Universidad de Buenos Aires

Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

“Vigilancia masiva y manipulación de la opinión pública”

Autor: Ing. Juan Ignacio Schab

Tutor: Dr. Pedro Hecht

Año de presentación: 2020

Cohorte 2018

Declaración Jurada del origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Ing. Juan Ignacio Schab
DNI 37.338.256

Resumen

Dos escándalos de gran repercusión internacional han contribuido para probar la real dimensión de los dos temas que dan título al presente trabajo. El primero de ellos fue la revelación de miles de documentos clasificados de agencias de inteligencia, principalmente estadounidenses, realizada por Edward Snowden, ex contratista de la CIA y la NSA, en el año 2013, la cual dio detalles de la extendida y profunda vigilancia masiva a escala global, la cual destruye el derecho a la privacidad y limita las libertades individuales. El otro hecho fue la participación de la empresa Cambridge Analytica en procesos electorales de distintos países del mundo, especialmente en las elecciones presidenciales de Estados Unidos en 2016 y en el referéndum para la salida de Gran Bretaña de la Unión Europea en el mismo año, revelada por ex trabajadores de la misma y por investigaciones de medios de comunicación, el cual permitió dar detalles sobre la capacidad de manipulación de la opinión pública principalmente a través de redes sociales.
La vigilancia masiva está muy ligada a la manipulación de la opinión pública. En este sentido, los ciudadanos desprevenidos y no concientizados que compartan en una red pública como Internet datos sobre sus actividades, gustos, ideologías, preferencias, etc. estarán siendo víctimas de una vigilancia masiva por parte de agencias de inteligencia, nacionales o extranjeras, y de empresas que, vía servicios tecnológicos, también recopilan datos personales. Esta recopilación masiva de datos permite, además de configurar un historial que luego se transforme en antecedentes personales, la creación automática de perfiles de personalidad a partir de los cuales sea posible dirigir de forma simple, eficaz y automatizada una campaña direccionada compuesta de noticias falsas, propaganda y mensajes sutilmente diseñados para modificar comportamientos.
Este escenario, combinado con la falta de leyes y controles rigurosos por parte de los Estados, con la limitada lucha contra las noticias y cuentas falsas en redes sociales, con la escasez de conciencia ciudadana colectiva, con la ausencia de neutralidad de la red y con la concentración de los medios de comunicación en pocas manos, resulta propicio para llevar a cabo un control social del cual resulte muy difícil escapar.
La metodología del presente trabajo consistió en recopilar y analizar obras de diferentes autores y artículos de sitios web y organizaciones, con los objetivos de describir y dar detalles de la vigilancia masiva y de la manipulación de la opinión pública y de encontrar los puntos en que ambas se vinculan.

Palabras clave: vigilancia masiva, manipulación, datos personales, noticias falsas, propaganda, neutralidad de la red, control social.

Tabla de contenidos

Declaración Jurada del origen de los contenidos 2
Resumen 3
Tabla de contenidos 4
Introducción 7
Desarrollo 9
1- Historia de la SIGINT 9
2- Programas de vigilancia masiva de Estados 14
2.1- El Informe Moraes y la excusa de la seguridad nacional 14
2.2- Revelaciones de Snowden y métodos de vigilancia 15
2.3- Análisis de los datos recolectados 38
3- Historia de Internet y neutralidad de la red 43
3.1- Conceptos y principios sobre Internet 43
3.2- Origen de Internet 46
3.3- Revolución sobre Internet 49
3.4- Fin de la neutralidad y control de los Estados 53
4- Ámbito legal de la vigilancia y de la neutralidad de la red 63
4.1- Aspectos legales de la vigilancia masiva 63
4.2- Aspectos legales de la neutralidad de la red 66
5- El negocio de los datos personales 69
5.1- Fuentes de datos personales 69
5.2- Vigilancia de empresas de tecnología 72
5.3- Persecución al sospechoso, ausencia de privacidad y control social 77
5.4- Sistema de crédito social chino 81
5.5- El negocio de la nube 84
5.6- El negocio de las empresas de tecnología y los data brokers 85
5.7- Adicción a las redes sociales y Capitalismo de la Vigilancia 88
6- Manipulación de la opinión pública 91
6.1- Debilidades humanas y filtro burbuja 91
6.2- Manipulación psicológica 93
6.3- Dominio cultural 97
6.4- Guerra de la comunicación 99
6.5- Fact checking 104

6.6- Manipulación de encuestas y seguidores 104
6.7- Influencias de Grupos y ONGs 105
6.8- Diplomacia y espionaje 106
6.9- Lawfare 107
6.10- Ingeniería social 111
6.11- Máquina de propaganda automatizada 112
6.12- Origen de las fake news, bots y trolls 121
6.13- Otras estrategias para influir en elecciones 124
6.14- Historia de la interferencia en procesos electorales 125
7- Contexto geopolítico 126
7.1- Tipos de países y estrategias 126
7.2- Colonialismo de las democracias 129
7.3- Neocolonialismo 130
7.4- Estrategias en el ciberespacio 131
7.5- Secretismo y filtraciones 132
7.6- Principales agencias de inteligencia del mundo 133
7.7- Avances tecnológicos en la inteligencia de Estados Unidos 134
7.8- Dominio tecnológico y espacial 135
7.9- Satélites espía 136
7.10- Guerra militar 137
7.11- Guerra económica 138
7.12- Guerra híbrida 141
7.13- Operaciones de Inteligencia y Ciberataques 142
7.14- China vs Estados Unidos 147
7.15- Vigilancia en tiempos de pandemia 150
7.16- El abuso de los algoritmos 153
8- Posibles contramedidas 155
8.1- Navegación anónima 155
8.2- Seguridad en servicios de mensajería 157
8.3- Seguridad en correo electrónico 160
8.4- Seguridad en el almacenamiento y transferencia de datos 161
8.5- Redes descentralizadas 162
8.6- Blockchain 164
8.7- Criptografía cuántica 166
8.8- Seguridad en sistemas operativos 167
8.9- Protección de datos personales 168

8.10- Seguridad en big data 169
8.11- Seguridad en IoT.....171
8.12- Derecho al olvido.....173
8.13- Combatir la manipulación y la desinformación.....175
Conclusiones.....180
Anexos.....189
Schrems y la revocación del Safe Harbor 189
Técnica GAN.....189
Causas económicas en las dos guerras mundiales.....190
Citas bibliográficas 191
Índice de imágenes 200

Introducción

La inteligencia de señales (SIGINT) puede definirse como la interceptación y análisis de señales electrónicas, electromagnéticas o señales provenientes de comunicaciones, por ejemplo, a través de radares o teléfonos. A su vez, debido a que buena parte de la información que se propaga a través de estas señales viaja cifrada, la SIGINT también requiere de técnicas de criptoanálisis, que permitan romper el cifrado y obtener la información en crudo. La SIGINT le permite a un país llevar a cabo investigaciones sobre delitos a fin de encontrar evidencias o pistas, o, en un contexto de conflicto internacional, aplicar inteligencia sobre las comunicaciones de un adversario. Con el avance tecnológico, la SIGINT ha ido incorporando el uso de programas de inteligencia que permiten la automatización de los procesos de recolección, almacenamiento y procesamiento de la información, cada vez con mayores capacidades y con un alcance más extendido.

En junio de 2013, Edward Snowden, que trabajaba como contratista de las agencias de inteligencia estadounidenses CIA y NSA, filtró documentación confidencial que demostraba las capacidades y verdaderos objetivos de las agencias de inteligencia, incluyendo espionajes a políticos y empresas y un nivel de vigilancia masiva a escala mundial del que no se tenía demasiada evidencia. Estas revelaciones incluían detalles de los programas de inteligencia que usaban distintas agencias violando por completo el derecho a la privacidad, tanto de los ciudadanos extranjeros como locales.

