a sus intereses a través de estos instrumentos tecnológicos.

En 1862, en el marco de la guerra civil estadounidense, se sentó una de las bases del espionaje a través de las telecomunicaciones. Fue Abraham Lincoln quien durante su presidencia autorizó el control sobre la estructura del telégrafo en su país durante la Guerra Civil. La labor quedó en manos del secretario de guerra Edwin Stantonl, y se se encargó de espiar estadounidenses, arrestar periodistas y decidir qué mensajes podían ser enviados.

En nuestro país las líneas telegráficas existen desde 1857, con un tendido en paralelo al Ferrcarril Oeste, erigido bajo el mandato de Bartolomé Mitre. El 5 de agosto de 1874, en la Casa de Gobierno, fue la inauguración de las comunicaciones internacionales de Argentina con Europa a través de un cable de telégrafo transatlántico con Domingo Faustino Sarmiento como primer mandatario. “La conexión unía Buenos Aires y Montevideo, subía hasta Brasil hasta llegar a Pernambuco. Desde allí cruzaba el Océano Atlántico hasta Lisboa” (Zuazo, 2015).

Al otro día, el diario *La Nación* tituló: “Gran fiesta nacional”, y continuaba: “La República se halla desde hoy al habla con todos los países del mundo civilizado. De hoy en adelante, las pulsaciones del pensamiento humano podrán repercutir, casi simultáneamente, en todas las naciones de la tierra. ¡Gloria al progreso y a la civilización de nuestro siglo!”. Fue Sarmiento el primer argentino que tuvo la posibilidad, como dirigente, de impulsar una medida en favor de iniciar el camino de las comunicaciones, mucho antes de su actual y evidente significancia.

Telefonía y radio

A fines del 1800 el teléfono y la comunicación a través de ondas de radio ya eran una realidad. En 1876 Graham Bell patenta su teléfono y al año siguiente crea la empresa Bell. Ya en el siglo XX era posible la comunicación pública a través del teléfono. Por su parte la radio nace en 1894 de la mano del italiano Guglielmo Marconi quien “conjugó el aparato oscilador de Hertz, la antena de Popov y el cohesor de Branly, naciendo así la telegrafía sin hilos” (Breve historia de la radiofonía). En 1906 se realizó la primera transmisión a larga distancia por parte de R. A. Fessenden, y hay quienes lo consideran el padre de la radiofonía. Sin embargo, la radio tuvo su primera difusión pública en 1920, y en 1922 es creada la British Broadcasting Corporation (BBC) para la emisión de programas de radiodifusión.

> Con la invención del teléfono se fueron creando las condiciones para el posterior surgimiento de la radio. El nacimiento de este medio estuvo condicionado por tres factores fundamentales: descubrimientos técnicos, necesidades militares y competencia política. Los aportes de Alexander Lee de Forest, de Guglielmo Marconi y Thomas Alba Edison facilitaron la aparición de la radio, que con la magia del sonido y la palabra permitió construir y transmitir la realidad al pie del micrófono (Navarro Pujól, 2012).

De esta manera se iría configurando el sistema de comunicación global, que se irá perfeccionando durante las futuras guerras mundiales.

"Esta radio de principios de siglo de la que hablamos se caracterizaba por la insuficiencia de un factor esencial: "el ser un medio informativo con libertad de expresión". Debemos tener claro que el nacimiento de la radio en España no va ligado al concepto de información, sino al de propaganda política, y a partir de asentar esta base podremos continuar explicando la situación en la que se encontraba el medio radiofónico en sus albores en nuestra nación". (Historia de la radiofonía, Universidad de Murcia, España).

En los dos ejemplos expuestos anteriormente se deja ver cuáles fueron los cimientos al establecerse la radio como medio de comunicación masivo, tanto en Cuba como en España. Y no fue diferente en otras partes del mundo. Para este entonces el telégrafo quedaba como un instrumento arcaico, y las redes de telefonía y radio comienzan su evolución, así como también el control del Estado sobre sus habitantes.

Las guerras

Las nuevas herramientas tecnológicas desarrolladas por las fuerzas de los ejércitos fueron puestas al servicio de las dos grandes guerras del siglo. La Primera Guerra Mundial no fue sólo un enfrentamiento entre ejércitos, sino que también se trataba de una disputa cultural e ideológica incentivada por los propios gobiernos, una "guerra de creencias", como la calificó el alemán Werner Sombart. En este contexto era necesario incentivar un odio visceral contra el enemigo y que el ciudadano se alinee a las tropas de guerra por voluntad propia.

¨En la Primera Guerra Mundial, los medios de comunicación jugaron, por primera vez en la Historia, un papel importante en el desarrollo de una guerra. Un verdadero diluvio de panfletos, carteles,

caricaturas, poemas, canciones y, también, películas cinematográficas inundaban los países beligerantes¨. (Schulze Schneider, 2013)

En ese entonces la manera de llegar a la población consistía en lo que decía Schneider. Los países aliados emplearon intensamente esta metodología como medio de guerra psicológica. Todavía la radio y la telefonía no eran propiamente medios masivos de comunicación. Sin embargo, fueron pieza fundamental para la comunicación interna en el conflicto armado y también entre los líderes políticos y del ejército.

Las telecomunicaciones y su desarrollo parecían cumplir dos funciones esenciales en los enfrentamientos bélicos: la primera es la comunicación entre los altos mandos de los ejércitos para elaborar estrategias de ataque y de defensa (y por qué no un acuerdo de paz entre adversarios), es decir, lo que tiene que ver con cómo y dónde ejecutar el poder de destrucción militar. Y la segunda tiene que ver con la población civil: qué se le dice, cómo y para qué. La primera Guerra fue un buen experimento en este sentido.

Para la Segunda Guerra Mundial el panorama era otro. Los avances tecnológicos en materia de telecomunicaciones plantearon un nuevo posicionamiento de las potencias involucradas. La masividad que en la primera guerra fue equiparada por cartelería y panfletos quedaba relegada a un segundo o tercer lugar debido al alcance ahora más potente de la radiofonía. Se incluyó además la Modulación en frecuencia (FM) que permitía una alta calidad en sonido y había aparecido también la televisión.

En materia militar y armamentística fue el desarrollo del Radar lo que marcó una gran diferencia, además de la evolución de los equipamientos que se venían utilizando como las redes telefónicas o la radio. Esta herramienta permite la reflexión de las ondas de radio o electromagnéticas sobre objetos sólidos, es decir, identificar un proyectil o un ataque de tropas por parte del adversario. Fueron los ingleses quienes supieron aprovecharlo mejor en la segunda guerra.

Utilizados por los espías ubicados en territorio enemigo, los equipos de telecomunicaciones fueron otra innovación importante en el terreno de la Segunda Guerra Mundial. Estos aparatos permitían realizar operaciones de alto riesgo, sin embargo, cuanto más grande era la distancia que debían recorrer sus ondas mayores era el tamaño de los equipos, mayor el tamaño de las antenas y utilizaban también más baterías. Ser interceptados por el enemigo con uno de estos aparatos podía

poner en riesgo la operación y la vida del espía, por esta razón era fundamental que pase desapercibido. El equipo Transcreptor Aliado HF, por ejemplo, simulaba una maleta de viaje.

Durante la Segunda Guerra Mundial han jugado un papel central las agencias de seguridad, algunas bastante consolidadas para ese momento (como por ejemplo el MI5 del Reino Unido), que distintas potencias habían creado con el fin de detectar amenazas, pasando por ellas todo lo importante en materia de seguridad y comunicaciones. En trabajo en conjunto con los ejércitos, estas agencias se encargaban de espiar al enemigo y armar un mapa de sus estrategias, ya sea a través del envío de espías dobles o por interceptar sus comunicaciones, aunque estén cifradas.

Un caso clave en esta guerra fue el descifrar el código Enigma, la herramienta de cifrado de los mensajes nazis, por parte de la GC&SC (Government Code and Cypher School, la escuela de criptología británica), la cual "evitará a los barcos estadounidenses y británicos muchos sinsabores frente a los submarinos alemanes en el Atlántico Norte. También permitirá seguir a distancia el despliegue de las tropas alemanas en Europa y prever las incursiones aéreas de Luftwaffe sobre las ciudades inglesas" (Lefébure, 2014).

Agencias de seguridad

A fines del siglo XIX y principios del siglo XX, en medio del desarrollo tecnológico en materia de telecomunicaciones, los Estados potencia comienzan a crear instituciones encargadas de la seguridad interna (dentro de su territorio) y externa (contra alguna amenaza externa que pueda afectar la integridad del Estado). Ya existían antecedentes de entidades de seguridad aplicadas a empresas y bancos, sin embargo, el mapa beligerante que se estaba aproximando (o al que las propias potencias decidieron encarar) hizo de estas instituciones una necesidad.

La Rusia de los zares fue la primera en disponer de un servicio de inteligencia realmente eficaz: Okhrana.

> Esta organización se creó el 14 de agosto de 1881 como consecuencia del asesinato del zar Alejandro II de Rusia el 13 de marzo de ese mismo año. Su misión fundamental fue garantizar la seguridad de la familia imperial, pero también actuaría como policía secreta cuyo objetivo era principalmente político, es decir, la represión de todos los movimientos revolucionarios,

> encabezados por los grupos anarquistas y socialistas. Asimismo, sus funciones se dirigieron también hacia el espionaje y el contraespionaje militar, entre cuyos objetivos estaba fundamentalmente Alemania y el Imperio austrohúngaro, Gran Bretaña y Francia (Herrera Hermosilla, 2014).

Desde sus orígenes las agencias de seguridad tuvieron el objetivo de cuidar de la clase dominante y mantener el orden que éstas han establecido. Como en el caso de la agencia rusa, todas ellas han luchado contra los movimientos revolucionarios y han instaurado los mecanismos necesarios para salvaguardar el orden. La más avanzada tecnología de cada época fue puesta al servicio de ellas suscitando una retroalimentación entre seguridad, espionaje y tecnologías; engrosando (sino provocando directamente) el desarrollo de la globalización que hoy vivimos.

Las más representativas en intercepción de telecomunicaciones y espionaje

Las agencias más conocidas en cuanto a seguridad, investigaciones y servicios secretos son probablemente el FBI (Buró Federal de Investigaciones u Oficina Federal de Investigación) y la CIA (Agencia Central de Inteligencia), el primero creado en 1908 y la segunda en 1947. Tanto el cine hollywoodense como los medios de comunicación se han encargado que la humanidad sepa de su existencia con una idea muy vaga de sus operaciones a lo largo del planeta.

En 1909 el Imperio Británico creó el MI5 y el MI6 (Inteligencia Militar 5 y 6), dos servicios de seguridad e inteligencia para operar dentro y fuera de su territorio respectivamente. Más adelante es creada la GC&SC, que nombramos anteriormente, rebautizada durante la Segunda Guerra Mundial con el fin de engañar al Eje: su nuevo nombre es GCHQ (Government Communications Headquarters, Cuartel General de Comunicaciones del Gobierno).

Sin embargo, el organismo de seguridad e inteligencia que más ha tenido que ver en operaciones de espionaje sobre las telecomunicaciones y que hoy en día se encarga de la intercepción de los datos que circulan por la red, es la NSA (Agencia de Seguridad Nacional). Fue creada en 1952 a partir de las insuficiencias de la inteligencia estadounidense, llegando a su punto máximo con el caso del espía ruso William Wolf Weisband el cual se infiltró en el servicio de criptología en Virginia,

imposibilitando a Estados Unidos la capacidad de leer los mensajes secretos entre los soviéticos y los norcoreanos en un momento clave de la Guerra Fría. El trabajo de Weisband dio a la URSS una amplia ventaja en materia de telecomunicaciones, y costó la vida a más de cuarenta mil soldados estadounidenses.

"Desde su creación la NSA estuvo al servicio del ejército estadounidense, en particular de la US Air Force. Su objetivo era ayudar a aprehender la organización de la defensa aérea soviética" (Lefébure, 2014). Sin embargo, se encargó rápidamente del espionaje de sus propios ciudadanos, primero de telegramas y de redes de telegrafía con miras a producir informes para la CIA y el FBI. Luego de las redes de telefonía con "listas de personas que debían escuchar", entre ellos empresarios, políticos y líderes de organizaciones sociales, violando todas las garantías constitucionales.

Los abusos de la vigilancia de la NSA se inscriben en la historia. Los estadounidenses adquirieron muy temprano la certeza de que el hecho de disponer de una estructura eficaz de interceptación de las telecomunicaciones constituía una ventaja política y estratégica fundamental. El interés de una estructura tal es que sirve tanto para espiar a los enemigos como a los aliados (Lefébure, 2014).

Al finalizar la Guerra Fría las actividades de la NSA debieron reinventarse. Sus misiones pasaron de interceptar comunicaciones de radio cifradas o señales de radar a interceptar llamadas telefónicas que circulan por vía satelital y cables de fibra óptica, perseguir terroristas internacionales y realizar operaciones secretas argumentando la defensa, como su nombre lo dice, de la seguridad nacional.

Antoine Lefébure, en su investigación sobre el espionaje estadounidense a nivel global, expone que una vez terminada la Segunda Guerra Mundial el Reino Unido y Estados Unidos firman un tratado secreto "que apunta a mejorar la eficacia de sus intercambios para la interceptación de las comunicaciones dentro del bloque soviético". El tratado UKUSA fue firmado en 1947 y su existencia se mantuvo en secreto por treinta años, hasta que en 1976 un joven periodista las hizo públicas (más adelante hablamos de Duncan Campbell). La alianza incluía además la participación de varios países más (Canadá, Australia y Nueva Zelanda; llamada la alianza de los five eyes), los cuales se repartieron las zonas de espionaje.

Más de cincuenta años después, el eje anglo-estadounidense sigue fortalecido a través de sus dos exponenciales agencias de seguridad. Edward Snowden, de quien hablaremos en profundidad en otro capítulo, declaró en 2013 a *The Guardian* que "los hombres de la agencia inglesa son peores

que los estadounidenses", y dos meses después a través del mismo diario pudo saberse que desde 2009 hasta 2012 la NSA había subvencionado al GCHQ en al menos 100 millones de libras (119 millones de euros) para diversas operaciones (en su mayoría espionaje e interceptación de comunicaciones de estaciones secretas que no necesariamente están en sus territorios, sino que operan en otros países).

La metodología que la comunidad UKUSA utiliza para la interceptación, análisis y clasificación de las comunicaciones es a través del sistema ECHELON, considerada la mayor red de espionaje de todos los tiempos. Se sabe de su existencia desde 1976 y fue creado para interceptar las comunicaciones de la Unión Soviética y sus aliados, y se encuentra bajo la administración de la NSA. A través de este programa el eje UKUSA es capaz de capturar las comunicaciones de radio, satélite y fibra óptica, llamadas telefónicas, mensajes de texto, correos electrónicos y faxes.

En 1998, a través del STOA (Comité de Evaluación de las Opciones Tecnológicas y Científicas), es realizado un informe sobre "tecnologías intrusivas" por parte de la NSA. Al año siguiente es ordenada una investigación desde diputados europeos, y la lleva adelante el periodista Duncan Campbell. En su nueva investigación comprueba la red tentacular del sistema ECHELON, evidenciando que a través de él la NSA escucha todas las comunicaciones intercambiadas a través de Europa. Y no solo eso. Según el informe, a través de ECHELON se espía a las empresas para promover los intereses de los gigantes industriales de Estados Unidos.

Según Campbell ECHELON permite "estimar los precios futuros de los productos básicos, conocer los objetivos de los Estados durante las negociaciones comerciales, controlar el comercio internacional de armas, seguir de muy cerca la evolución de las tecnologías sensibles, o incluso evaluar la estabilidad política y la capacidad económica de un determinado país". Las investigaciones causaron un gran revuelo y un cruce de declaraciones entre autoridades europeas y estadounidenses.

Pero también secretos industriales que pongan en franca ventaja en la competición a las empresas estadounidenses sobre las europeas. E incluso datos personales de los dirigentes porque la información es poder. A excepción de Gran Bretaña, ningún país europeo forma parte de Echelon, pese a que todas las naciones de la UE son aliadas de Estados Unidos de forma bilateral y dentro

de la Organización del Tratado del Atlántico Norte. Ha sido esta exclusión lo que levantó la alarma en el Parlamento Europeo porque el que no espía es espiado.

Ante las repercusiones del informe de Campbell y la negativa de Europa, en el año 2000 el Reino Unido habilitó un marco legal que restringe aún menos la vigilancia electrónica y humana: la Ley de Regulación de Poderes de Investigación (RIPA), la cual obligó a dar acceso en forma secreta a sus redes y a sus infraestructuras submarinas a empresas de telecomunicaciones como British Telecom, Vodafone, Verizon Business, Global Crossing, Level 3, Viatel e Interoute.

> La ley RIPA le permite al gobierno vigilar la totalidad de las comunicaciones que transitan por el territorio británico, así como las actividades de Internet de cualquier persona –que, si es interpelada, está obligada a suministrar las claves criptográficas que le permitieron cifrar sus informaciones-. Por último, RIPA prohíbe la publicación por parte de todos los tribunales de todas las informaciones recolectadas, así como de todo documento que haya permitido recolectarlas (Lefébure, 2014).

Sin embargo, el ataque a las Torres Gemelas el 11 de septiembre de 2001 neutralizó la investigación del Parlamento Europeo sobre el sistema ECHELON. Post 11/9, y luego de las revelaciones de Edward Snowden en *The Washington Post*, se sabe que la NSA utiliza otros dos sistemas para interceptar comunicaciones: PRISM, que permite extraer datos de Google, Facebook, Apple y Microsoft; y UPSTREAM, que la toma de los cables submarinos y las infraestructuras de Internet.

> "Como el 80% del tráfico mundial de Internet proviene de Estados Unidos, la NSA tiene sobre este un control casi absoluto. En efecto, todos los cables submarinos de fibra óptica que existen alrededor del planeta están conectados con treinta y dos cables que transitan por Estados Unidos, veinte de los cuales llegan a la costa Oeste y doce a la costa Este. Para que ningún cable escape a su vigilancia, la NSA también cuenta con la ayuda del GCHQ inglés, debido a la proximidad histórica de ambos países, pero también debido a que muchos de esos cables submarinos que unen a Europa con América pasan por el Reino Unido" (Lefébure, 2014).

En el anexo de este trabajo añadimos una tabla con los TIERS: los principales cables que transportan los datos que comprenden internet. En el cuadro puede observarse que la mayoría son propiedad de entidades estadounidenses.

6- Acción y reacción - Herramientas y recursos en la web

Como acabamos de estudiar en el capítulo precedente, la informatización es un proceso en marcha que va modificando nuestra manera de ser en el mundo. El pasaje de tecnologías analógicas a digitales implicó transformar todos los formatos comunicacionales preexistentes al sistema binario. La disponibilidad, en términos informacionales, es ahora prácticamente ilimitada.

Que así sea no es ni bueno ni malo. Es una condición insospechada 30 años atrás, que ofrece la potencialidad de que un mensaje llegue a toda la población mundial en segundos. La red que nos conecta a todos es poderosa. Depende quién y cómo sea utilizada podrá convertirse en la más sofisticada herramienta de dominación, o la más novedosa arma de democratización de la cultura jamás creada.

En el capítulo anterior vimos cómo la estructura comunicacional surge y se afianza. También dimos cuenta que son los Estados imperiales quienes construyeron y dominan la infraestructura sobre la cual se basan estos sistemas. A medida que su uso se expande y domina las esferas de la economía, el mercado, el entretenimiento, se vuelve un foco de conflicto en tanto espacio de disputa de poder. ¿Cuáles son los riesgos de depender de un sistema informático? ¿quiénes son potenciales atacantes? ¿qué es lo que está en riesgo? ¿qué herramientas existen para hacer frente a estas problemáticas? Esos son los temas de este capítulo.

La seguridad informática

En la medida en que los sistemas informáticos se convirtieron en parte esencial de las estructuras gubernamentales, se les ha adjudicado una importancia acorde en materia de seguridad. A tal punto, en la cumbre de la OTAN de Varsovia de 2016 se declaró:

"Habiéndose constatado que un ciberataque puede ser tan perjudicial como un ataque convencional, en el campo de la ciberdefensa se han adoptado varias decisiones relevantes, una de ellas es que: El ciberespacio se reconoce como un nuevo dominio de las operaciones, al lado de los de tierra, mar, aire y espacio" (Corletti Estrada, 2017, p. 15).

Existen precedentes de conflictos cibernéticos en diversos países[1], lo cual nos evidencia que estamos ante el surgimiento de una nueva dimensión de disputa de poder, con todo lo que ello implica. Si bien en la mayoría de los casos nunca se llega a conocer a los responsables, cada año se destina más presupuesto para la defensa, y en particular, la ciberdefensa.

Pero no son los Estados los únicos actores decisivos en esta nueva dimensión en disputa. Desde una muy temprana fase del desarrollo informático existen expertos que se han dedicado a intervenir en este ámbito, con propósitos no siempre claros y muchas veces opuestos a los de las grandes instituciones. Ellos son los hackers. Hoy se entiende por hacker tanto a un experto informático que trabaja para mejorar la seguridad informática como aquél que emplea sus conocimientos para materializar algún tipo de daño. Es importante remarcar que, a diferencia de en una guerra tradicional, donde sólo tenían "poder de fuego" los ejércitos o guerrillas, en la disputa por los espacios virtuales es el conocimiento el que otorga el poder. Muchos de los mejores especialistas son reclutados para los grandes conglomerados, y otros tantos mantendrán su soberanía al servicio del software libre.

Sitios de publicación de información sensible

El hecho de que existan sitios como *Wikileaks* demuestra que no todo está perdido. Que la red, pese a su estructura centralizada y hegemonizante, tiene aún la capacidad de poseer fisuras significativas, a la vez que aún es un canal de información que, con muchos esfuerzos, puede seguir siendo libre y seguro (cuando se lucha por ello). Este portal de informaciones sensibles no es el único en su haber, pero sí el más importante dada su gravitación generada posiblemente por el accionar de su principal pero no único impulsor, Julian Assange, de quien hablamos más pormenorizadamente en un capítulo aparte.

Wikileaks es un sitio web que publica y aloja documentación sensible provista por filtraciones hechas por colaboradores anónimos. A diferencia de un sitio web tradicional, está preparado para recibir embates cibernéticos de todo tipo. En primer lugar, existe un principio que dice que ¨es más fácil encriptar información que desencriptarla¨ (Assagnge, 2013, p. 17). Con esa primera y sencilla noción, se construye el universo de procesos de criptografía que posibilita la existencia del sitio

[1] ver en Corletti Estrada (2017), p. 19

Wikileaks. La misión del sitio, según sus fundadores, es "recibir datos de parte de informantes, hacerlos públicos y luego defenderse contra los inevitables ataques legales y políticos" (Assange, 2017, p. 23).

Básicamente este sitio web permite publicar información manteniendo en secreto la fuente desde dónde fue filtrada la misma. Quienes pueden correr un riesgo por proporcionar cierta documentación sensible acuden a este sitio web para publicarla.

El equipo de trabajo que da lugar a *Wikileaks* existe desde principios de los años 90, aunque el sitio fue creado en 2006. Estamos hablando de la comunidad criptopunk, que surge a la par que la red de internet, y se conforma por especialistas de todas partes del globo. Algunos de ellos han trabajado para gobiernos o empresas, aunque su visión política del uso de la red los posiciona en la vereda de la democratización de la misma. Entre las figuras destacadas de este movimiento hallamos a Julian Assange, Jacob Appelbaum, Andy Muller-Maguhn, Jéremie Zimmermann.

En octubre del 2010 la plataforma *Wikileaks* publica 391.000 documentos del Pentágono sobre la Guerra en Irak y la ocupación estadounidense desde 2004 al 2009. La filtración fue publicada también por las ediciones digitales de *The New York Times*, *Der Spiegel*, *The Guardian* y en esta ocasión se sumaron *Le Monde* (Francia), *El País* (España), *Al Jazeera* (Qatar) y *Bureau of Investigative Journalism* (Oficina de Periodismo de Investigación).

En noviembre del mismo año publica la correspondencia secreta de diplomáticos estadounidenses, 250 mil documentos con comunicaciones entre el Departamento de Estado de Estados Unidos y sus embajadas por todo el mundo. Se trata de la mayor filtración de la historia. La publicación se hace desde la plataforma de *Wikileaks* y de manera simultánea a una cobertura de prensa de *El País*, *Le Monde, The New York Times, Der Spiegel y The Guardian*. Los datos registrados incluyen investigaciones y espionaje de las comunicaciones y los negocios de primeros mandatarios y empresas importantes de países de todo el mundo. Esta megafiltración fue llamada Cablegate: “El imperio quedó desnudo, yo no sé qué va hacer Estados Unidos, bueno, a ellos no les importa mucho esto no, pero cuántas cosas están saliendo, cómo irrespetan hasta a sus aliados, ¡cuánto espionaje!”, expresó Hugo Chávez, en ese entonces presidente de Venezuela, durante un consejo de ministros transmitido por la televisión estatal. (*El Espectador*, 13 de octubre de 2010).

“Gracias a *WikiLeaks* supimos, por ejemplo, que la embajada de EE.UU. en Madrid trató de boicotear las causas judiciales abiertas en España contra políticos y militares estadounidenses presuntamente implicados en crímenes de guerra en Irak, en las torturas en Guantánamo o en los vuelos secretos de la CIA” (Portal del *Canal Historia*, 9 de enero de 2014).

Lo que la existencia de *Wikileaks* y sitios similares viene a decirnos es: con internet no sólo podemos hacer circular los datos que las corporaciones desean. Es también un vehículo de la libertad, siempre y cuando se pongan a trabajar en ello los conocimientos (y las personas) necesarios para garantizarlo. Esta herramienta creada por Assange y sus colaboradores es apenas un vehículo para que la información llegue al público. Para que resulte exitoso el cometido hacen falta además otros dos componentes: alertadores y medios de comunicación.

Los alertadores son todas aquellas personas que acceden por algún u otro motivo a la información sensible. Por lo general se trata de personas que por su trabajo tienen acceso a bases de datos, aunque también se obtienen mediante la intrusión a los sistemas de almacenaje. Estos informantes acuden a los sitios de divulgación de información como medio de protección. Se les asegura el anonimato, y mediante un protocolo de seguridad se hace efectiva la transferencia de datos. A partir de ese momento, la labor del alertador se da por concluida. El sitio se compromete a no revelar la identidad del informante, pero eso no significa que toda la información vaya a publicarse instantáneamente. De hecho, uno de los puntos críticos de *Wikileaks* es el criterio utilizado para la publicación del material donado. Mientras que Assange era partidario de dosificar la información y someterla a un criterio determinado, Daniel Domscheit-Berg, uno de los colaboradores más activos del sitio, consideraba que no había que juzgar ni filtrar los datos sino más bien publicarlos tal cual llegaban. Este tipo de conflictos aceleraron el desgaste y fracaso de estas plataformas. Respecto al tratamiento que recibían los informantes, Domscheit-Berg dice:

> Antes de llegar a las manos de *wikileaks*, ellos (los editores) se encargaban de que los documentos con información delicada diera varios rodeos, pasasen por procesos de cifrado y de eliminación de la identidad y añadidura de ruido de fondo. Ellos mismos no podían contactar a las fuentes directas, por tales motivos, nuestros remitentes no dejaban rastro alguno en la red, ni la menor huella dactilar, ni un solo byte que pudiera delatarlos (Domscheit-Berg, 2011).

El otro componente de este engranaje son los medios. Cuando la información que llega a sitios como *Wikileaks* es muy grande, se vuelve insuficiente su publicación autónoma: se hace necesaria una interpretación de los datos y su posterior replicamiento en los medios masivos. El ejemplo emblemático de esto es el caso de panamá papers, que para lograr trascendencia contaron con la colaboración de medios de todo el mundo. El trabajo estuvo a cargo de Frederik Obermaier y Bastian Obermayer, quienes procesaron la información recibida por un alertador anónimo, y elaboraron un significativo operativo de publicación en colaboración con medios de todo el mundo. En el caso de *Wikileaks*, el caso más emblemático es el de la publicación de "Collateral Murder", video de una operación militar estadounidense en Irak, que contó con una amplia cobertura mediática al momento de su publicación.