Las filtraciones también revelaron vínculos de estas agencias de inteligencia con corporaciones tecnológicas y de telecomunicaciones, las cuales colaboran con la vigilancia aportando datos que recopilan de sus clientes. También, este tipo de compañías hacen negocios con estos datos, ya sea vendiéndolos a otras empresas o a anunciantes publicitarios. A su vez, se han conocido diferentes escándalos de distintas empresas tecnológicas por filtraciones de datos personales o por una falta de protección de los mismos. Esto ha generado que existan empresas que, recopilando estos datos de miles de personas, puedan generar perfiles muy precisos de ciudadanos, sobre los cuales luego sea posible dirigir mensajes o publicidad para influir en su comportamiento, por ejemplo, modificando su voto.

En aquellos países donde el pueblo elige a sus gobernantes es fundamental que los ciudadanos estén bien informados acerca de los candidatos, a fin de emitir un voto consciente: después de todo serán sus representantes. Para lograrlo, es esencial conocer las nuevas modalidades de las campañas políticas, incluyendo la publicidad direccionada, las noticias falsas y la actividad de los perfiles falsos en redes sociales.

A raíz de esta problemática planteada, el presente trabajo se enfoca no solo en dar a conocer la forma en que se lleva a cabo la vigilancia masiva y la manipulación de la opinión pública, sino también en dar un contexto integral que permite analizar los objetivos que éstas persiguen.

En el primer capítulo se darán detalles de la inteligencia de señales, incluyendo la creación de las primeras agencias de inteligencia, la primera colaboración entre ellas, las primeras alianzas y algunas operaciones que han llevado a cabo.

El segundo capítulo hace énfasis en los programas de vigilancia masiva de agencias de inteligencia de Estados revelados por Snowden y brinda detalles sobre sus capacidades y funcionamientos.

En el tercer capítulo se realiza un repaso de los inicios de Internet y sobre cómo durante su evolución fue perdiendo neutralidad.

En el cuarto capítulo se abordan diferentes leyes y regulaciones que han impactado en el ámbito de la vigilancia masiva de Estados y en el de la neutralidad de Internet.

El quinto capítulo ofrece una visión de cómo las empresas de tecnología recopilan datos personales para hacer negocios y de cómo la vigilancia masiva impacta sobre los ciudadanos.

En el sexto capítulo se analizan las diferentes maniobras que llevan a cabo Estados y diferentes organizaciones para manipular psicológicamente a los ciudadanos y hacerlos actuar en pos de determinados intereses.

En el séptimo capítulo se brinda un panorama geopolítico que permite dar cuenta de los objetivos que persiguen la vigilancia masiva y la manipulación de la opinión pública.

El capítulo ocho da cierre al desarrollo con un listado de diferentes herramientas, medidas y conceptos que, bien aplicados, colaboran a hacer frente a las diferentes problemáticas tratadas en este trabajo.

Desarrollo

1- Historia de la SIGINT

José Gabriel Paz comenta que la Inteligencia de Señales (SIGINT) se realiza con un alto grado de sigilo, por lo que resulta muy difícil detectarla y atribuirla a algún país, a menos que se disponga de una tecnología muy precisa o se descalsifiquen o filtren documentos. [1]

La cooperación en materia de inteligencia de señales comenzó informalmente entre Estados Unidos y Reino Unido en la Primera Guerra Mundial y formalmente, mediante acuerdos, en la Segunda Guerra Mundial.

En cuanto a Reino Unido, desde finales del siglo XIX disponía de capacidades para interceptar y decodificar telegramas, correos postales y señales Morse, así como también la intervención de redes telefónicas y telégrafo. En 1919 nace el British Government Code and Cypher School (GC&CS), que en 1949 cambiaría su nombre al actual Government Communications Headquarters (GCHQ).

En el caso de Estados Unidos, la primera organización de SIGINT se funda en 1917 y se llama Cipher Bureau (MI-8). En 1952 se incorpora la National Security Agency (NSA) como un nuevo miembro de la comunidad de inteligencia estadounidense

El primer antecedente de cooperación fue durante la Primera Guerra Mundial, cuando en enero de 1917 los servicios de inteligencia británicos interceptaron y descifraron un telegrama encriptado enviado por el ministro de Asuntos Exteriores del Imperio Alemán, Arthur Zimmermann, al embajador alemán en México, Heinrich von Eckardt, el cual proponía al gobierno mexicano una alianza para enfrentarse a Estados Unidos. Reino Unido dio aviso a Estados Unidos de este contenido y este fue uno de los desencadenantes del ingreso de Estados Unidos al combate.

Una vez terminada la guerra, Reino Unido y EEUU comenzaron a considerar monitorear las comunicaciones de sus oponentes y también al movimiento comunista internacional. Fueron instalando estaciones de escucha estratégicamente ubicadas para poder espiar a Japón, la Unión Soviética, Alemania, Oriente Medio y la India, entre otros.

En 1940, durante la Segunda Guerra Mundial, se establecieron pactos para el intercambio periódico de material de SIGINT entre EEUU y Reino Unido (máquinas de desencripción, manuales de señales, documentos encriptados de los oponentes e intercambio de personal y recursos técnicos).

En 1941, Estados Unidos y Reino Unido firman una alianza SIGINT y cooperan entre sí en materia de inteligencia de señales [2]. El objetivo principal era quebrar el método de codificación de la célebre máquina alemana Enigma, siendo esto logrado en 1942 por el equipo de criptógrafos británicos agrupados alrededor de Alan Turing. Luego de este logro, se firma en mayo de 1943 entre ambos países el acuerdo BRUSA, que tiene como objetivo "[…] el intercambio de toda información relativa al descubrimiento, identificación e interceptación de señales, así como el desciframiento de los códigos y claves" [3], sentando las bases de un sistema mundial de vigilancia.

En 1946, se renegocia un nuevo acuerdo, el British-US Communication Intelligence Agreement, que establece "el intercambio de información relacionado con operaciones de comunicaciones extranjeras en materia de colección de tráfico, adquisición de comunicaciones y equipamiento, análisis de tráfico, criptoanálisis, descifrado y traducción, y adquisición de información respecto de organizaciones de comunicación, prácticas, procedimientos y equipamiento". El acuerdo logra su redacción textual final en 1948, al que a los pocos años se incorporan Canadá, Australia y Nueva Zelanda. Esta alianza se conoce como UKUSA, pero también se la llama Alianza de los Cinco Ojos. Actualmente, UKUSA es la estructura de SIGINT más importante del mundo, con numerosos y calificados medios para obtener y analizar comunicaciones. Gabriel Paz menciona cómo se reparten geográficamente la vigilancia:

> *"Estados Unidos centra su tarea en Asia, Rusia asiática, el norte de China, Latinoamérica y el Caribe, donde cuenta con estaciones en Puerto Rico, Brasilia, Bogotá, Caracas, Ciudad de México y Ciudad de Panamá. Gran Bretaña intercepta principalmente las comunicaciones en Europa, Rusia, África, aunque tiene instalaciones en todos los continentes. En América posee dos estaciones de escucha identificadas: Daniels Head en Bermuda y Mount Pleasant en las Islas*

Malvinas. Canadá cubre Centro y Sudamérica, Australia se dedica a las comunicaciones de Indochina, Indonesia y el sur de China, mientras que Nueva Zelanda tiene a su cargo el Pacífico occidental".

La alianza UKUSA también ha establecido convenios de cooperación con otros países, como el nexo entre la NSA y su homólogo de Israel, la Unidad 8200 (Yehida Shmoneh-Matayim), para el intercambio de información, tecnología y software para la inteligencia de señales.

Luego del inicio de la Guerra Fría, desde 1950 y hasta fines del siglo XX la alianza UKUSA realizó operaciones de inteligencia sobre la Unión Soviética, sus aliados y países con grupos pro comunistas (entre ellos, China, Vietnam, Corea del Norte, Cuba y Malasia). Durante la Guerra de Corea (1950-1953) realizó trabajos de intercepción de señales contra las fuerzas norcoreanas.

A fines de la década de 1950, en plena carrera de desarrollo de tecnología aeroespacial entre Estados Unidos y la Unión Soviética, comienzan a lanzarse los primeros satélites norteamericanos para SIGINT. El objetivo de los mismos era la toma de imágenes y la intercepción de comunicaciones (incluyendo señales de radio y de telefonía).