Lo que algunos especialistas insisten en remarcar, es que, pese al auge de las plataformas virtuales, el cuestionado y crítico rol de los medios no ha perdido ni vigencia ni propósito. La congruencia y significancia de los mismos es igual de pertinente que siempre, sólo que el escenario cambia y éstos deben adaptarse. Aportar claridad en la incertidumbre, información procesada ante tanta sobreinformación, son las conclusiones a las que Becerra arriba que la influencia de la prensa es reivindicada en todos los estudios contemporáneos sobre construcción de agenda y liderazgo de opinión: "La megafiltración ha demostrado nuevamente que el mundo digital, previsto como relevo de los medios tradicionales, necesita nutrirse de la credibilidad y el oficio editorial de los grandes periódicos para alcanzar impacto público" (Becerra, 2012, p. 44).

El ocaso de este tipo de sitios quedó evidenciado al volverse insoslayable la fragilidad para hacerse cargo de la cantidad de información digital que la humanidad es capaz de producir. El criterio de publicación, que en el caso de *Wikileaks* era una decisión personal de su mentor Assange, la necesidad de contar con recursos permanentes para mantener un adecuado equipo de trabajo, fueron los principales factores que llevaron al sitio al estado crítico que marcó su final, si bien sigue online. Daniel Domscheit-Berg intentó en 2011 abrir OpenLeaks, un sitio que intentaba corregir algunas de las deficiencias de su predecesor. La principal era que no operaba como medio con un criterio de selección, sino que pretendía funcionar como buzón seguro, donde los alertadores pudieran enviar el material. Otro factor fue la administración de las donaciones, que en el caso de *Wikileaks* era una tarea que Assange nunca consideró pertinente sociabilizar. En definitiva, el dilema

principal después de la experiencia de los “ciber leaks” es que fueron incapaces de superar la obra personal, tratándose de procesos con implicancia global.

Ejemplos de ciberataques (y ciber defensas)

Ahora que ya hemos explicitado en qué consisten los sitios de divulgación de información sensible, vamos a hacer un repaso no exhaustivo por algunos de los mecanismos que estos sitios deben sostener para mantenerse disponibles para los usuarios del mundo. Este apartado está basado en gran medida en la interesante charla que Julian Assange sostuvo con directivos de Google en junio de 2011, que está documentada en el libro “Cuando Google encontró a *Wikileaks*” y en “The new digital age”, escritos por Assange y los directivos de Google respectivamente.

> -Ataque de denegación de servicios (Dos en inglés). Es el intento por parte de algún organismo de impedir el acceso a una página web mediante el envío de tantas peticiones de acceso que la página es incapaz de responder a todas. Es una forma de censura que se enfoca en neutralizar la fuente de información. Los directivos de Google le preguntaron a Assange sobre los métodos con que *Wikileaks* evadía este tipo de ataques. Su respuesta fue: ¨Siempre dispones de una forma u otra. Se pueden obtener cientos de nombres de dominio de varios tipos registrados en servidores DNS realmente grandes, de forma que si se producía un filtrado se filtraban también 500.000 dominios junto con el nuestro, y ello provoca una reacción política violenta. Cualquier dominio que incluya *Wikileaks* en alguna parte, sea donde sea, es filtrado. Esto significa que tiene que haber una variante que aún no han descubierto, pero esta variante tiene que ser lo suficientemente conocida como para que la gente se dirija a ella¨ (Assange, 2014, p. 87).
>
> -Cambios de dirección de IP. Assange explica que es clave la elección del ISP (proveedor de servicio de internet), compañía que proporciona enlaces de comunicación o espacio de servidor para crear una página web. “A la hora de elegir un ISP para una página como *Wikileaks*, es necesario considerar algunas cuestiones muy importantes, como por ejemplo ¿te apoyará este ISP en tu lucha contra la censura, o te censurará el mismo?” (Assange, 2014).

> Assange pone como ejemplo el caso de TCI Journal (Turks and Caicos Islands Jorunal). Se trata de un pequeño grupo de activistas con ideas ecologistas que se encontró con casos de corrupción y especulación inmobiliaria en las islas turcas y caicos, situadas en el caribe, unos 600 kilómetros al este de Cuba. El grupo inició una campaña a favor de la buena ordenación territorial, en oposición a estos emprendimientos. Los promotores de estos proyectos encontraron la forma de expulsar de los servidores a los activistas de las islas. Estos contrataron un ISP indio, los promotores que los habían expulsado contrataron abogados en Londres, que a su vez subcontrataron abogados en India, que se encargaron de anular también los servidores locales.
>
> Seguidamente los activistas los trasladaron a Malasia, pero ocurrió exactamente lo mismo: tan pronto como empezaron a llegar comunicados legales al ISP local, los activistas dejaron de ser rentables para el ISP. Por último, se trasladaron a Estados Unidos, pero su ISP estadounidense directamente se rehusó a aceptarlos, por lo que escogieron otro que era un poco mejor. A causa de las amenazas, los editores eran anónimos; aunque los columnistas a menudo no lo eran, la parte responsable de la publicación sí. Sin embargo, cuando los abogados de los promotores se percataron de que los acvtivistas utilizaban una cuenta de correo de Gmail, presentaron entonces una demanda en California, y como consecuencia los juzgados comenzaron a emtir citaciones judiciales, incluso contra el propio Gmail. El resutado fue que Google comunico al TCI Jorunal que tenian que trasladarse a California para defendere y que si no lo hacian, tendría que cancelar el servicio de la cuenta de correo (Assange, 2014).

Ante la imposibilidad del grupo de hacer frente a demandas de tal magnitud, se comunicaron con el grupo de Assange, que mediante los abogados pertinentes hallaron una disposición en el código estatutario de California que invalidaba la estrategia de los demandantes. Google no presentó objeción.

“Esto es un ejemplo de lo que ocurre cuando estás en un grupo bastante brillante –tenían un técnico indio muy bueno y brillantes estrategas políticos- y te propones acabar con la corrupción en tu país utilizando internet como mecanismo de publicación. ¿qué ocurre? ¡te persiguen literalmente por todo el mundo!” (Assange, 2014).

Assange indica que existen pequeños ISPs que contemplan el valor ético de lo que sus clientes publican. El ISP sueco PRQ, en conjunto con un ISP más grande llamado Banhof, se dedica a publicar contenido de refugiados. (www.prq.se). Este ISP da servicio a *Wikileaks*, a la asociación de propietarios de viviendas de EEUU, al centro de noticias del Cáucaso Kavaz, que suele recibir ciber ataques rusos, entre otros.

Unos párrafos más arriba se citó un principio fundamental que Assange enuncia. Es ese que dice que es más fácil encriptar información que desenctriptarla. Un ejemplo de ello es explicado atravéś de la función hash (picadillo en inglés), que consiste en la vinculación entre una información y una denominación abreviada de la misma. De tal manera que para acceder a la información basta con poseer el hash, que es generado por una fórmula matemática. Algunos hash se programan para que sean fáciles de recordar, a la vez que la información en sí es imposible de rastrear (para ser censurada).

Recursos web

Existen un gran número de herramientas y recursos web que están inspiradas en la preocupación por el libre acceso a la información. Dado que todo lo que concierne a internet tiene una significancia global, sería imposible hacer una lista completa o representativa de todo el universo web. Por el contrario, aquí exponemos algunas que se nos fueron presentando en nuestra investigación, y que consideramos fieles ejemplos del tipo de recursos que están disponibles en la red de redes.

-Reporteros sin fronteras. La ONG internacional Reporteros Sin Fronteras (RSF)[2], creada en 1985, tiene estatus consultivo en la ONU y se dedica a defender periodistas y personas

[2] RSF organiza sesiones de entrenamiento en seguridad digital y ofrece tutoriales gratuitos, ver wiki.rsf.org y slides.rsf.org

cercanas al ámbito de la comunicación perseguidos o encarcelados en cualquier parte del mundo. Lleva un registro de ataques a la libertad de información y prensa, ayuda económicamente a diversos medios en situaciones límite, provee asistencia en zonas de conflicto. Desde 1992 publica un manual de seguridad para periodistas, con diferentes recomendaciones y recursos.

Si bien la actividad periodística puede ser una profesión riesgosa de por sí, cuando ésta se practica en zonas de conflicto los riesgos se intensifican. En el manual publicado por RSF se da cuenta de diversos recursos que tienen que ver con los riesgos ante el uso de la tecnología. Aquí un repaso de ellos.

- Limpieza general antes de salir. La regla número uno de este manual es poseer la identidad digital más virgen posible, para que en caso de una interceptación no puedan hallar información sobre uno en sus dispositivos. Esto implica no sólo eliminar fotos y publicaciones, sino también considerar la posibilidad de emplear perfiles con nombres falsos.
- El segundo paso es instalar herramientas de seguridad informática sobre este "perfil sano". Eso implica activar un firewall (cortafuegos) y cifrar el disco rígido (a través de FileVault en Mac, o BitLocker y TrueCrypt en Windows). Otro recurso es instalar un VPN (virtual private network o red privada virtual), que cifra las conexiones a internet. Esto implica prestar atención a las redes de wifi que se utilizan. El navegador Tor Browser permite navegar de manera "segura" o cifrada, y se emplea con la VPN. El cifrado cuenta no sólo para el wifi sino también para los SMS y chats. Para correo electrónico: Thunderbird, Enigmail; para mensajería instantánea: OTR, CryptoCat, Pidgin, Adium; para llamadas telefónicas o videollamadas: Hello de Firefox o Qtox.
- Para que estas herramientas funcionen es necesario que tanto el emisor como el receptor las utilicen.
- El tercer consejo del manual es detectar los riesgos y trabajar por bloques separados. Esto quiere decir que, dado que es imposible mantener bajo seguridad irrestricta toda la información que circula por nosotros, es conveniente detectar y aislar bajo un halo de máxima seguridad aquellos datos que consideramos de mayor importancia o que pueden traernos un mayor riesgo. Algunos ejemplos de esta medida son: utilizar una tarjeta de

telefonía prepaga para una llamada determinada, emplear una casilla de email para una comunicación concreta, etc.

- Otro punto fundamental es el especial cuidado a tener sobre los celulares inteligentes. Si se trata de operaciones en terreno, donde el factor de riesgo puede ser la ubicación, es preferible emplear celulares básicos, con tarjetas prepagas y chips que contengan la mínima información necesaria. El smartphone es en sí mismo un dispositivo que indica dónde estamos situados, por lo cual, si eso podría ser un riesgo, hay que evitar su uso. "El smartphone es, a menudo, un compendio de datos tuyos. Ten en cuenta que, si te capturan y te requisan el teléfono móvil, toda la información que contiene (fotos, contactos, historial de navegación o llamadas) podrían volverse en tu contra o poner en peligro a otras personas." (Manual RSF, 2017, p. 75).
- EDRI (https://edri.org) es una asociación de organizaciones civiles y de DD HH con injerencia en el continente europeo. Se avoca a defender los derechos y libertades en el entorno digital. Desde su web se pueden realizar donaciones, suscribirse al material que publican, enterarse de eventos en los distintos países, consultar bibliografía, etc.

Por ejemplo, una de las organizaciones que integran el EDRI es xnet, de Barcelona. Al tratarse de una entidad de habla hispana investigamos un poco más la actividad de esta organización respecto de las demás. Entre las actividades que desarrollan encontramos reclamos y propuestas a leyes vigentes, como por ejemplo la primera ley de alertadores de la unión europea fue promovida por Xnet. Otras actividades impulsadas por Xnet: conformación de grupos ciudadanos de políticas digitales, presentaciones de libros sobre el tema, manifiestos, cartas abiertas, etc.

Existen muchas organizaciones similares en todo el mundo. Ejemplos de ella: la quadrature du net, en Francia. La mayoría comparten visiones, aunque cada una tiene sus características propias. Por lo general todas coindicen con defender la libertad de expresión en la red, lo cual las lleva a generar intensos debates en materia de software, derechos de autor, políticas estatales e intraestatales, privacidad, etc.

Otra organización integrante del EDRI es Nodo 50, un ISP (proveedor de internet) orientado a proveer servicios sin ánimos de lucro a movimientos sociales y agrupaciones de izquierda de diversos estados. (agregas masISPs independientes, como la red francesa de datos, de Bayart).

- https://buggedplanet.info – Este sitio es una wiki (enciclopedia colaborativa online) específicamente de SIGINTs de todo el mundo. El sitio mantiene una lista de proveedores de armas cibernéticas y tecnologías de vigilancia de todos los países del mundo. Funciona a modo de base de datos y se nutre y perfecciona mediante la colaboración de usuarios, como todas las wikis.
- Cryptophone.de Esta empresa alemana comercializa diversos modelos de teléfonos "antiespías", que únicamente garantizan seguridad en las comunicaciones si se utilizan para comunicarse con otro modelo de la misma firma. Utilizan tecnología GSM igual que los celulares convencionales, sólo que están encriptados a prueba de interceptaciones.
- Pentesting o examen de penetración – Es un recurso que emplean desarrolladores para identificar falencias, vulnerabilidades y errores de seguridad que puedan tener los sistemas informáticos. Para ello se ataca al sistema en cuestión con diversos métodos para encontrar fallas de seguridad. Diaspora – Es una red social basada en el software libre de mismo nombre. Está formada por un grupo de servidores independientes que interactúan para formar la red, por lo cual esta es siempre descentralizada y carente de un dominio central. La red no es propiedad de ninguna empresa, por lo que se la considera una red libre y segura.
- https://www.freehaven.net/anonbib/ - Un vasto compendio de bibliografía anónima sobre seguridad informática, en inglés. La base de datos corresponde al proyecto Free Haven, que es a su vez una plataforma que brinda seguridad y anonimato para los documentos que aloja. En el sitio explica que actualmente no está activa, si bien todos los documentos están disponibles. La lógica de creación colectiva, característica del software libre, se ve reflejada en la forma en la que anuncian los problemas: listas de defectos, posibles soluciones, distintas versiones, todo a corregir, todo a disposición de quien lo quiera ver.
- http://he.net/ - Hurrican electric: información técnica sobre las rutas de internet

Telefonía y mensajería

"El celular es un dispositivo de rastreo que también permite hacer llamadas"
Julian Assange

Además de las citadas herramientas pensadas para los profesionales de la comunicación, también se han desarrollado softwares orientados al consumo masivo para dar respuesta a los peligros que implica el uso de las aplicaciones que las grandes corporaciones por parte de los usuarios corrientes.

Las aplicaciones más utilizadas hoy en día en los países occidentales están proporcionadas por los mismos proveedores. Tal es el caso de Facebook, Instagram y Whatsapp. Si bien dicen resguardar la información de sus usuarios, ya se ha revelado insuficiente esa medida ante la petición (o por qué no, compra) de gobiernos u entidades jurídicas autorizadas, como veremos en el próximo capítulo con las revelaciones que posibilitó Edward Snowden.

El problema no es que una entidad autorizada solicite la información de los usuarios con motivos de seguridad. El problema es que la aplicación conserva esos datos, cuando no debería hacerlo. Ante eso, la única alternativa consiste en ser consciente del riesgo que implica ceder voluntariamente los datos personales a empresas oligopólicas, y utilizar aplicaciones diferentes.

De cada aplicación de uso masivo existe siempre una versión similar de código abierto. Por ejemplo así como existe Whatsapp existe telegram, una aplicación de mensajería instantánea de similares prestaciones. Si bien la ventaja inicial de telegram era su cifrado (mecanismo para garantizar el anonimato de la comunicación), desde que whatsapp "corrigió" esta característica mejorando los protocolos de seguridad de su aplicación, aún queda el pequeño detalle de que los servidores de la primera son propiedad de Facebook, mientras que telegram es una inventiva de los rusos Nikolai y Pavel Dúrov, con sede principal en los Emiratos Arabes.

El caso de Google es más complejo. Las prestaciones del gigante de internet crecen día a día. Comenzó como un simple indexador de contenidos y creció hasta ofrecer la más poderosa gama de recursos web. La misma comprende su propio navegador, servicio de email doméstico y empresarial, buscador, servidor online, mapeo de casi todo el mundo, etc. Sería imposible plantear

la solución a Google con aplicaciones parecidas, porque el problema en sí mismo es la concentración oligopólica que posibilita su existencia, más que las utilidades en sí mismas.

La herramienta más utilizada para navegar por internet sin dejar rastros es Tor, un navegador que se enlaza a la red por medio de un sistema de conexión más complejo (de ahí su lentitud) pero a la vez infinitamente más seguro. Los promotores de la seguridad informática despotrican de Tor, aduciendo que es la vía de acción de los ataques cibernéticos, lo cual es cierto, pero desestima la importancia del anonimato en la red. (Corletti Estrada, 2017, p. 36)

Sobre servicios de host alternativos a Google drive ya analizamos la existencia de ISPs en el apartado anterior. Existen también sitios web de mapas e imágenes satelitales de mayor resolución que Google earth y Google maps, como por ejemplo https://imagehunter.apollomapping.com/ o gaia gps.

Durante las revueltas que ocurrieron en Egipto en 2011, el gobierno interrumpió el sistema de telefonía movil. En su entrevista con Google, Assange explica que los dispositivos móviles tienen la capacidad de comunicarse mediante ondas de radio. En una ciudad, por ejemplo, suele haber una alta densidad de teléfonos móviles, haciendo que exista una posible comunicación sólo entre los teléfonos, a modo de red de usuarios.

La necesidad de una estación intermedia se debe principalmente a que cada modelo de teléfono recibe y transmite señales a frecuencias diferentes. Pero ante la flexibilidad del mercado, y la necesidad de los fabricantes de poder vender los dispositivos en distintos países, los teléfonos smart están teóricamente capacitados para funcionar a diversas frecuencias, volviendo (aún en teoría) posible la tesis de Assange. Aún para teléfonos que no son lo suficientemente flexibles, se están desarrollando tecnologías que permitan a los teléfonos comunicarse entre sí.

“Durante los períodos revolucionarios, las personas muy implicadas necesitan ser capaces de transmitir rápidamente información sobre su entorno para adaptarse dinámicamente a ella y planificar la siguiente estrategia. Si el gobierno desconecta el sistema de telefonía móvil, y únicamente los servicios de seguridad son capaces de comunicarse, estos servicios cuentan con una enorme ventaja” (Assange, 2014). Generar una red de comunicación que no dependa de los servicios que el Estado pueda controlar, “no significa que el gobierno vaya a ser derrocado necesariamente, sino que tendrán que hacer más concesiones” (Assange, 2014).

Otra situación en la que puede ser necesario establecer una llamada segura es durante una filtración. Daniel Domscheit-Berg realizó, durante sus primeras experiencias junto a Wikileks, innumerables conversaciones desde un locutorio, o empleando tarjetas SIM compradas. “Aveces me compraba varios números consecutivos, buscaba en internet alguna familia numerosa que hubiera colgado fotos de una fiesta de aniversario en un blog y utilizaba sus nombres y direcciones para registrar todas las tarjetas SIM”. (Domscheit-Berg, 2011).

En este capítulo dimos cuenta de diversos problemas alrededor del uso en clave comunicacional de herramientas y dispositivos digitales. Dimos también una visión esperanzadora, al hablar de un sinnúmero de proyectos alternativos y recursos orientados de alguna manera a contrarrestar el orden establecido por los principales proveedores de servicios: los servidores más grandes, las generadoras de contenidos más importantes, las redes sociales de mayor uso, los medios de comunicación masivos. Ante esa estructura dominante, que evidencia defectos y peligros en todos sus estratos por una cuestión esencial relativa a su carácter hegemonizante, existen resistencias, caminos posibles, alternativas.

La red, como toda arma potencial, es un instrumento de poder y de lucha. Y así como vimos las implicancias del uso pasivo, aún es un medio en donde la sociedad puede manifestarse con libertad. Por eso existe la disidencia, encabezada desde su brazo más comprometido por la comunidad hacker, pero no sólo por ella. La cantidad de recursos, colectivos y comunidades que forman parte de la red solidaria que lucha por mantener una virtualidad libre es enorme, y eso se ve reflejada en la diversidad y variedad de herramientas y recursos de los que hablamos en este capítulo.

Es importante remarcar que el universo de la virtualidad es cada vez más vertiginoso, por lo que toda necesidad de seguridad informática debe resolverse mediante una actualización indispensable de las herramientas disponibles, ya que el mapeo aquí realizado es sólo ilustrativo y fluctúa constantemente.

7- Casos y protagonistas

-O la prueba de la permeabilidad de la información-

"Ni la filtración como tal ni el discurso libertario del líder de *Wikileaks*, Julian Assange, constituyen en sí mismas grandes novedades" Shila Vilker

Podemos referirnos al telegrama Zimmermann, un mensaje cifrado interceptado por uno de los servicios de inteligencia británicos en el año 1917, en plena Guerra Mundial, como una de las primeras filtraciones, ocurrida en medio de la gran disputa entre Estados modernos. Este comunicado, que utilizaba el código secreto de la diplomacia alemana, fue enviado por el Ministro de Asuntos Exteriores alemán Arthur Zimmermann al embajador alemán en México Heinrich von Eckardt para proponer una alianza entre Alemania y México en contra de los Estados Unidos. Para ello fueron utilizados dos circuitos cablegráficos (uno sueco y otro estadounidense). Ver telegrama en el anexo.

> Alemania estaba dispuesta a suministrarle armamento, ayuda financiera y a permitir que México recuperara los territorios de Texas, Nuevo México y Arizona, perdidos durante la guerra de 1846-1848. (…) Los servicios de inteligencia naval británicos interceptaron los mensajes ya que tanto el cable sueco como el estadounidense tocaban tierra en el Reino Unido y habían sido pinchados a principios de la guerra (*La Vanguardia*, 16/01/2017).

Lo que para Alemania significaba intentar convencer a Carranza, el entonces presidente mexicano, de entablar un conflicto con Estados Unidos para mantenerlo distraído de lo que ocurría en Europa, resultó ser finalmente un tiro por la culata. Lo que generó esta filtración fue que Estados Unidos apresure su entrada a la Primera Guerra Mundial, luego de mantenerse neutral, tres meses después del envío del cablegrama.

Papeles del Pentágono

El 13 de junio de 1971 ocurrió una de las primeras filtraciones que tuvo repercusión pública y que llevó al entonces presidente de Estados Unidos, Richard Nixon, a intentar silenciar a la prensa: los Papeles del Pentágono. Dos ex militares empleados en el Departamento de Defensa del país norteamericano, Anthony Russo y Daniel Ellsberg, fotocopiaron en secreto las siete mil páginas de

un documento clasificado como "Top secret –Sensitive", llamado "Relación Estados Unidos – Vietnam 1945 – 1967: Un estudio preparado por el Departamento de Defensa".

Ante la negativa de varios senadores opositores a la guerra de Vietnam de difundir los documentos, Daniel Ellsberg decidió filtrarlos a la prensa para que su contenido no se mantenga en secreto. Lo hizo a través de Neil Seerhama, reportera de *The New York Times*. Las repercusiones fueron grandes a nivel nacional como internacional, debido a que el contenido de los Papeles dejaba al descubierto que una serie de asesinatos políticos, imposiciones e intervenciones en Vietnam eran responsabilidad de Estados Unidos; sumado que en el asunto habían implicados cuatro presidentes norteamericanos: Harry Truman, Dwight Eisenhower, John F. Kennedy y Lyndon Johnson.

La censura por parte del entonces jefe de Estado norteamericano no se hizo esperar y después de la primera publicación de una serie de siete a publicarse en *The New York Times*, logró interrumpirla fundamentando bajo la Ley de Espionaje del año 1917 en su Sección 793[3]. Sin embargo, días más tarde la Corte Suprema de Justicia autorizó al diario retomar las publicaciones. Ante esta arremetida del gobierno, Ellsberg ya había decidido filtrar los documentos a otros 18 diarios incluyendo a *The Washington Post*. A causa de estas filtraciones Daniel Ellsberg es considerado el primer "alertador" (whistleblower) de la historia, y nació con él la generación "W".

"La publicación de los Papeles del Pentágono marcaron en su época una victoria judicial a favor de la libertad de expresión en Estados Unidos y en contra de los intereses del gobierno, así como un avance para los informantes que buscan equilibrar los abusos de poder en los que pueden caer los Estados bajo el cobijo de la secrecía." (Sánchez Onofre, s/f, p. 1)

[3] En ella se establecen castigos a quien "…teniendo de manera legal posesión, acceso o control sobre cualquier documento, escrito, libro de códigos, libro de señales, dibujo, fotografía, negativo fotográfico, plano técnico, plan, mapa, modelo, instrumento, aparato, o nota relativa a la defensa nacional, o información relativa a la defensa nacional, respecto de la cual el poseedor tiene razones para creer que podría ser utilizada para lesionar a los Estados Unidos o en beneficio de cualquier nación extranjera, comunica voluntariamente , entrega, transmite o hace que pueda ser comunicada, entregada o transmitida, o intenta comunicarla, entregarla, transmitirla hacer que se comunique, entregue o transmita a cualquier persona que no tenga derecho a recibirla, o la conserva, o falla en la entrega al funcionario o empleado de los Estados Unidos facultado para recibirla".

Watergate

Un año más tarde, en 1972, el presidente Richard Nixon se vio inmiscuido en un nuevo escándalo de espionaje y filtraciones que terminó en 1974 con su renuncia como presidente de los Estados Unidos, la única de un mandatario estadounidense en la historia. El caso es conocido como Watergate, nombre del edificio donde el Partido Demócrata, el opositor al del primer mandatario, tenía su cuartel general para las elecciones de 1972 en las que Nixon fue reelegido por una amplia mayoría.

En junio de 1972 cinco personas entraron de manera ilegal en el edificio para revisar archivos, fotografiar y colocar instrumentos de escucha. Entre los detenidos se encontraba James McCord Jr.,un ex agente del FBI, el cual había formado parte del Comité de Reelección del Presidente Nixon. Luego de ser acusados de robo y espionaje los detenidos se declararon culpables.

Sin embargo, una investigación llevada adelante por los periodistas Jonathan Bernstein y Bob Woodward del reconocido medio *The Washington Post* terminó, años más tarde, por poner en jaque la Administración Nixon. Los reporteros descubrieron vínculos entre los culpables del caso Watergate y los hombres más directos al presidente, y fueron guiados por un informante que poseía un puesto sensible en la Administración del presidente, apodado Garganta Profunda.

Nixon ganó las elecciones, aunque a medida que la investigación avanzaba se encontraba cada vez más entre la espada y la pared. Una carta de McCord Jr. al juez de la causa, en la que expresaba que estaban recibiendo presiones para callarse y declararse culpables, terminó por dar el giro que orquestó a otros medios de comunicación. El Senado inició una comisión de investigación y al dar con los asesores de Nixon fueron develadas distintas maniobras como pagos secretos a los acusados para mantener el silencio y grabaciones secretas a través de magnetófonos ocultos.

Durante el juicio con las pruebas irrefutables de las extorsiones de Nixon y sus hombres, los jueces resolvieron el debate con una votación de ocho a cero contra el presidente. El propio Partido Republicano le soltó la mano y el 8 de agosto de 1974 Richard Nixon anuncia su renuncia como presidente de los Estados Unidos. Un año antes *The Washington Post* había recibido el premio Pulitzer de periodismo a raíz de las investigaciones de este caso, gracias a la labor de Woodward y Bernstein.

Duncan Campbell

En mayo de 1976, Duncan Campbell, un joven científico estudiante de un doctorado en física en la Universidad de Oxford, publica junto a Mark Hosenball, luego de un mes de investigación, un artículo en la revista londinense “Time Out”. El informe exhibe las actividades secretas de la NSA y el GCHQ desde 1947 en materia de espionaje y escuchas. “…Habían logrado sacar a la luz el funcionamiento interno de los servicios de inteligencia angloestadounidenses dedicados a la inteligencia electromagnética” (Lefébure, 2014).

A partir de la publicación del artículo, los jóvenes son perseguidos. Hosenball es expulsado de Gran Bretaña y Campbell, que logra escapar a esta sentencia por demostrar que sólo utilizó material de acceso público, está en la mira de los servicios secretos (particularmente del MI5). Tiempo después su casa es registrada por la policía y encuentra casi mil páginas de documentos que la justicia británica consideró como informaciones del sistema de comunicación de la defensa nacional. Campbell es considerado culpable, condenado y luego puesto en libertad condicional.

Años más tarde, en junio de 1980, Duncan Campbell publica un artículo en el periódico The New Statesman en el que revela que la NSA espía a su aliado más cercano, el Reino Unido, a la vez que éste espía al resto del mundo. En 1988 el periodista volvió a publicar un importante artículo, en el cual saca al descubierto el sistema de vigilancia ECHELON en el marco del programa P415, explicando su funcionamiento y la metodología de los Five Eyes de distribución de las zonas de espionaje. Según Campbell el GCHQ es “de lejos el componente más importante de la inteligencia británica” y contaba en ese entonces con cerca de quince mil operadores y recibiendo 500 millones de dólares por año.