UKUSA también operó durante la Guerra de Vietnam (1955-1975), con operaciones de inteligencia en el sudeste asiático.

En la Guerra de Malvinas (1982) entre Reino Unido y Argentina, los británicos, además de contar con sus propios medios, recibieron importantes contribuciones en materia de SIGINT de Estados Unidos (ya que el Atlántico Sur era su área de competencia). Dentro de la ayuda recibida se destacan los satélites que proveían de imágenes de alta resolución, inclusive durante la noche, revelando la ubicación terrestre, naval y aérea de las fuerzas argentinas. Además, la NSA descifraba el código secreto de los servicios de inteligencia argentinos y lo transmitía al Reino Unido, dándole una importante ventaja. La débil seguridad de las máquinas de cifrado de Datotek, utilizadas por Argentina durante dicha guerra para codificar mensajes, le permitió a la NSA quebrar su sistema de cifrado y así desencriptar los mensajes clasificados de Argentina y proporcionar a la agencia inglesa GCHQ su texto en claro. [4]

Según una investigación del Washington Post y la emisora alemana ZDF [5], además de las Datotek, Argentina, al igual que más de 120 países desde la

Segunda Guerra Mundial hasta 2018, usó durante el conflicto bélico con Reino Unido cifradores de texto de la empresa suiza Crypto AG, que fue secretamente adquirida por la CIA, en asociación con la BND (su par alemana), desde la década de 1970. Estas agencias manipularon las máquinas de cifrado de dicha compañía para poder fácilmente descifrar los mensajes que enviaban a través de éstas los países clientes de la misma. Se trató de una operación, inicialmente llamada “Thesaurus”, y luego “Rubicon”, con la cual Estados Unidos y sus aliados les cobraban dinero a otros países para robarle sus secretos, a través del uso de las máquinas de Crypto AG. La investigación afirma que, entre otros logros, esto les permitió enviar información a Gran Bretaña sobre el ejército argentino durante la guerra de Malvinas y rastrear las dictaduras en América del Sur. También sirvió para descifrar cables diplomáticos y otras trasmisiones confidenciales de gobiernos extranjeros.

En la década de 1970, la NSA crea el programa Echelon, con el objetivo inicial de espiar las comunicaciones de la Unión Soviética y sus aliados, y poco tiempo después fue puesto a disposición de la alianza UKUSA. La existencia de Echelon fue ocultada al público durante muchos años hasta que, luego de diversos rumores acerca de la existencia de un sistema de captura masiva de comunicaciones, el periodista británico Duncan Campbell en 1988 expuso en un documento detalles sobre su funcionamiento.

Con el paso del tiempo y el avance de la tecnología, Echelon se fue actualizando hasta ser capaz de recolectar a nivel mundial toda comunicación telefónica o vía satélite, fibra óptica y cables submarinos y también señales por microondas y radio. Así también, amplió su objetivo inicial incorporando como parte de su tarea el espionaje a gobiernos, partidos políticos, sindicatos, movimientos sociales y empresas (con el fin de proporcionar ventajas comerciales a empresas de los países miembros de UKUSA), que luego de verse afectados por este programa colaboraron para las investigaciones que permitieron revelar su existencia.

Otra denuncia sobre vigilancia masiva fue la encabezada por Willian Binney, un matemático que trabajó para la NSA, en 2002 ante el Inspector General del Departamento de Defensa de EEUU por sospecha de fraude en la compra y abusos sobre la privacidad de la gente del programa Trailblazer.

Este programa reemplazó en 2001 (tres semanas antes de los atentados del 11S) al programa ThinThread, diseñado por Binney, que era efectivo, ya que rastreaba comunicaciones a nivel mundial y alertaba en tiempo real amenazas terroristas, era mucho más barato y tenía en consideración la privacidad de los ciudadanos, por lo que encriptaba las comunicaciones, brindando solo información sobre sospechosos. Según demostraciones del propio Binney, si se hubiera continuado con el programa ThinThread se hubieran detectado pistas para prevenir estos atentados. [6]

En el documental Citizenfour [7], William Binney comenta:

> *"Mi trabajo en la NSA fue desarrollar un programa para automatizar el análisis de grandes volúmenes de datos. No más de una semana después del 11S el gobierno de EEUU decidió comenzar a espiar masivamente a todos los habitantes de EEUU, y lo que hicieron fue utilizar parte de ese programa para llevar a cabo ese espionaje. El programa de espionaje se llamaba Stellar Wind".*

Pero, sin duda, la filtración más reveladora e impactante fue la llevada a cabo por Edward Snowden[1] a la documentalista Laura Poitras y a los periodistas Gleen Greenwald y Ewen MacAskill durante junio de 2013. Con estas revelaciones dejó expuesta la mayor red mundial de SIGINT organizada por la alianza UKUSA, entregando millones de archivos de las agencias de UKUSA a los principales medios de comunicación mundiales (The Guardian, Der Spiegel, The New York Times, El País, The Washington Post, Le Monde, O Globo, entre otros).

En febrero de 2013, Snowden le escribe a Laura Poitras:

> *"Stellar Wind ha crecido y con la acción de la unidad SSO de la NSA ha llegado a cubrir prácticamente todo Estados Unidos y se ha extendido por todo el mundo […] La NSA jamás ha recolectado tantos datos como ahora […] Las grandes empresas de telecomunicaciones de Estados Unidos están traicionando la confianza de sus clientes".* [7]

[1] Snowden, desde su exilio en Rusia desde agosto de 2013 (Estados Unidos le impuso cargos por robo de propiedad gubernamental y difusión de datos clasificados), se dedica a desarrollar herramientas que ayuden a periodistas a proteger sus fuentes.

2- Programas de vigilancia masiva de Estados

2.1- El Informe Moraes y la excusa de la seguridad nacional

Luego de las revelaciones de Snowden, el 4 de julio de 2013 el Parlamento Europeo le encargó a su Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) que realice una investigación exhaustiva de los programas de vigilancia masiva. El 21 de febrero del 2014 el LIBE presentó un informe al respecto, popularmente conocido como Informe Moraes [8] (debido a que su autor y ponente fue el británico Claude Moraes), el cual pone de manifiesto que las prácticas secretas de vigilancia masiva a través de tecnología invasiva y de alcance mundial existen:

> *"[…] las recientes revelaciones en la prensa por parte de denunciantes y periodistas, junto con las pruebas periciales proporcionadas durante esta investigación, el reconocimiento por parte de las autoridades y la insuficiente respuesta a estas acusaciones, han resultado ser una prueba convincente de la existencia de sistemas tecnológicamente muy avanzados, complejos y de amplio alcance diseñados por los servicios de inteligencia de los Estados Unidos y de algunos Estados miembros para recopilar, almacenar y analizar datos de comunicaciones, incluidos datos de contenido y datos y metadatos de localización de todos los ciudadanos en todo el mundo a una escala sin precedentes y de una manera indiscriminada y no basada en sospechas".*

A su vez, el informe destaca la inquietud de la Unión Europea sobre “[...] la posibilidad de que estas operaciones de vigilancia masiva se utilicen por motivos distintos a la seguridad nacional y a la lucha contra el terrorismo en su sentido estricto, como, por ejemplo, para el espionaje económico e industrial o la elaboración de perfiles por razones políticas".

Ewen Macaskill, en una entrevista de la TV Pública Argentina en 2015 [9], hizo las siguientes declaraciones sobre la vigilancia masiva:

> *"La gente piensa que la privacidad no es importante […] No hay país en el mundo al que la NSA y el GCHQ no puedan acceder a sus comunicaciones […] Y pueden obtener el perfil de cualquier persona en solo cinco minutos.*

[…] Estas agencias de inteligencia tienen el modus operandi de recopilar toda la información de las comunicaciones para que, si se encuentra algún sospechoso de terrorismo, secuestro o algún otro delito poder llegar a él y a sus vínculos a partir de estos datos recolectados. Sin embargo, para poner a prueba esa teoría que parece razonable, hemos consultado a directores de agencias de inteligencia de la NSA y el GCHQ acerca de si tenían registro de algún caso satisfactorio y no pudieron dar un solo caso de éxito. […] Hasta ahora nadie ha podido identificar el porqué de esta vigilancia masiva a todo el mundo.