Nuevo milenio, nuevos artilugios

El atentado del 11 de septiembre de 2001 fue la excusa perfecta para los Estados imperiales de reforzar su seguridad, engrosando los presupuestos a sus ejércitos y agencias de inteligencia. El enemigo fue apodado terrorismo y bajo este marco entraron aquellos que pudieran llegar a generar algún tipo de desestabilización, con este pretexto se dio carta libre a los organismos de defensa para controlar y vigilar a toda la población.

> En los cinco años que siguieron a los atentados, el presupuesto asignado a la NSA aumentó a más del doble, pasando a representar entonces más del 20 % de los gastos del conjunto de los servicios de inteligencia. (…) De 2000 a 2013, la NSA recibió más de 40.000 millones de dólares de inversión y contrató a cerca de 10.000 personas. Pero también se topó con un problema fundamental: la necesidad de acrecentar la capacidad de almacenamiento de sus servidores informáticos para conservar la enorme cantidad de datos digitales recolectados cotidianamente por sus múltiples programas a través del mundo (Lefébure, 2014, p. 144 y 205).

Los organismos de defensa más poderosos a nivel internacional están redoblando sus inversiones y esfuerzos en la Red, trabajando secretamente para no ser descubiertos por los agentes de ese enemigo invisible al cual combaten, incluso si tienen que pasar por encima de las libertades individuales. Ya sea a través de programas de vigilancia masiva completamente secretos (un ejemplo entre tantos es Stellar Wind, que le permitió a la gestión de Bush almacenar datos telefónicos) o a través de armas cibernéticas destinadas a insertarse y destruir instalaciones enemigas (por ejemplo el virus Stuxnet, también de la NSA). Fue Edward Snowden quien dio a conocer públicamente la existencia de estas herramientas.

Julian Assange

"Cualquier reforma a gran escala debe basarse en la información, porque la información que se extiende como un virus es la que puede conseguir esas reformas", dijo Assange en una entrevista realizada por dos reporteros de la televisión sueca. Su nombre recorrió el mundo por ser el creador y editor en jefe de *Wikileaks*..

Esta metodología que reserva la fuente de la información ha derivado todos los ataques directamente sobre *Wikileaks* y más particularmente sobre Julian Assange, la cara visible de la organización. Sin embargo, su historial inició años antes, cuando en su juventud comenzó a interesarse por la informática y luego desarrolló una gran habilidad en el dominio de esta materia.

Básicamente, Assange y los activistas considerados como criptopunks tenían conocimiento de cómo se estaba estableciendo la Red como un campo de batalla, donde la conectividad en los niveles de la globalización tendría un efecto total sobre la población. Fueron ellos quienes entendieron que los hilos del entramado comunicacional estarían en quien tenga la supremacía en internet, cuya

creación y puesta en funcionamiento fueron planeadas con este objetivo. Es así que en la década del noventa se da lo que ellos llaman la "primera guerra criptográfica", en el marco de internet.

> Cuando los activistas criptopunks empezaron a divulgar sólidas herramientas criptográficas como software libre, la administración estadounidense tomó medidas para impedir que dichas herramientas criptográficas fueran usadas efectivamente. Washington clasificó la criptografía como munición de guerra y restringió su exportación; trató de imponer tecnologías deliberadamente vulnerables para que las autoridades siempre pudiesen desencriptar la información, y trató de implementar el polémico esquema de "depósito en custodia de claves" (Assange, 2013, p. 42)

La disputa entre los activistas y las corporaciones evidenció nuevas complejidades en el entramado comunicacional actual, siendo la Red el espacio por excelencia de la manifestación cultural en todo el planeta y en cual se desarrollan nuevas prácticas, nuevos intereses, nuevas pujas y nuevos riesgos. La hegemonía de las potencias mundiales sobre las nuevas tecnologías es la que marca cómo debe establecerse la conectividad a lo largo del globo, y más que un servicio para la sociedad, internet puede ser la nueva herramienta de dominación. Esto es lo que los activistas como Julian Assange evidenciaron e intentaron combatir.

Assange en Wikileaks

La primera experiencia directa de Assange con la justicia por su actividad como hacker se dio a principios de la década del noventa, cuando siendo todavía un adolescente supo detectar errores de seguridad en computadoras de diversas organizaciones. Entre ellas una universidad australiana y el grupo de telecomunicaciones Nortel. Esta hazaña la realizó en conjunto con los integrantes de la organización "Gusanos contra los asesinos nucleares", un grupo de jóvenes hacktivistas. Unos años más tarde, en 1994, Assange fue multado por la justicia por este caso, y luego puesto en libertad por buena conducta.

Sin embargo, su vida no llamó verdaderamente la atención ni supo hacerse de verdaderos enemigos hasta la creación del sitio *Wikileaks*. A través de este sitio web Julian Assange se metió en una jurisdicción compleja.

En el año 2009 un soldado llamado Bradley Manning (posteriormente Chelsea Manning), que tenía acceso a documentos clasificados sobre la guerra en Afganistan e Irak, hizo llegar el video de un ataque aéreo por parte de soldados estadounidenses sobre civiles iraquíes en Bagdad, filmado en desde el helicóptero que propinó la balacera asesinando a doce personas incluidos dos periodistas de la agencia Reuters. El video de cuarenta minutos fue publicado en abril del año 2010 por *Wikileaks* y titulado "Asesinato colateral"; los hechos datan del 12 de julio de 2007 y al ser revelados causaron gran conmoción en la opinión pública.

Más aún cuando tres meses después, a través de un trabajo articulado con los medios *The New York Times* (EEUU), *The Guardian* (Reino Unido) y *Der Spiegel* (Alemania), fueron publicados 77.000 documentos sobre la guerra de Afganistan que fueron facilitados por *Wikileaks*. En ellos se exponían datos sobre víctimas de civiles por parte del ejército estadounidense, operaciones de combate y conexiones con servicios secretos. La filtración fue inmediatamente condenada por la Casa Blanca.

A mes siguiente, en agosto, la fiscalía sueca abre una investigación contra Assange por presunto acoso sexual, y queda con orden arresto en ese país. Sin embargo, no se habían realizado las denuncias formalmente, pero la policía permitió iniciar las investigaciones por la posibilidad de que abandonara el país. Según él, los cargos no tenían fundamento. (Nueve años más tarde, en noviembre de 2019, la Fiscalía sueca cerró definitivamente la investigación por "debilitamiento de las evidencias y la falta de base para una acusación"; *Infobae* 19 de noviembre 2019).

Las causas que acorralaban al informático, además de las persecuciones políticas y diplomáticas, tenían que ver con dos órdenes de arresto en que se lo acusaba de violar a dos mujeres. Hasta el 2017 estuvo detenido, y nunca se logró comprobar si fue culpable de las acusaciones. "Detenido durante 7 años sin cargos mientras mis hijos crecían y mi nombre era vilipendiado. Ni olvido ni perdono", fueron las palabras de Assange en Twitter.

En 2012, tras considerar que sus derechos podrían continuar siendo violados, la cancillería de Ecuador le concedió asilo político en su embajada en Londres, siendo Rafael Correa el presidente

ecuatoriano. Incluso en el año 2017 le fue concedida la ciudadanía de aquel país. Sin embargo, ya por 2019, con Lenin Moreno como presidente, le fue quitado el asilo y también la ciudadanía. Es entonces encarcelado en la prisión de máxima seguridad de Belmarsh, Inglaterra, mientras se lo amenaza con extraditarlo a Estados Unidos, donde enfrentaría hasta 175 años de prisión o incluso la pena de muerte.

Edward Snowden

El otro caso que ha tenido fuerte repercusión a nivel global a causa del alto valor de la información develada es el de Edward Snowden, un joven estadounidense que, a los 29 años, siendo un empleado de gobierno de alto nivel en la comunidad de inteligencia de su país, realizó una filtración programada con los medios de comunicación más importantes e influyentes del mundo. Lo publicado por Snowden correspondía a documentos clasificados de alto secreto sobre programas informáticos de vigilancia masiva llevados a cabo por la NSA de Estados Unidos y por el GCHQ del Reino Unido.

Snowden trabajaba para Booz Allen Hamilton (una de las empresas de consultoría y gestión más importante de EEUU) como analista de infraestructura para la NSA en Hawai cuando decidió convertirse en un "alertador". Trabajó como ingeniero de sistemas, administrador de sistemas, asesor principal para la Agencia Central de Inteligencia (CIA) y como oficial de sistemas de información de telecomunicaciones. Su acreditación era "Ultrasecreto", lo que le permitía el acceso a informaciones de cualquier clasificación a través de una autorización especial llamada PrivAcc (Acceso Privado).

Para que las revelaciones se sostengan y tuvieran un respaldo estructural que permitan su conocimiento sin ser tergiversados o censurados en el proceso de publicación, fue necesario un procedimiento cauteloso e inteligente por parte del alertador. Por eso, los archivos que tenía en su poder no fueron publicados todos de un solo golpe, sino de manera dosificada, a sabiendas de lo que podría ocurrir sin una planificación precisa.

> Snowden sabe que es imposible acometer contra entidades tan poderosas sin pagar un precio alto. Leyó en la prensa las terribles condiciones en las que se encuentra detenido el joven soldado estadounidense alertador Bradley Manning, sometido a un aislamiento penitenciario máximo por haber transmitido documentos militares clasificados a *Wikileaks*, en 2010. También

> vio como fue hostigado Julian Assange, el fundador del sitio, recluido desde junio de 2012 en la Embajada de Ecuador en Londres. “Entiendo que me harán pagar por mis acciones y que haber hecho pública esa información sella mi condena a muerte”, explicará más tarde a los dos periodistas que publicarán los primeros artículos (Lefébure, 2014, p. 39).

A fines de 2012 Snowden se contactó vía internet con Laura Poitras, una distinguida documentalista estadounidense que ya había sido puesta en la lista de vigilancia de la NSA tras la publicación de su documental Flag Wars. A través de mensajes cifrados, le informó que poseía en su haber una cantidad de documentos clasificados y ultrasecretos de las agencias de seguridad más importantes de EEUU y Reino Unido, y que en ellos se evidenciaba una red global de negocio y espionaje estatal que hasta ese momento no era de público conocimiento.

Snowden le comunicó a Poitras que creía conveniente contactarse con Glenn Greenwald para realizar las publicaciones, ya que su carrera como periodista lo había llevado a conocer ampliamente sobre las filtraciones trabajando para *The Guardian* en el caso *Wikileaks*. Tras mantener varias conversaciones cifradas y comprender que lo que estaba ocurriendo podría cambiar completamente sus vidas, acuerdan un encuentro en Hong Kong. El informático sabe cómo funcionan los tentáculos del espionaje que está a punto de denunciar, por eso siempre prevé cada paso y el 20 de mayo parte hacia allí. Greenwald, que en ese entonces residía en Rio de Janeiro, viaja a Nueva York para encontrarse con Poitras y allí preparar la publicación de los artículos a publicar junto al editor estadounidense de *The Guardian*. El 1 de junio viajan juntos a Hong Kong.

Ese mismo día Snowden se reúne con Poitras y Greenwald tras entablar un código de encuentro en la esquina de un restaurante. Una vez juntos se dirigieron a la habitación del informático en el Hotel Mira. Se reunieron allí por varios días tomando precauciones precisas para no ser descubiertos a través de sus dispositivos. Durante esos días Snowden les mostró la documentación que tenía en su poder, les explicó cómo funcionan los mecanismos de espionaje y el gran aparato de vigilancia mundial; y cómo estos violan los derechos de millones de personas en todo el mundo.

Un hecho no menor protagonizó el periodista Barton Gellman de *The Washington Post*, quien también recibió información de Edward Snowden para que forme parte del equipo de publicaciones. Sin embargo, antes de comenzar el trabajo consultó con *The Washington Post* sobre el alcance de impacto que estas podrían tener, y los directivos del medio se pusieron en contacto con las autoridades estadounidenses para consultarles si la información recibida por su periodista podía

afectar la seguridad nacional. Gellman dejó al medio que trabajaba fuera de la primicia y a Snowden decepcionado: las autoridades estadounidenses ya estaban al tanto que a la brevedad sería revelada información sensible, aunque sin saber su alcance.

La hora de publicar

Para las primeras publicaciones y el armado de las notas, fue sumado por Greenwald el periodista de gran trayectoria Ewen MacAskill, también de *The Guardian*, quien entrevistó a Snowden y tuvo acceso a la documentación recopilada por el informático en los encuentros en el Hotel Mira.

La primera publicación se realizó el miércoles 5 de junio en *The Guardian*, y reveló una orden judicial que solicitaba a Verizon (una de las empresas más importantes de telecomunicaciones en Estados Unidos, con aproximadamente 113 millones de clientes) la transmisión diaria de las comunicaciones de sus abonados a la inteligencia estadounidense (NSA). El dictamen estaba avalado por el Tribunal de Vigilancia de Inteligencia Extranjera (FISC) y catalogado como secreto. El documento finaliza así:

Nadie debe revelar que el FBI y la NSA pidieron u obtuvieron informaciones por medio de esta orden. (…) Toda persona que quisiera transgredir esta interdicción o la llevará a cabo deberá ser denunciada al director del FBI" (Lefébure, 2014, pág 55).

Al día siguiente se realiza la próxima publicación: en *The Washington Post*, por Laura Poitras y Barton Gellman. Minutos después le sigue otra en *The Guardian*, por Glenn Greenwald y Ewen MacAskill. Las noticias revelan información sobre Prism, un programa de vigilancia de la NSA en el cual se invierten unos veinte millones de dólares al año. La acción de Prism es "interceptar información de nueve de las principales empresas estadounidenses de Internet, directamente de sus servidores centrales, de donde extraen los chats de audio y video, las fotografías, los correos electrónicos, los documentos y los identificadores de conexión, lo que les permite a los analistas llegar hasta blancos extranjeros, según un documento ultra confidencial". (*The Washington Post*, 6/6/2013).

Las empresas de internet a las cuales el artículo se refiere son Microsoft, Yahoo, Google, Facebook, Pal Talk, AOL, Skype, Youtube y Apple. Sus directivos desmintieron inmediatamente la transferencia de los datos a las oficinas del gobierno estadounidense, y lo hizo también el presidente Barack

Obama, indicando que nadie escucha las conversaciones de la gente y que es importante "balancear" la protección de la vida privada y las exigencias de la lucha antiterrorista. *The New York Times*, sin embargo, publicó al día siguiente en su editorial que "la administración (el gobierno estadounidense) ha perdido toda credibilidad sobre el tema".

Snowden deja el anonimato

Tan solo tres días después de la última publicación que generó un revuelo mundial al exponer el aparato de espionaje de las agencias de seguridad de EEUU (NSA y FBI), y junto con ellas a las empresas de telecomunicaciones más importantes del mundo, Edward Snowden se presenta como el responsable de las filtraciones. Fue a través de una entrevista realizada por Greenwald y filmada por Poitras, un video de 12 minutos publicado por *The Guardian* el 9 de junio.

Allí se veía al joven de 29 años presentándose y exponiendo públicamente qué fue lo que lo motivó a tomar documentación clasificada y hacerla pública. Reconoce también haber ingresado a trabajar en Booz Allen Hamilton porque le permitía recoger información sobre los programas de vigilancia mundiales de la NSA. "Me niego a vivir en un mundo en el que cada cosa que digo, cada cosa que hago es grabada, en un mundo en el que no hay privacidad, por lo que no hay espacio para el pensamiento libre", expresó Snowden frente a la cámara de Poitras en lo que sería su primera aparición pública luego de convertirse en alertador.

El día 12 de junio Snowden ofreció una entrevista exclusiva al *South China Morning Post*:

"No estoy aquí para ocultarme sino para revelar actos criminales", declaró. Agregó que el gobierno de Obama "haría lo que fuera para prevenir que filtre más información" y confirmó que hacía varios años que Estados Unidos espía tanto a Hong Kong como a China. Sobre su situación aclaró que su intención es "luchar contra Estados Unidos en un juzgado (…) siempre y cuando se me asegure un juicio justo y libre y pueda comparecer, me parece razonable".

Servicios secretos

Una vez conocida la identidad de Snowden, el equipo periodístico continuó en la planificación y la edición de las publicaciones venideras:

El 17 de junio de 2013 se conoce a través de *The Guardian* que los gobiernos de Estados Unidos e Inglaterra espiaron a diplomáticos extranjeros durante la cumbre del G20 en el año 2009. Pusieron bajo escucha al Ministerio de Relaciones Exteriores de Sudáfrica y planificaron espiar la cumbre de Commonwealth de ese mismo año. La razón fue favorecer a empresas estadounidenses en la concreción de contratos. A los dos días Greenwald publica, también en *The Guardian*, extractos de documentos que muestran la falta de transparencia del organismo encargado de supervisar las órdenes que autorizan la vigilancia (la FISC, Foreing Intelligence Surveillance Court).

Lo que se dio luego fue una seguidilla de revelaciones de programas de los servicios secretos estadounidenses y británicos utilizados para espiar a la población o a líderes políticos en todo el mundo. Desde junio del 2013 hasta abril del año siguiente quedó al descubierto lo que Lefébure llamó la "red tentacular de la NSA" gracias a las revelaciones de Snowden. Gran parte de los documentos develados respectan a programas de vigilancia a través de los cuales las agencias de inteligencia espían e interceptan información, como lo fue el caso del programa ECHELON, sobre el cual ahondamos en la parte final de la historización, o el propio PRISM.

Abundan también las escuchas secretas (e ilegales) en lugares estratégicos, con sus respectivos métodos y planos anexados. En junio de 2013, a través de *Der Spiegel*, los europeos se enteran que además de escuchar a la ciudadanía la NSA también espía a sus dirigentes, interceptando comunicaciones telefónicas y de internet, además de haber colocado micrófonos en embajadas y salas de reuniones. "Nuestros aliados no nos tratan como amigos, sino como a sospechosos", expresaba por aquel entonces la parlamentaria europea Sophia Veld. En julio *Der Spiegel* vuelve a revelar otros documentos de Snowden (con planos incluidos) que demuestran que las embajadas de la Unión Europea en Washington y Nueva York están "sonorizadas". Se conoce la SCS (Special Collection Service), una estructura conjunta entre la CIA y la NSA que permite la recolección de datos y las escuchas externas.

Se conoció que los estadounidenses espiaron también la Agencia Internacional de Energía Atómica (AIEA), la ONU (bajo el programa titulado "Blarney), el Ministerio de Relaciones Exteriores francés (a través de la red informática VPN "Virtual Private Network"). En este último caso los franceses entendieron que los objetivos de las escuchas son su política exterior, los contratos militares y nucleares y las negociaciones comerciales.

Se conoció que George Bush autorizó un programa de vigilancia secreto que facilitó la interceptación de datos y metadatos de correos electrónicos e internet, el cual continuó en la administración Obama. También se hizo de público conocimiento el programa Fairview de la NSA para tener acceso a los datos de internet y teléfonos de ciudadanos extranjeros en Irán, Rusia, Pakistán, China y Brasil. Se supo que también se espió a la presidenta de Brasil Dilma Rousseff y al candidato a presidente de México Enrique Peña Nieto.

Otros informes revelan que la NSA tiene acceso a todos los teléfonos inteligentes que hay en el mercado (Smartphones), incluyendo correos electrónicos, notas, ubicación física y contactos. También se profundizó más con respecto a las empresas del mundo que ofrecen servicios en línea y se supo que la NSA recoge masivamente las listas de contactos.

El alertador expuso a la humanidad los mecanismos utilizados a través de la red para establecer un control unificado y mundial por parte de los servicios secretos de las mayores potencias mundiales. Expuso los programas PRISM, XKeyscore, TEMPORA, Stellar Wind; los virus Stuxnet y Flame; y una increíble red de seguridad, vigilancia, espionaje e intercepción de datos que conecta a la NSA, el FBI, la CIA, el Pentágono (todos estadounidenses) con el GCHQ inglés.

En el anexo del trabajo añadimos la información más relevante que expuso Snowden junto a su equipo de comunicadores, organizada cronológicamente por RT (Russian Television).

¿Dónde está Snowden?

"Si Hong Kong no actúa pronto, eso complicará las relaciones bilaterales y despertará interrogantes sobre el compromiso de Hong Kong respecto del Estado de derecho", fueron las palabras de uno de los responsables de la administración de Obama, en ese entonces a cargo del gobierno de Estados Unidos. Es decir, las amenazas a Snowden y su equipo periodístico no tardaron en llegar. El país norteamericano pedía la extradición del alertador y que allí sea juzgado, sin embargo, el territorio chino no tiene esas intenciones, menos después de las revelaciones que afirman que la NSA piratea sus computadoras: "El caso Snowden pasa de un caso de filtración a ser un caso de alta política entre las principales potencias del mundo" declara el analista Bruce Riedel, ex agente de la CIA e investigador de Brookings Institutions (Lefébure, 2014, pág 69).

Por este motivo no fue nada fácil para Snowden conseguir asilo político. Desde Washington, Estados Unidos sometió a presiones políticas y económicas a varios países para que no permitan el aterrizaje del avión del alertador. Incluso contactó al gobierno cubano para que no permita el descenso de la nave ni siquiera para su abastecimiento de combustible. La NSA solicitó al Departamento de Defensa de EEUU una investigación criminal en su contra por robo de documentos y espionaje.

El hecho de que Hong Kong posea un sistema judicial autónomo, más allá de pertenecer a China, dio tiempo al informático. Como explica Antoine Lefébure, en el año 1998 la administración de la ciudad firmó un tratado de extradición con Estados Unidos el cual establece una excepción para los delitos políticos. El caso de Snowden pertenecía a esa excepción.

Julian Assange fue quien se encargó de auxiliar al informático cuando envió a Sarah Harrison, quien desde 2011 formó parte de *Wikileaks* y supo ayudar a Assange en sus defensas legales tras sus revelaciones. Fue con ella que Snowden voló a Moscú el 23 de junio de 2013. Al día siguiente partirían hacia La Habana, sin embargo, por presiones de Estados Unidos, Cuba debió cambiar de postura y el alertador quedó sin documentación para poder residir allí (ni en ningún otra parte). Quedaron varados en el aeropuerto de Moscú por cinco semanas, y a pesar de ser muy buscados por la prensa no fueron hallados.

Al quedar varados en zona de tránsito, Sarah Harrison se encargó de enviar pedidos de asilo para Snowden a 21 países (primero a Ecuador e Islandia, luego a Bolivia, India, Austria, Brasil, China, Cuba, Finlandia, Francia, Alemania, Irlanda, Italia, Países Bajos, Nicaragua, Venezuela, Noruega, Polonia, Rusia, España y Suiza; información proporcionada por *Wikileaks*). Sin embargo, las respuestas no eran positivas, los países se negaban a aceptar el pedido de asilo argumentando, por ejemplo, que no era "jurídicamente admisible" o que "no respeta las condiciones oficiales de un pedido de asilo". Para ese entonces *Wikileaks* ya había denunciado las presiones estadounidenses.

Luego de un mes en el aeropuerto de Moscú, Snowden recibió la autorización de asilo por un año en Rusia, hasta el 31 de julio de 2014. Fue tal la molestia de las autoridades del país norteamericano que Obama canceló la visita a Moscú que tendría por aquellos días. La condición que el informático debía cumplir desde su asilo es no difundir más documentos sobre los servicios de inteligencia estadounidenses. Una vez cumplido el año Rusia otorgó tres años más de asilo al alertador, y en

2017 una vez cumplido este plazo se prolongó hasta 2020. Sin embargo, el equipo formado por Poitras y Greenwald continuó haciendo públicos muchos de los documentos que les reveló Snowden.

Otros nuevos casos

Katharine Gun

El caso de esta joven inglesa ocurre en 2003. Es uno, sino el primero de los que podemos llamar "alertadores" de este milenio. Trabajaba para la agencia nacional de seguridad británica (GCHQ) traduciendo al inglés un montón de conversaciones chinas interceptadas por este organismo gubernamental. Tras recibir un correo calificado como "Top Secret" por parte de la NSA, les es anunciado a ella y varios compañeros que se acababa de lanzar una operación de espionaje de las oficinas y comunicaciones de seis representantes de la ONU.

La razón de tal maniobra tenía que ver con la presentación de Estados Unidos a la Organización de las Naciones Unidas, de una resolución que les permita a ellos y a Gran Bretaña una invasión a Irak. Sin embargo, seis delegados (de Pakistán, Camerún, Chile, México, Guinea y Angola) estaban en una posición dudosa en cuanto a avalar esta intervención armada. Por esto, qué mejor manera de convencerlos que espiarlos y reunir la información necesaria para presionarlos si es necesario.

Gun decide revelar la información, abogando que podría generar que no se lleven adelante tales intervenciones. En marzo de 2003 The Observer (de Gran Bretaña) publica el memorándum "Top Secret". La joven es apresada y luego liberada, quedando su causa en suspenso por unos meses. Aunque la información fue de público conocimiento, los ataques contra Irak fueron igualmente realizados y el ejército británico formó parte de ellos. Finalmente, las acciones legales contra la joven fueron levantadas, tras recibir el apoyo de quienes se oponían a la guerra e incluso de personalidades destacadas.

Sin embargo, Katharine Gun está sujeta a la Ley de Secretos Oficiales del Reino Unido, la cual rige sobre todo ciudadano de esa nacionalidad que haya sido miembro de las fuerzas de seguridad y de inteligencia británicas. Por lo tanto, no tiene permitido realizar declaraciones ni entrevistas sobre lo que atañe a la seguridad nacional. El año pasado se estrenó la película llamada "Secretos de

Estado", basada en los hechos de su vida que acabamos de relatar. Hoy Gun tiene 46 años.

Manning

Como explicamos anteriormente, uno de las filtraciones que tomó mayor relevancia a nivel mundial fue el video del llamado "Asesinato colateral", publicado por *Wikileaks* en 2010. Bradley Manning, un soldado que había estado en Irak y trabajaba para el gobierno de Estados Unidos como analista de inteligencia, tenía acceso a una gran cantidad de información catalogada como confidencial. Según el propio gobierno presidido en ese entonces por Barack Obama, Manning filtró al sitio *Wikileaks* unos 700.000 documentos clasificados, entre ellos, secretos de las guerras de Irak y Afganistan.

Pero, ¿no es que *Wikileaks* no permite que se sepa desde dónde provienen las filtraciones? Bueno sí. Sin embargo, el error de Manning fue haberle contado a Adrian Lamo, un hacker estadounidense, a través de conversaciones que mantuvieron por internet, que poseía esos importantes documentos en su poder. Entonces Lamo acudió a las autoridades adjudicando a Manning el robo de datos, a quien le fueron presentadas 22 acusaciones y una condena de 35 años de prisión en 2013.

Al igual que Julian Assange, Manning estuvo detenido en condiciones inhumanas. Se han realizado movilizaciones y petitorios para exigir su trato digno, ya que estaba bajo el régimen de "prevención de riesgos por lesiones" y es considerado un detenido de máxima seguridad. Tras los tratos denigrantes e inhumanos en prisión, y como resultado de las movilizaciones, el ex soldado fue trasladado a un centro de detención preventiva. En 2020 quedó en libertad. Tiene hoy 32 años.

Thomas Drake

Thomas Drake trabajó para el gobierno de Estados Unidos desde 1979, pasando por la Fuerza Aérea, la CIA y también siendo un alto funcionario de la NSA. A este puesto llega tras el atentado a las Torres Gemelas en 2001, cuando la agencia comenzó a optimizar las herramientas informáticas para administrar y manejar la masa de datos que circulaban en internet. Su labor pasó a ser perito de dos programas utilizados por la NSA para el análisis del flujo de datos, el Trailblazer y el Thin Thread.

Según el punto de vista de Drake y de otros especialistas, el primer programa (Trailblazer) no respetaba la privacidad de los ciudadanos y era más costoso, por lo que consideraban que la NSA terminaría por elegir el segundo para realizar sus operaciones. Sin embargo no. Ante los ojos de Drake la agencia se inclina por la utilización del Trailblazer, considerado como un software de vigilancia generalizada de las telecomunicaciones. En 2005 el agente decide exponer esta decisión de la agencia estadounidense, contando datos sobre corrupción y fraude, que se publica en un artículo en The Baltimore Sun, sin exponer su identidad.

Dos años más tarde la agencia lo identificó como detractor y su casa fue allanada y registrada por oficiales armados en busca de información sensible. Sus computadoras fueron secuestradas por orden del gobierno. Creyendo estar protegido por la Whistleblower Protection Act (aprobada por EEUU en 1998)[4] el denunciante recibió un acoso constante hasta su juicio en 2011. Finalmente fue condenado a un año de libertad condicional y 240 horas de "trabajos comunitarios". Tiene hoy 63 años.