[…] Creo que es obligación de las agencias de inteligencia explicar por qué se necesita una vigilancia masiva, explicación que hasta el momento no han dado".

La seguridad nacional se ha vuelto una excusa de las agencias de inteligencia y de gobiernos para enmascarar al verdadero objetivo: conseguir más poder a través del control total de los ciudadanos [10]. Y buena parte de la ciudadanía es consciente de que las actividades que realiza en Internet, lo que está comprando o lo que está hablando por chat o por llamadas telefónicas está siendo vigilado, a pesar de estar lejos de relacionarse con actividades delictivas.

El informe Moraes hace referencia a la alianza de los Nueve Ojos y a la alianza de los Catorce Ojos. Los Nueve Ojos lo forman los cinco países que integran los Cinco Ojos más una serie de países que mantienen una relación de inteligencia relativamente estrecha con ellos: Dinamarca, Francia, Países Bajos y Noruega. Los Catorce Ojos lo integran todos los miembros anteriores más Alemania, Bélgica, Italia, España y Suecia, y su propósito es coordinar el intercambio de señales militares y de inteligencia entre ellos.

El informe también destaca la implicación, directa o indirecta, de empresas de Internet y de telecomunicaciones.

2.2- Revelaciones de Snowden y métodos de vigilancia

Rafael Bonifaz realiza una descripción de los programas de vigilancia de la alianza de los Cinco Ojos revelados por Snowden [11]. Explica cómo la NSA

intercepta y analiza información de las comunicaciones, no solo del resto de los países del mundo sino también de los habitantes de Estados Unidos, sin orden judicial. Esto último viola la ley FISA (Ley de Vigilancia de Inteligencia Extranjera) aprobada por el congreso norteamericano en 1978, por la cual para interceptar comunicaciones de ciudadanos norteamericanos se debe tener una aprobación en la corte de FISA. En 2001, pocas semanas después de los atentados del once de septiembre, se aprueba la Ley Patriota que, según ACLU (Unión Americana de Libertades Civiles), la sección 215 de esta ley permite al FBI forzar a ISPs (Proveedores de Servicios de Internet) a entregar información sobre sus clientes. La propia Ley Patriota indica que los ISPs tienen prohibido informar sobre esto a los usuarios que habían sido vigilados. La propia ACLU sostiene que la Ley Patriota viola la primera enmienda (que garantiza la libertad de expresión) y cuarta enmienda (que prohíbe realizar pesquisas sin orden judicial) de la constitución de Estados Unidos.

En el año 2008 se añadió la sección 702 a la ley FISA, la cual permitió justificar programas de vigilancia como PRISM (que se analizará más adelante), el cual permite vigilar incluso a ciudadanos norteamericanos. La EFF (Electronic Frontier Foundation) sostiene que la sección 702 viola la cuarta enmienda de la constitución de Estados Unidos.

En 2015, el Senado de Estados de Unidos aprobó la ley conocida como USA Freedom Act, que puso fin a la vigilancia masiva de ciudadanos de Estados Unidos (dentro de territorio norteamericano), pero no para el resto de los ciudadanos del mundo.

Revelaciones de Edward Snowden muestran que la NSA tiene acuerdos con empresas tecnológicas, los cuales le permiten a la agencia recolectar información sobre los usuarios de estas empresas. Nunca fue puesta en duda la veracidad de los documentos que prueban estas revelaciones por parte el gobierno de Estados Unidos. De hecho, luego de las primeras revelaciones, el hasta ese momento presidente de Estados Unidos, Barack Obama, dijo en rueda de prensa: “No me gustan las filtraciones, porque existe un motivo para que estos programas sean clasificados”[2]. [12]

[2] "I don't welcome leaks, because there's a reason why these programs are classified".

Las agencias de inteligencia recolectan tanto datos como metadatos. Los primeros son el contenido de las comunicaciones mientras que los segundos describen a ese contenido. En una comunicación telefónica el dato es el audio de la conversación y los metadatos son, por ejemplo, los números telefónicos, la hora en que se produjo, la duración de la llamada o los tipos de teléfono utilizados.

A continuación, se puede observar la Imagen 1, que corresponde a un documento revelado por Snowden donde se ve qué metadatos recopila la NSA de una llamada telefónica.

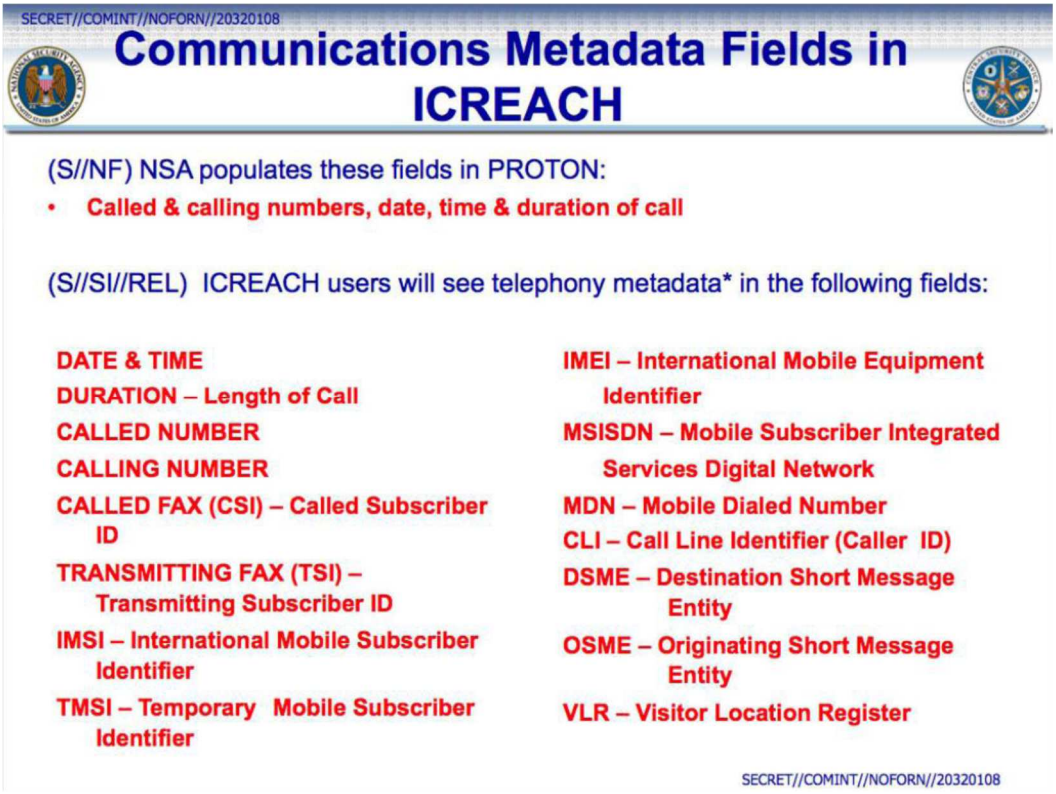

Imagen 1 - Metadatos recopilados por la NSA
Fuente: https://edwardsnowden.com/es/2014/05/18/communications-metadata-fields-in-icreach/

Según Snowden, en la mayoría de los casos, el contenido no es tan valioso como los metadatos, ya que se puede recuperar contenido basándose en los metadatos o, si no, simplemente se pueden recolectar todas las comunicaciones futuras que sean de interés ya que los metadatos indican qué flujos de datos son los que le interesan a los vigilados. [13]

Tal como menciona Eva Mejías Alonso [10], en una llamada telefónica los metadatos suelen ser bastante más informativos que el contenido de la

misma. Primero, porque el audio puede resultar bastante difícil de comprender debido a diferencias lingüísticas o por el uso de "códigos" o cualquier cosa que confunda el significado. Y segundo porque puede resultar muy difícil analizar ese audio desestructurado de manera automatizada. Los metadatos son nítidos y precisos y, lo más importante, son fáciles de analizar. Además, los metadatos pueden informar sobre muchísimas cosas relativas a costumbres, asociaciones, patrones de comportamiento, rutinas, hábitos, afiliaciones y aptitudes sociales.

Mejías Alonso también sostiene que las agencias de inteligencia pueden acudir a diferentes métodos para recopilar información. Estos métodos se pueden resumir en interceptación, cesión, compra y colaboración.

La recopilación de datos a través de la interceptación hace referencia al tipo de vigilancia secreta que ejercen los gobiernos a través de sus agencias de inteligencia, usando herramientas tecnológicas capaces de interceptar, recolectar, almacenar y analizar grandes conjuntos de datos procedentes de cualquier fuente, como los data centers de las grandes empresas tecnológicas y los cables submarinos de fibra óptica.

La recopilación de datos mediante la cesión se refiere a todos aquellos datos que ceden las grandes empresas a estas agencias, ya sea voluntariamente o por obligación.

La recopilación de datos a través de la compra hace referencia a las adquisiciones de software especializado en ciberseguridad a empresas privadas que se dedican a desarrollar y vender malware (software malicioso) y software de monitoreo ilegal de redes. Son empresas que trabajan codo con codo con gobiernos de todo el mundo.

Finalmente, gran parte de la entrada de datos a los sistemas de las diversas agencias de inteligencia no sería posible sin la colaboración con otras agencias, por diversos motivos. Acá entran en juego las alianzas de los Cinco, Nueve y Catorce Ojos.

A continuación, se describen estas etapas junto con algunos de los programas de vigilancia y herramientas usadas por las agencias de la Alianza de los Cinco Ojos, según los trabajos de Bonifaz y Mejías Alonso.

2.2.1- Interceptación

Comenta Bonifaz que la NSA posee 5 programas para la recolección de datos. Ellos son 3rd PARTY/LIAISON (se basa en la colaboración de la NSA con agencias de inteligencia de otros países), REGIONAL (basada en el espionaje que realiza la agencia en embajadas y consulados alrededor del mundo), CNE (consistente en ataques a redes de computadoras realizadas por la unidad TAO de la NSA), LARGE CABLE (encargado de recolectar la información en colaboración con empresas de comunicaciones) y FORNSAT (encargado de las comunicaciones satelitales).

Las revelaciones de Snowden también confirman la existencia de Echelon, bajo el mencionado nombre de FORNSAT, consistente en la interceptación de comunicaciones satelitales a través de estaciones terrestres que poseen antenas esféricas que permiten apuntar a varios satélites simultáneamente. Un ejemplo es la estación de Menwith Hill ubicada en Reino Unido, que se puede apreciar en la Imagen 2.

Imagen 2 - Estación de Menwith Hill
Fuente: https://theintercept.com/2016/09/06/nsa-menwith-hill-targeted-killing-surveillance/

XKEYSCORE es el programa de vigilancia más intrusivo de la NSA. Sus servidores almacenan datos procedentes de distintas fuentes como, por ejemplo, el espionaje de diplomáticos y líderes políticos extranjeros, el programa FORNSAT, los datos procedentes de proveedores de servicios de telecomunicaciones (Vodafone, Verizon, etc.), los datos procedentes de

aviones espía, drones y satélites norteamericanos, los datos procedentes de operaciones relacionadas con hackers y guerras cibernéticas, los datos de la vigilancia aprobada por el Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos (FISA) y los datos recopilados por otras agencias socias de la NSA (3rd Party).

Dentro de la alianza de los Cinco Ojos, y junto con la NSA, el GCHQ es la agencia con mayor acceso a las comunicaciones de Internet. La misma posee, al menos, dos programas de recolección de información de Internet y de comunicaciones telefónicas, llamados Mastering the Internet (Dominar el Internet) y Global Telecoms Exploitation (Explotación Global de las Telecomunicaciones). Por otra parte, para interceptar las comunicaciones vía fibra óptica posee el programa TEMPORA, aprovechando que por Reino Unido pasan gran cantidad de cables que unen Europa con América.

El programa TEMPORA, creado por el GCHQ británico, si bien permite capturar los mismos datos que XKEYSCORE y tiene el mismo límite de persistencia (tres días para datos y treinta para metadatos), lo hace a un nivel superior debido a su más amplio acceso a cables de fibra óptica. Se nutre principalmente del tráfico telefónico y de los datos que pasan por cables de fibra óptica de diferentes países. Además, a diferencia de lo que ocurre con la NSA, no se necesita de ninguna sospecha ni mucho menos de una orden judicial para espiar a un objetivo.

En buena medida, la intervención del GCHQ sobre los cables de fibra óptica se debe a que algunas compañías de telecomunicaciones se ven forzosamente obligadas a cooperar con dicha agencia y se les prohíbe revelar la existencia de las órdenes que las obligan a dar acceso a sus cables.

Tal como lo explica un artículo de The Guardian [14], de forma similar a lo que ocurre con XKEYSCORE, TEMPORA utiliza software para filtrar el tráfico que entra. El primer filtro que se suele aplicar es para descartar tráfico de poco valor, como las descargas Peer to Peer (P2P)[3], reduciendo un 30% del volumen. Y otro de los filtros es el empleo de selectores fuertes como

[3] P2P es un tipo de arquitectura de red de computadoras donde, a diferencia de la arquitectura cliente-servidor, cada nodo de la red puede actuar como servidor, es decir, ofrecer servicios, y como cliente, es decir, consumir servicios, al mismo tiempo. Por lo tanto, todos actúan como pares iguales.

cuentas de correo electrónico, direcciones IP, números de teléfono y asuntos de búsqueda.

Tanto la NSA como el GCHQ poseen dos programas, Bullrun y Edgehill, para poder acceder a datos cifrados, eludiendo los mecanismos de encripción utilizados. La poca información que hay al respecto de estos programas hablan de los acuerdos con empresas tecnológicas para implementar puertas traseras[4] en sus softwares de cifrado. Además, una diapositiva muestra que estas agencias tienen la capacidad de actuar contra los principales mecanismos de encripción, como SSL, SSH y VPNs (ver Imagen 3).

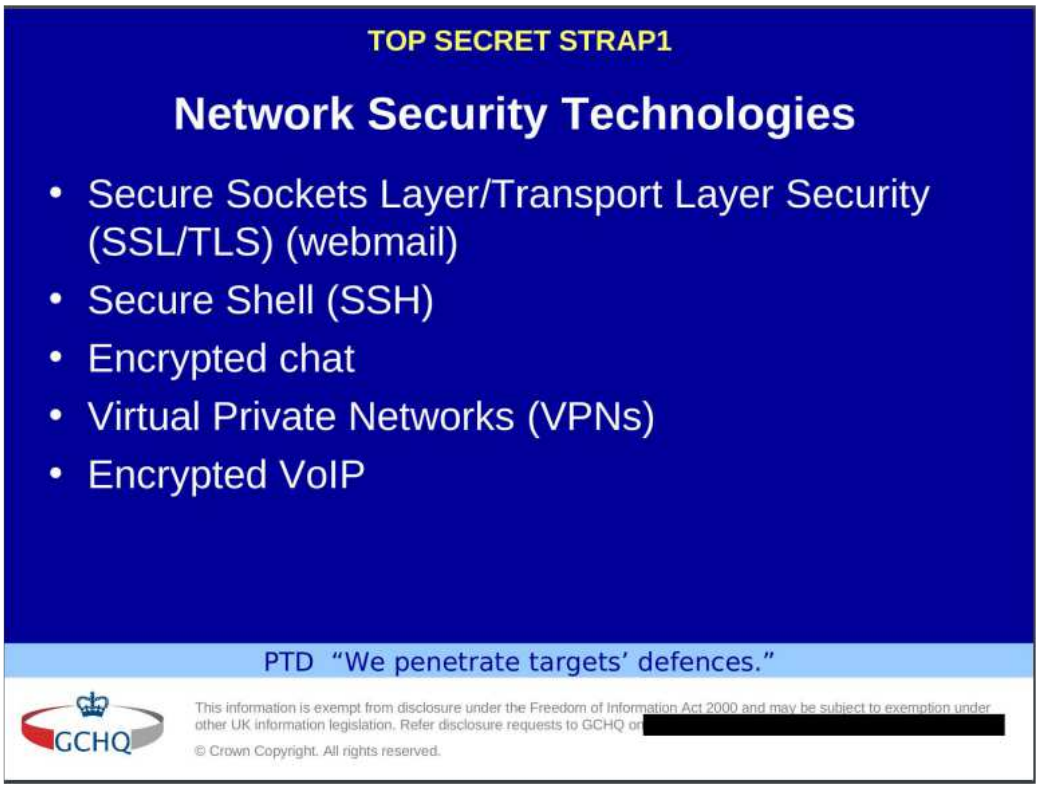

Imagen 3 - Medidas de seguridad que las agencias de inteligencia intentan vulnerar
Fuente: https://www.aclu.org/sites/default/files/field_document/GCHQ%20Presentation%20on%20the%20BULLRUN%20Program%27s%20Decryption%20Capabilities.pdf