La enseñanza

A diferencia del debate teórico, lo que realza la importancia del riesgo real de personas reales es que es la única forma de vincular una problemática discutible, sobre la que los liberales y demócratas insisten en ignorar, desde un enfoque más pragmático e ineludible. De ahí que el rol de los comunicadores que deciden hacer circular la información caliente, es decir los alertadores, se vuelve sumamente importante. ¿de qué otra manera se explica entonces que, en plena era de las libertades individuales, sean perseguidos solo por poseer información?

El impacto de los casos que expusimos en este capítulo ha generado movimientos en el tablero de la política a nivel mundial. Sin embargo, no han tenido el impulso suficiente para perpetuarse en transformaciones duraderas que permitan la democratización o la modificación en el uso de la tecnología de la información en términos evolutivos y de equidad. Por el contrario, ayudó a perfeccionar los mecanismos de seguridad y control. Cada vez que se halló una falla en el sistema o cada vez que aconteció una filtración, posibilitó entrever las falencias existentes, se ajustaron los

[4] Esta Ley de Protección a los Alertadores entró en vigor en Gran Bretaña en 1998, y fue promovida por la sociedad civil.

mecanismos de seguridad y también de vigilancia, estrechando también el margen de la libertad en el uso de la red.

El devenir de la disputa por los usos de la red encuentra su correlato con la suerte que corren los protagonistas. Así, vemos cómo estos son criminalizados y aislados, asentando un precedente para posibles futuros informantes.

8- Algunas conclusiones

> "El incremento de la libertad individual puede coincidir con el incremento de la impotencia colectiva, en tanto los puentes entre la vida pública y la vida privada están desmantelados o ni siquiera fueron construidos alguna vez; o, para expresarlo de otro modo, en tanto no existe una forma fácil ni obvia de traducir las preocupaciones privadas en temas públicos e, inversamente, de discernir en las preocupaciones privadas temas de preocupación pública"
>
> Zygmunt Bauman

Tener a nuestra disposición una enciclopedia universal, todas las discografías del mundo, no nos hace automáticamente ni sabios, ni expertos. Hasta inclusive puede que sean contraproducentes. La sobreinformación puede ser peor que la desinformación.

La circulación de ideas sigue aparentando tener una condición potencialmente libre. La disponibilidad de la información en un nivel casi planetario es aún una realidad. Nunca fue más rápido y fácil hacer llegar el conocimiento a algún lado. Dar la debida importancia a la soberanía de la red es crucial. Las batallas libradas por hacktivistas, alertadores y organizaciones que defienden el uso libre de la red es desde este punto de vista, una de las batallas más necesarias de la actualidad.

La diagnosis de nuestro momento histórico es precisa para dar un paso más, hacia un compendio de proposiciones que contemplen la toma de posturas definidas. La posverdad, en ese sentido, es un ejemplo de cómo actúa un discurso vacío en una red. El arco situacional que presentamos en este trabajo da cuenta de un presente donde el discurso pierde relevancia ante la predominancia de la imagen, la inmediatez y lo efímero. Esta trilogía nos modifica la valoración de nuestro trabajo y de nuestro rol como sujetos críticos y actores de transformación social, que no por encontrarnos con esa situación dejamos de confiar en nuestra capacidad de aportar a un proyecto humano que, contemplando los errores, haga uso de ellos para evolucionar conscientemente.

Hoy vivimos la era de la destrucción de las tradiciones. Con ella, se destuyen también los modos de vida, los oficios, las certezas. Nos acostumbramos cada vez con más naturalidad a convivir con un

entorno cambiante, vertiginoso e incierto. La hipercomunicación nos apadrina en esa vorágine. La autoridad ha sido puesta en duda y sometida a una atomización peligrosa. Todos son potenciales comunicadores. ¿Qué voz predomina? ¿A quién escuchar?

Hemos sido testigos en nuestro paso por la facultad de la caducidad de muchos formatos de comunicación. El primero de ellos el diario en papel. Pero ¿alguien sigue leyendo en la misma calidad, aun desde una pantalla? ¿Se sigue investigando con la misma rigurosidad en la era de la posverdad?

Es evidente que el consumo masivo de información no se orienta precisamente hacia lo que producen los especialistas en comunicación. Más allá de eso, y por suerte, existe una serie de ámbitos donde todavía es valorado (y necesario) un flujo de informaciones chequeadas y debidamente procesadas, como vimos en el caso de las megafiltraciones.

Mientras sean unos pocos los que se exponen a riesgos por filtrar información, y muchos los que observemos desde la platea qué ocurre con ellos, y sentirnos impotentes ante lo que nos revela esa información (además de engrosar nuestra sobrecargada conciencia), nos quedará esa sensación de que esas voluntades individuales por hacer sacar a la luz información públicamente valiosa se han desperdiciado.

Como ocurrió con Panamá Papers: se convirtieron en posverdad, desde el momento en que supimos que con esa información no podíamos hacer nada (además de corroborar algo que ya sabíamos).

La informatización de la sociedad es una condición singular en el devenir humano con un potencial caótico e incalculable. ¿Son las mismas plataformas que cautivan nuestro tiempo con contenidos absurdos los canales de nuestra liberación futura? ¿Se puede convertir la red en un instrumento de la superación humana?

Ni si quiera es necesario saber la respuesta. Más vale mejor imaginarlo de la mejor forma que podamos.

9- Bibliografía

- Alandete, David (2019). *Fake news, la nueva arma de destrucción masiva*. Barcelona, Deusto.
- Alonso, Patricia (2017). '*Fake news' y posverdad en tiempos de populismos: lecciones para periodistas*. Festival Internacional de Periodismo de Perugia.
- Alvarez Rufs, Manuel (2018). *Estado del arte sobre posverdad y fake news*. UNED.
- Assange, Julian (2013). *Cryptopunks*. Buenos Aires, Marea.
- Assange, Julian (2014). *Cuando Google encontró a Wikileaks*. Buenos Aires. Capital Intelectual.
- Bauman, Zygmunt (2001). *En busca de la política*. Buenos Aire. Fondo de cultura Económica.
- Berardi, Franco (2018). *Fenomenología del fin*. Buenos Aires. Caja Negra.
- Berardi, Franco (2019). *Futurabilidad*. Buenos Aires. Caja Negra.
- Canal Historia (2014). 2010: Wikileaks, la mayor filtración de la historia. Recuperado de: https://canalhistoria.es/blog/2010-wikileaks-la-mayor-filtracion-de-la-historia/
- Charaudeau, Patrick (2004). "La problemática de los géneros: De la situación a la construcción textual". En Revista Signos, 37(56), 23-39.
- Corletti Estrada, Alejandro (2016). *Seguridad en redes*. Madrid. Darfe.
- Corletti Estrada, Alejandro (2017). *Ciberseguridad*. Madrid. Darfe.
- Domscheit-Berg, Daniel (2011). *Dentro de Wikileaks*. Barcelona. Roca Editorial
- El Espectador (2010). Chávez dice que el "imperio quedó al desnudo" tras revelaciones de Wikileaks, diario El Espectador, Colombia, recuperado de: https://www.elespectador.com/noticias/el-mundo/chavez-dice-que-el-imperio-quedo-al-desnudo-tras-revelaciones-de-wikileaks/
- Estepa, R (2004). *Evolución histórica de las telecomunicaciones.*
- Estulin, Daniel (2011). *Desmontando Wikileaks*. Barcelona. Planeta.
- Fernández Savater, Amador (2015). "Entrevista a Miguel Benasayag". En Lobo Suelto. Argentina. Recuperado de: http://anarquiacoronada.blogspot.com/2015/04/entrevista-miguel-benasayag.html
- Han, Byung-Chul (2014). *En el enjambre*. Barcelona. Herder.

- Han, Byung-Chul (2014). *Psicopolítica*. Barcelona. Herder.
- Herrera Hermosilla, Carlos (2015). *Breve historia del espionaje*. Ediciones Nowtilus.
- Infobae (2019). La Fiscalía sueca cerró la investigación contra Julian Assange por violación, Diario Infobae, Argentina, recuperado de: https://www.infobae.com/america/mundo/2019/11/19/la-fiscalia-sueca-cerro-la-investigacion-contra-julian-assange-por-violacion/
- La vanguardia (2017). El telegrama Zimmermann. Diario La Vanguardia. España. Recuperado de: https://www.lavanguardia.com/hemeroteca/20170116/413329878424/primera-guerra-mundial-alemania-estados-unidos-telegrama-zimmermann.html
- Lefébure, Antonie (2014). *El caso Snowden*. Buenos Aires. Capital Intelectual.
- Mazzone, Daniel (2018). *Máquinas de mentir*. Buenos Aires. Crujía.
- Monasterio Astobiza, Aníbal (2017). *Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos*. Revista Dilemata.
- Monleón-Getino, Antonio (2015). *El impacto del Big-data en la sociedad de la información. Significado y utilidad*. Universidad de Barcelona.
- Navarro Pujol, Lazaro, (2012). Breve historia del surgimiento de la radio. Del libro Periodismo y realización radiofónicos. Recuperado de: https://camaguebaxcuba.wordpress.com/2012/06/20/breve-historia-del-surgimiento-de-la-radio-del-libro-periodismo-y-realizacion-radiofonicos/
- Obermaier, Frederik; Obermayer, Bastian (2016). *Panamá papers*. Buenos Aires. Planeta.
- O´donell, Santiago (2011). *ArgenLeaks*. Buenos Aires. Sudamericana.
- Pabón Cadavid, Jhonny Antonio (2010). La criptografía y la protección a la información digital. Revista de la Universidad Externado de Colombia.
- Palazzolo, Fernando y Vidarte Aseroy, Verónica (2012). “Claves para abordar el diseño metodológico”. En Giordano, C., Migliorati, M. y Souza, M. S. (eds.) (2012). Hacia la tesis. Itinerarios conceptuales y metodológicos para la investigación en comunicación (pp. 83-92). La Plata: Universidad Nacional de La Plata.
- Ramonet, Ignacio (2016). *El imperio de la vigilancia*. Buenos Aires. Capital Intelectual.
- Revista Lavaca (2014). “Entrevista a Miguel Benasayag”. Recuperado de: https://www.lavaca.org/notas/miguel-benasayag-homo-sapiens-2-0/

- Sánchez Onofre, Julio César, s/f. Los Papeles del Pentágono: 45 años de lucha para los whistleblowers y la libertad de expresión. UNAM.
- Sin autor, (s/f). Breve historia de la radiofonía. Universidad de Murcia. Recuperado de: https://www.um.es/documents/3239701/10855030/9radio-universidad.pdf/ca7f1437-8ff5-4ffe-9f17-76532d7df133
- Shahin, Saif (2012). *A critical axiology for big data studies*. Bowling Green State, EEUU.
- Schulze Schneider, I. (2013). Los medios de comunicación en la Gran Guerra: "Todo por la Patria"; Historia Y Comunicación Social, 18, 15-30.
- Suazo, Natalia (2015). *Guerras de internet*. Buenos Aires. Debate.
- The Guardian (2013). El programa Prism de la NSA aprovecha los datos de usuarios de Apple, Google y otros, diario The Guardian. Inglaterra. Recuperado de: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
- Valdivia Miranda, Carlos (2010). El cable transoceánico. ACTA (Autores científico-técnicos y académicos). Recuperado de: https://www.acta.es/medios/articulos/comunicacion_e_informacion/056113.pdf
- Vilker, Shila (comp) (2012). *Papeles secretos*. Buenos Aires. Eudeba.
- Zizek, Slavoj (2014). *Pedir lo imposible*. Madrid. Akal.
- Zizek, Slavoj (2016). *Problemas en el paraíso*. Barcelona. Anagrama.

10- Anexos

Nombre	Sede	Nº as (asN)
Cogent anteriormente PSINet	Estados Unidos	174
Level 3 Communications (Ex Level 3 y Global Crossing)	Estados Unidos	3356 / 3549 / 1
XO Communications	Estados Unidos	2828
AT&T	Estados Unidos	7018
Verizon Business (anteriormente UUnet)	Estados Unidos	701 / 702 / 703
CenturyLink (anteriormente Qwest and Savvis)	Estados Unidos	209 / 3561
Sprint	Estados unidos	1239
Zayo Group anteriormente AboveNet	Estados Unidos	6461
GTT (anteriormente Tinet)	Estados Unidos	3257
NTT Communications (anteriormente Verio)	Japón	2914
Teliasonera International Carrier	Suecia - Finlandia	1299
Tata Communications (adquirió Teleglobe)	India	6453
Deutsche Telekom (Hoy: International Carrier Sales & Solutions)	Alemania	3320
Seabone (Telecom Italia Sparkle)	Italia	6762
Telefónica	España	12956

Listado de TIERS: proveedores primarios de conexiones de internet. Fuente: Corletti Estrada (2017).