Dishfire es un programa de la NSA que recopila de forma indiscriminada mensajes de texto. Su principal objetivo no es la comunicación que se a través de estos mensajes, ya que su uso ha caído estrepitosamente, sino aquellos datos que se reciben vía mensajes de texto, por ejemplo, los avisos

[4] Vulnerabilidad que permite entrar en un sistema informático por fuera de los accesos convencionales.

de llamadas perdidas (revelan red de contactos), los avisos por transacciones financieras (como los pagos con tarjetas, que se asocian al número de teléfono), información sobre viajes y geolocalización. Esta justificación de su existencia se puede ver en la Imagen 4.

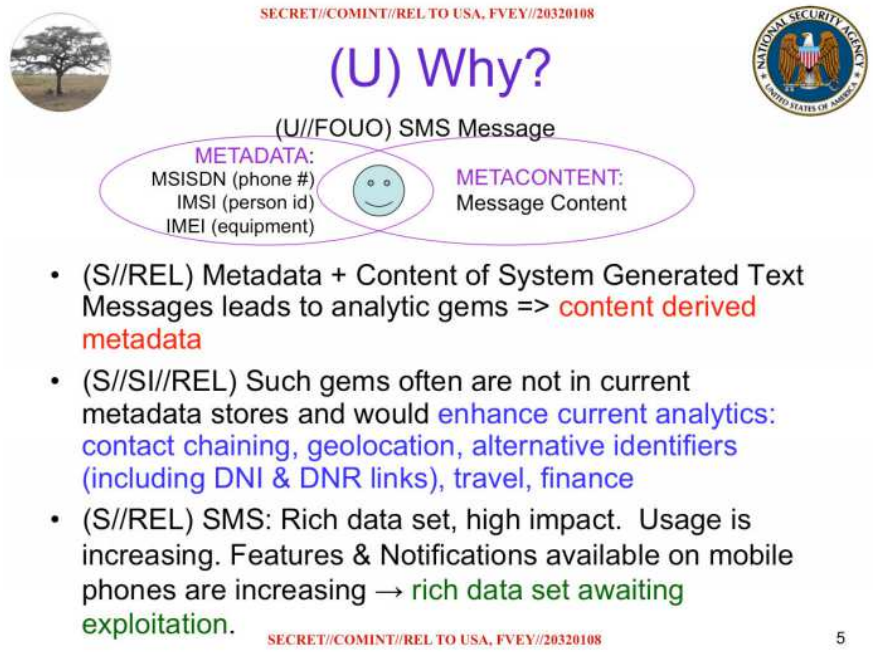

Imagen 4 - Justificación de la NSA a la vigilancia de los SMS
Fuente: https://edwardsnowden.com/docs/doc/sms.pdf

Los datos recolectados por Dishfire pasan por la herramienta PREFER que actúa como filtro y deja únicamente la información que sea de interés, que se almacena en diferentes bases de datos, según el tipo de dato que sea.

Otro programa de vigilancia masiva es MUSCULAR, que pertenece a la agencia GCHQ, aunque también es usado por la NSA. Su objetivo básicamente es interceptar el tráfico de datos que pasa por los cables de fibra óptica que transportan la información de los data centers de Yahoo! y Google (tanto metadatos como contenido), distribuidos entre cuatro continentes por cuestiones de performance de sus sistemas. Funciona como complemento de PRISM, el cual también permite acceder a los servidores de estos dos gigantes tecnológicos, pero con la diferencia de que para MUSCULAR no se requiere ninguna orden judicial y es mucho más agresivo que PRISM.

MUSCULAR consiste en un punto de acceso que lograron instalar estas agencias por el que pasa el tráfico de ambas compañías tecnológicas y,

aprovechando que dentro de la nube privada de estas compañías la información viajaba sin encriptar (al menos, hasta el momento en que este programa salió a la luz), recolectaba este tráfico y lo almacena en sus bases de datos.

Tracfin es un programa de la NSA que permite la colección de información bancaria y financiera [1]. Su principal función es analizar las transacciones de los usuarios de grandes compañías de tarjetas de crédito, principalmente de aquellas áreas geográficas que sean definidas como prioritarias. Esta información la obtiene accediendo a la base de datos de SWIFT (Society for Worldwide Interbank Financial Telecommunication), organización con sede en Bruselas que concentra las millones de transacciones bancarias que se realizan en el mundo.

Otra modalidad de espionaje es la que realiza el grupo SCS (Servicio Especial de Captación), formado por agentes de la NSA y de la CIA (Agencia Central de Inteligencia de Estados Unidos) en embajadas y consulados de Estados Unidos en distintos países del mundo recolectando información de las redes de telefonía celular. Uno de los casos más conocidos es el de la embajada de Estados Unidos en Berlín, Alemania. El mecanismo de vigilancia consiste en la existencia de paneles dieléctricos en las paredes superiores de estas embajadas con forma de ventanas para poder esconder antenas estratégicamente ubicadas que permiten interceptar las comunicaciones de telefonía celular de toda una ciudad.

Cuando las anteriores formas de espionaje no son posibles, la NSA puede recurrir a ataques informáticos a través de la unidad de Operaciones de Acceso Personalizado (TAO: Tailored Access Operations, en inglés). Para estos casos, uno de los principales objetivos son los sistemas de administración de cables submarinos de fibra óptica. Otros de los principales objetivos son las principales compañías tecnológicas, como Google, Yahoo! y Microsoft, que se comprobó que fueron atacadas por la NSA, la cual aprovechó que el tráfico de datos en sus redes internas viajaba de forma insegura para capturarlo mediante el programa MUSCULAR. También son un objetivo de interés para estos casos los ISPs, por la gran cantidad de tráfico que fluye por su infraestructura, como lo fue la empresa alemana Telekom.

Tanto la NSA como el GCHQ pueden recurrir a ataques informáticos con la técnica de Quantum Insert que se basa en la redirección de servidores, es decir, a un usuario le cambia la ruta de la página web redirigiéndole el tráfico a un servidor FoxAcid. Un servidor FoxAcid puede introducir malware, monitorear cualquier actividad en tiempo real que esté llevando a cabo el objetivo infectado y copiar toda la información en una base de datos, todo esto resultando muy difícil de detectar. Los servidores FoxAcid eligen automáticamente el exploit[5] a utilizar según el objetivo en cuestión.

Tal como lo muestra un artículo de Der Spielgel [15], varios servicios fueron explotados por la NSA a través de Quantum: Alibaba, Hotmail, LinkedIn, Facebook, Twitter, Yahoo!, Youtube, Microsoft o Gmail, entre otros.

Otro software que incluyen los servidores FoxAcid es Validator, un troyano que se implanta como puerta trasera en sistemas que operan con alguna versión del sistema operativo Windows. Permite infectar un ordenador con otro malware, como Olympusfire, el cual logra tener control total sobre un equipo: modificación, creación y copia de archivos, control sobre la webcam y los micrófonos, control de todas las comunicaciones que se realizan a través del equipo y copia de los nombres de usuario y contraseñas que utilice el usuario objetivo.

La división ANT de la unidad TAO se encarga de desarrollar el software y hardware para realizar estos ataques. Por ejemplo, la implantación de puertas traseras en equipos de redes de marcas conocidas (como Cisco y Huawei) o en los sistemas BIOS de computadoras y servidores, que no podrían ser detectadas por los sistemas operativos.

Un documento del año 2010 revelado por Snowden demuestra la forma en que la NSA intercepta paquetes con servidores, routers, etc. que se envían por el sistema de correo tradicional redirigiéndolo hacia un lugar secreto donde la unidad TAO lo abre, aplica el implante y luego lo vuelve a colocar en el circuito del sistema de correo para que llegue a su destinatario original [16]. Lo anterior se puede apreciar en la Imagen 5.

[5] Código ejecutable que permite aprovechar una vulnerabilidad en la seguridad informática.

(TS//SI//NF) Left: Intercepted packages are opened carefully; Right: A "load station" implants a beacon

Imagen 5 - Interceptación de equipos e insersión de implantes
Fuente: https://edwardsnowden.com/wp-content/uploads/2015/01/media-35669.pdf

Dice Bonifaz:

> *"Sería sencillo para la NSA interceptar los paquetes de equipos de redes que compran gobiernos extranjeros e implantar puertas traseras. De esta forma, cuando los equipos estén instalados, la NSA podrá recolectar información de redes donde se pensaba estarían seguras".*

Encriptar el tráfico en la red dificulta a la NSA la tarea de espionaje, sin embargo, tanto la NSA como el GCHQ destinan un importante presupuesto en estrategias para vulnerar comunicaciones cifradas.

2.2.2- Cesión

La unidad SSO (Operaciones de Fuentes Especiales) de la NSA se encarga de gestionar las relaciones con las corporaciones tecnológicas. La agencia cuenta al menos con dos programas para recolectar información con estas empresas. Uno de ellos es UPSTREAM, con el que se recolecta información a través de las empresas que manejan los cables de fibra óptica (como AT&T y Verizon), aprovechando que gran parte de la infraestructura de comunicaciones en el mundo está implementada con tecnología de empresas norteamericanas (lo que representa una ventaja para la NSA). Además, gran parte de las comunicaciones por fibra óptica entre distintos países del mundo pasan físicamente por Estados Unidos, como se puede ver en la Imagen 6.

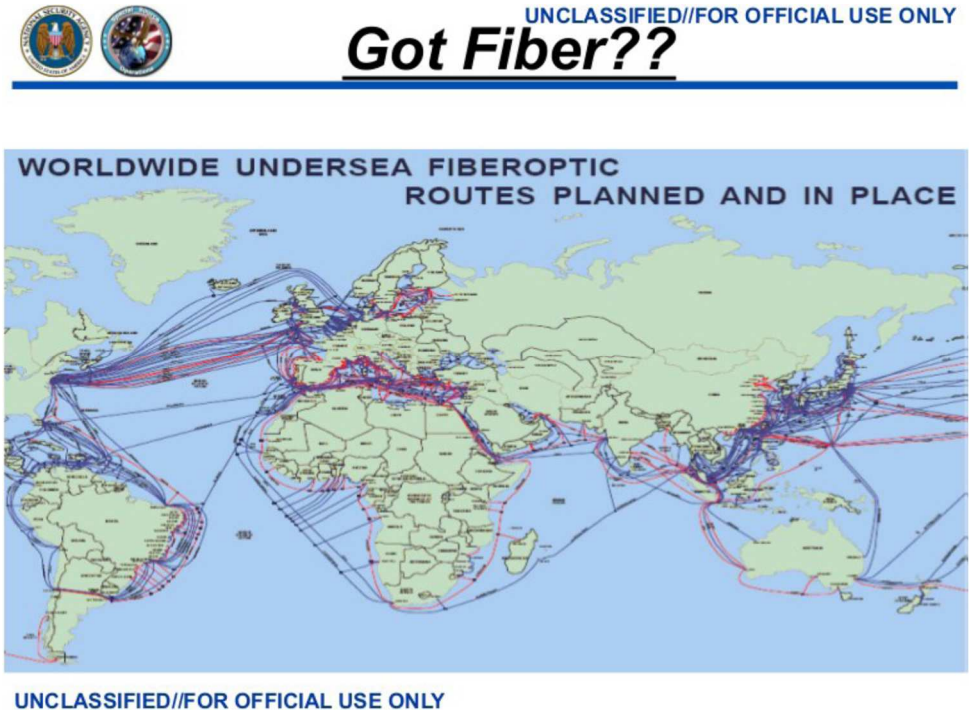

Imagen 6 - Mapa mundial de ruteo de fibra óptica
Fuente: https://edwardsnowden.com/wp-content/uploads/2013/11/sso4.pdf

El otro de los programas es el ya mencionado PRISM, el cual consiste en el trabajo que realiza la NSA y el FBI para acceder a información de los usuarios de empresas como Microsoft, Google, Yahoo!, Facebook, Youtube, Skype y Apple, como se puede ver en la Imágen 7.

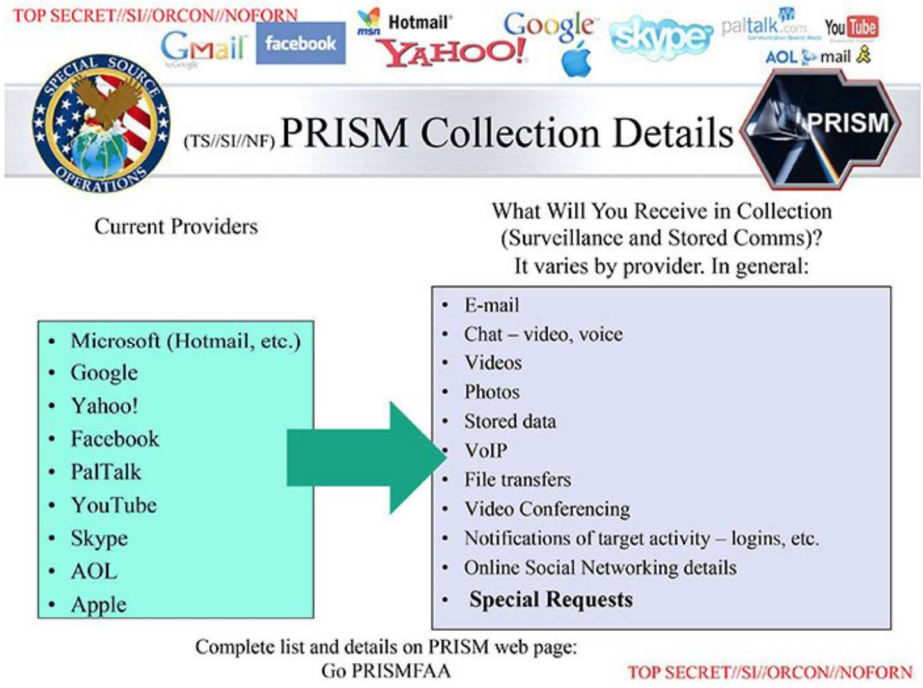

Imagen 7 - Programa PRISM
Fuente: https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Ejemplos de la información a la que tiene acceso la agencia con PRISM son correos electrónicos, chats, audios, videos y actividad en redes sociales. Sin embargo, no recolecta información todo el tiempo como sucede con UPSTREAM, sino que la NSA tiene acceso a los servidores en donde los usuarios guardan sus datos al utilizar los servicios que proveen dichas empresas (por ejemplo, al enviar un correo electrónico a través del servicio de Gmail, el mismo se almacena en servidores de Google, o al transferir un archivo por Dropbox, el mismo se almacena en los servidores de Dropbox). Es decir, cuando la NSA desea vigilar a alguien, la información ya fue recolectada y puede acceder a ella cuando lo necesite. Incluso, si un usuario elimina uno de estos archivos no hay garantías de que el mismo sea eliminado de los servidores de la empresa. Un ejemplo de esto último es que, en enero de 2017, se descubrió que Dropbox almacenaba archivos eliminados por los usuarios por hasta siete años. [17]

El funcionamiento técnico acerca de la forma en la que la NSA accede a la información de los usuarios de estas empresas no es claro. Sin embargo, estas empresas tienen obligación legal de proporcionar la información al gobierno de Estados Unidos.