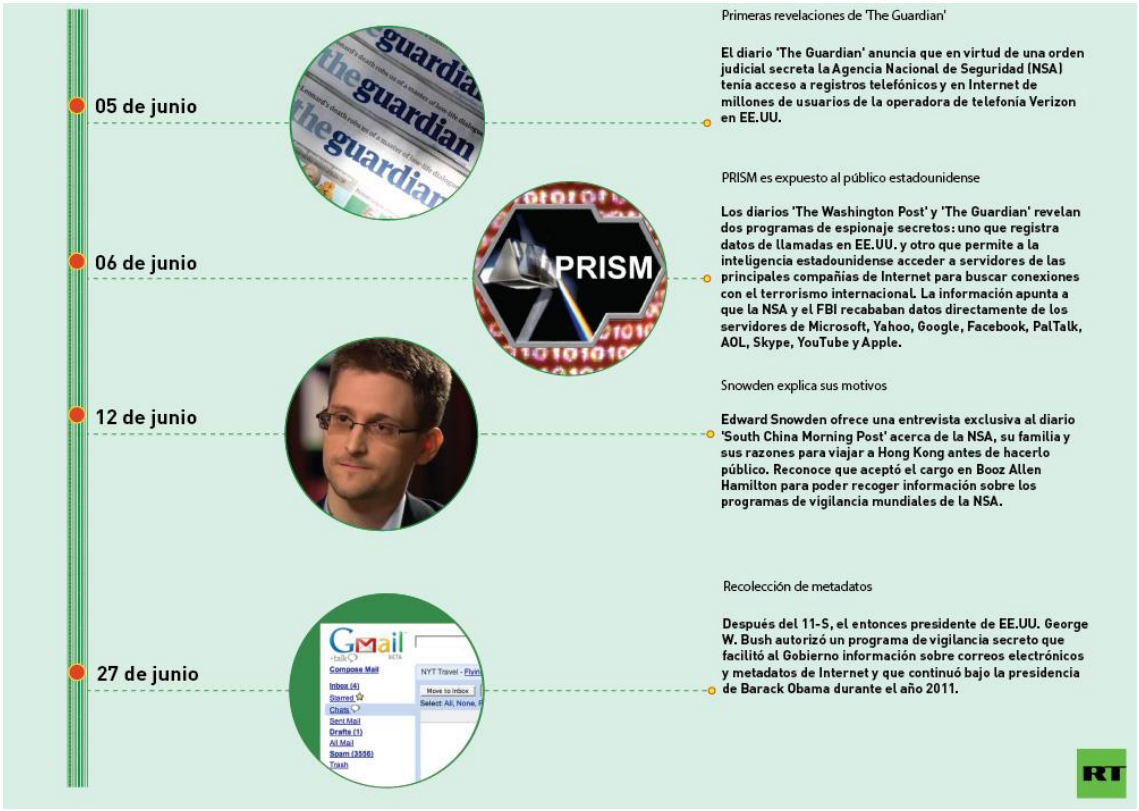
Enlaces

Dario Sztajnszrajber sobre la posverdad

https://www.youtube.com/watch?v=Mt8XeIQq1iU&ab_channel=FacultadLibre

https://www.youtube.com/watch?v=iEkhXwWq_ps&ab_channel=MediaMorfosis

Listado de las filtraciones propiciadas por Snowden. La cronología corresponde a 2013 – Fuente: Lefébure (2014)



07 de septiembre

La NSA puede espiar los datos de los 'smartphones'

'Der Spiegel' revela que la NSA tiene la capacidad de aprovechar los datos -incluyendo correos electrónicos, contactos, notas y ubicación física- desde todos los principales teléfonos inteligentes del mercado.

16 de septiembre

Redes financieras supervisadas por la NSA

'Der Spiegel' revela que una rama especial de la NSA llamada 'Follow the Money' realiza la recolección masiva de datos en las redes internacionales pertenecientes a Visa, Mastercard, la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT) y otras instituciones financieras. La vigilancia de la NSA de la SWIFT, en particular , viola un acuerdo de 2010 con la Unión Europea.

14 de octubre

La NSA recoge masivamente las listas de contactos en línea

El 'Washington Post' revela que la NSA recoge más de 250 millones de listas de contactos de correos electrónicos y cuentas de mensajería instantánea personales de todo el mundo de servicios en línea como Yahoo, Gmail y Facebook.

RT

20 de octubre

La NSA espía al presidente de México

'Der Spiegel' revela que la NSA se ha infiltrado en la cuenta de correo electrónico del expresidente de México Felipe Calderón junto con las cuentas de sus ministros y otros miembros del Gobierno mexicano. El espionaje cubría temas de seguridad, lucha contra las drogas y políticas comerciales.

23 de octubre

EE.UU. espía a la canciller alemana

La canciller alemana, Angela Merkel, llamó al presidente Barack Obama para pedirle explicaciones luego de enterarse de que la inteligencia de EE.UU. pudo haber espiado su teléfono móvil. Dijo que sería "una grave violación de la confianza" en caso de confirmarse.

24 de octubre

La NSA escuchó las llamadas de 35 líderes mundiales

Nuevos documentos publicados por 'The Guardian' muestran que la NSA supervisó las llamadas telefónicas de 35 líderes del mundo en 2006 después de que un oficial de otra rama del Gobierno de EE.UU. entregara sus números a la agencia.

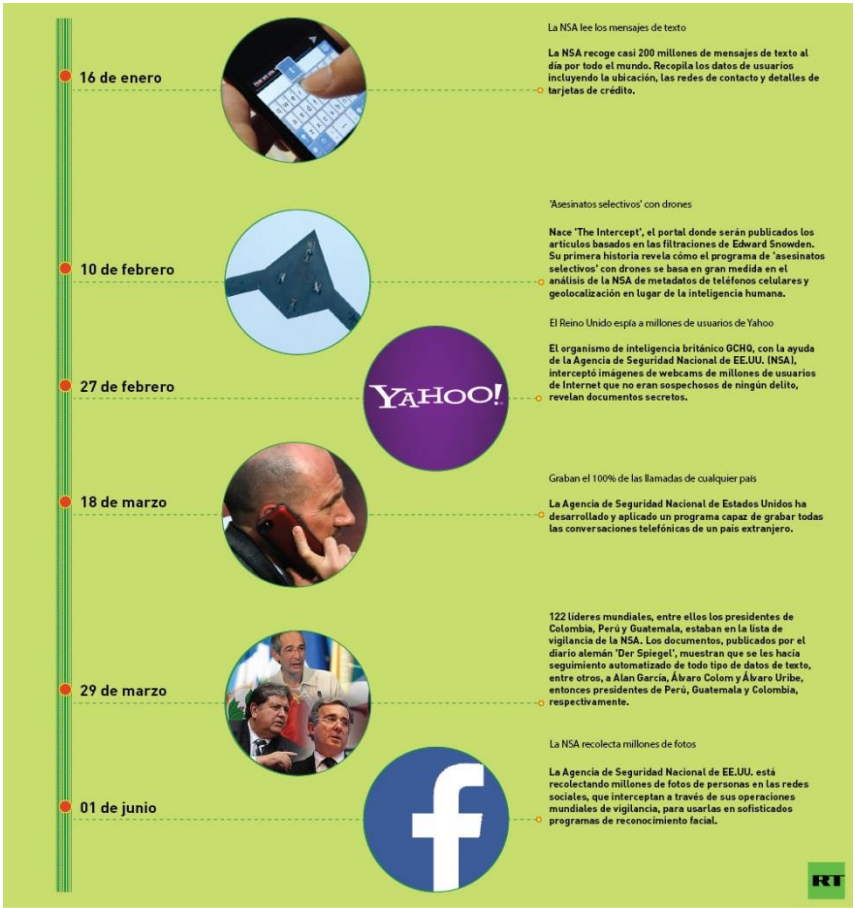
25 de octubre

La NSA espió masivamente a líderes y ciudadanos españoles

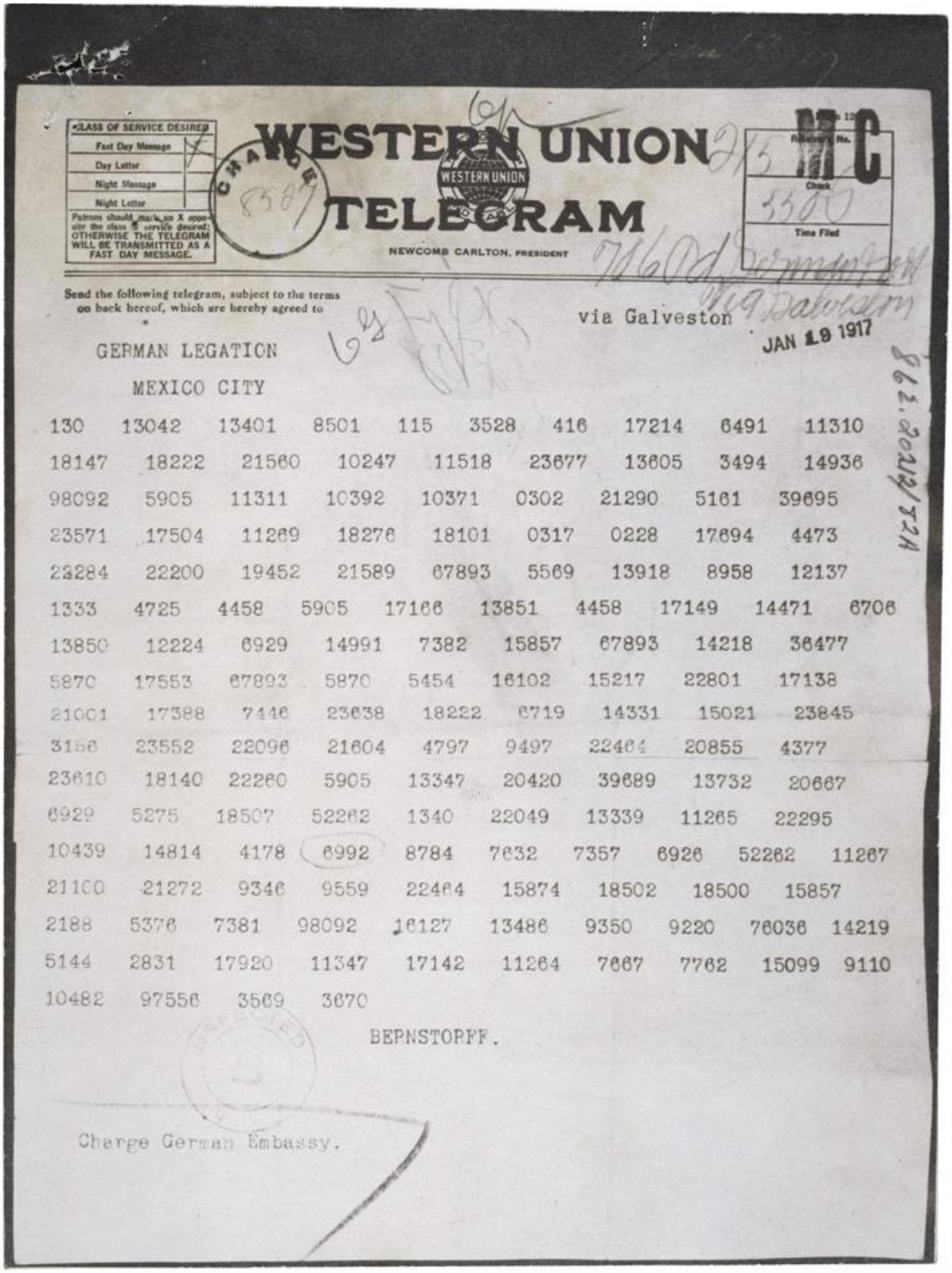
Los diarios españoles 'El País' y 'El Mundo' revelan la vigilancia en masa de la NSA a los líderes y ciudadanos españoles. Un documento publicado por 'El Mundo' explica que la agencia recogió 60 millones de llamadas telefónicas españolas en solo 30 días a finales de 2012 y principios de 2013. Dicha vigilancia masiva es ilegal según el derecho español.

RT


30 de octubre
La NSA infiltra los datos de Google y Yahoo
'The Washington Post' revela que la Agencia de Seguridad Nacional accedió de manera secreta a los centros de datos de Yahoo y Google en todo el mundo para recoger información sobre sus usuarios.
22 de noviembre
El poder de vigilancia: 'Cualquier persona, en cualquier momento y en cualquier lugar'
Un nuevo artículo del 'New York Times' expone el deseo de la NSA de poseer mayor poder legal y dominio tecnológico. De acuerdo con un documento interno de la agencia a partir de 2012, la NSA quería ampliar su ya amplia autoridad legal. También planea "influir en el mercado global de encriptación comercial" a través de alianzas con empresas de alta tecnología y sus propios espías dentro de las empresas privadas de alta tecnología. Su objetivo final, según el documento, es acceder a los datos de "cualquier persona, en cualquier momento y en cualquier lugar".
23 de noviembre
La NSA infecta 50.000 redes
La NSA infectó más de 50.000 redes de computadoras en todo el mundo con un software maligno diseñado para robar información confidencial. Entre los países blanco de este ataque están Venezuela, Bolivia, Brasil, Ecuador, Cuba, Colombia y Honduras, entre otros.
28 de noviembre
EE.UU. espía el G-20 de Toronto en 2010
La Canadian Broadcasting Corporation revela una masiva operación de vigilancia de la NSA dirigida a diplomáticos extranjeros durante las cumbres del G-8 y G-20 de 2010 en Toronto. Sus objetivos eran dar a EE.UU. una ventaja en las negociaciones económicas y políticas.
14 de enero 2014
La NSA 'hackea' ordenadores que no están conectados a la Red
El 'Washington Post' revela cómo la NSA logra acceder a los sistemas informáticos de todo el mundo mediante la implantación de malware y hardware personalizado, incluyendo hardware que permite a la agencia de forma remota acceder a las computadoras que no están conectadas a una red exterior.
RT


16 de enero
La NSA lee los mensajes de texto
La NSA recoge casi 200 millones de mensajes de texto al día por todo el mundo. Recopila los datos de usuarios incluyendo la ubicación, las redes de contacto y detalles de tarjetas de crédito.
10 de febrero
'Asesinatos selectivos' con drones
Nace 'The Intercept', el portal donde serán publicados los artículos basados en las filtraciones de Edward Snowden. Su primera historia revela cómo el programa de 'asesinatos selectivos' con drones se basa en gran medida en el análisis de la NSA de metadatos de teléfonos celulares y geolocalización en lugar de la inteligencia humana.
27 de febrero
El Reino Unido espía a millones de usuarios de Yahoo
El organismo de inteligencia británico GCHQ, con la ayuda de la Agencia de Seguridad Nacional de EE.UU. (NSA), interceptó imágenes de webcams de millones de usuarios de Internet que no eran sospechosos de ningún delito, revelan documentos secretos.
18 de marzo
Graban el 100% de las llamadas de cualquier país
La Agencia de Seguridad Nacional de Estados Unidos ha desarrollado y aplicado un programa capaz de grabar todas las conversaciones telefónicas de un país extranjero.
29 de marzo
122 líderes mundiales, entre ellos los presidentes de Colombia, Perú y Guatemala, estaban en la lista de vigilancia de la NSA. Los documentos, publicados por el diario alemán 'Der Spiegel', muestran que se les hacía seguimiento automatizado de todo tipo de datos de texto, entre otros, a Alan García, Álvaro Colom y Álvaro Uribe, entonces presidentes de Perú, Guatemala y Colombia, respectivamente.
01 de junio
La NSA recolecta millones de fotos
La Agencia de Seguridad Nacional de EE.UU. está recolectando millones de fotos de personas en las redes sociales, que interceptan a través de sus operaciones mundiales de vigilancia, para usarlas en sofisticados programas de reconocimiento facial.
RT

Telegrama Zimmerman



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8309

WESTERN UNION

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

NL C

Check 3300

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTOPFF.

Charge German Embassy.