Bonifaz comenta:

> *"La historia de colaboración entre el gobierno de Estados Unidos y las corporaciones no se limita a las empresas de PRISM. […] En 2001 la NSA creó el programa de vigilancia Stellar Wind del cuál AT&T fue la primera en sumarse. En 2006 Mark Klein, ex empleado de AT&T, denunció la existencia de un cuarto secreto donde operaba la NSA dentro de las oficinas de San Francisco".*

Microsoft colabora con la NSA en la implementación de líneas de código en sus productos (como el sistema operativo Windows y aplicaciones como Internet Explorer, Skype, y Outlook), para que generen agujeros de seguridad por los cuales la agencia acceder al control.

Buena parte de los datos recopilados por las grandes agencias de inteligencia son gracias a la colaboración de grandes compañías de telecomunicaciones y de algunos gigantes de Sillicon Valley, ya sea cediendo datos (como, por ejemplo, datos de sus usuarios a través del programa PRISM o datos sobre la tecnología de cifrado que utilizan) o a

través de la implantación de puertas traseras en sus sistemas o de vulnerabilidades en los softwares de encripción. A excepción de Microsoft, de la que se sabe que colaboró voluntariamente, no se puede garantizar de que el resto de las compañías hayan cooperado o que hayan sido víctimas. Sin embargo, con respecto a estas empresas, el informe Moraes expresa "su preocupación por el hecho de que estas organizaciones no hayan cifrado ni la información ni las comunicaciones que fluyen entre sus centros de datos, permitiendo de ese modo a los servicios de inteligencia interceptar información".

El programa PRISM se encuentra operativo desde 2007. Como se puede ver en una de las diapositivas de la NSA revelada por Snowden (Imagen 8), el programa contaba (al momento de creación de dicha diapositiva) con las siguientes características técnicas: dispone de nueve proveedores de servicios con base en EEUU que dan acceso a los selectores DNI (Digital Network Intelligence) -es decir, a cualquier actividad realizada vía Internet-, permite realizar búsquedas concretas al contenido de las comunicaciones almacenadas, puede procesar datos en tiempo real y es capaz de recolectar datos de voz.

Imagen 8 - Características técnicas de PRISM
Fuente: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH9cc7.dir/doc.pdf

Los programas de vigilancia que integran Upstream (Fairview, Stormbrew, Blarney y Oakstar), interceptan información procedente de los cables de fibra óptica, tanto llamadas como datos de Internet. No almacenan los datos que interceptan, pero sí permiten el acceso a ellos a tiempo real.

El funcionamiento de PRISM está descrito en otra de las diapositivas reveladas por Snowden (Imagen 9) y publicada por el diario The Washington Post.

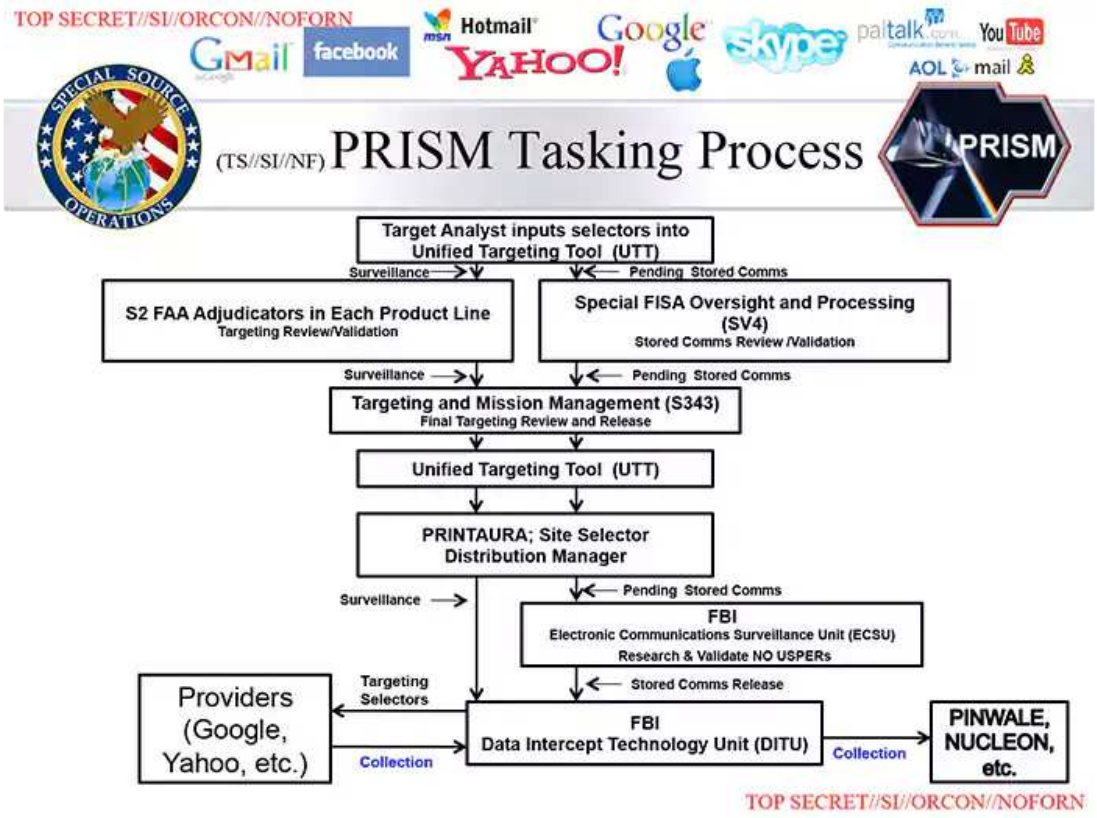

Imagen 9 - Funcionamiento de PRISM
Fuente: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Según indica el documento, un analista de la NSA identifica un objetivo a vigilar y lo ingresa en PRISM. Luego un supervisor se encarga de revisar los términos de búsqueda para asegurarse de que el objetivo a vigilar no sea un ciudadano estadounidense o un extranjero en suelo norteamericano. Luego, si la sospecha es razonable, da la aprobación para su vigilancia. El FBI se encarga de usar la tecnología de PRISM para acceder directamente a los servidores de las compañías que participan del programa. Una vez interceptados sus datos, estos pasan directamente a la NSA, a la CIA y al propio FBI sin ningún tipo de revisión.

Para la NSA tanto PRISM como UPSTREAM son sus dos principales programas para recolectar datos, tal como lo muestra la Imagen 10. En la misma puede verse que se define a UPSTREAM como una colección de comunicaciones procedentes de cables de fibra óptica e infraestructura por donde fluyen datos.

Imagen 10 - Definición de los programas UPSTREAM y PRISM
Fuente: https://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

De forma similar a la NSA, el GCHQ recolecta información a través de empresas de telecomunicaciones como Verizon, BT y Vodafone.

2.2.3- Compra

Gran parte de los presupuestos de las agencias de inteligencia se destinan a contratar los servicios de contratistas de inteligencia y empresas de ciberseguridad. A fines de 2011, WikiLeaks reveló documentación secreta, conocida como los SpyFiles, que muestra cómo los contratistas de inteligencia trabajan para las agencias de inteligencia y gobiernos de todo el mundo en labores de espionaje. Se tratan de compañías de países como Estados Unidos, Reino Unido, Alemania, Italia, Francia e Israel, que venden soluciones de ciberseguridad a gobiernos.

En agosto de 2012 Julian Assange, entrevistado por el periodista Jorge Gestoso [18], brindó las siguientes declaraciones:

> *"[…] la posición geográfica de Estados Unidos es tal que le ha dado gran poder a sus agencias de inteligencia. Las comunicaciones desde Latinoamérica fluyen hacia Europa y Asia, y atraviesan los Estados Unidos, donde son interceptadas por la Agencia Nacional de Seguridad, y luego juega una intercepción. […] El juego nuevo es la interceptación, es que registran todo. Es más barato registrar todo desde América Latina a los Estados Unidos y almacenarlo. Luego, dentro de un par de años, si te vuelves interesante para las agencias de EEUU y sus amigos y dicen <<revisemos qué estaba haciendo Assange hace dos años o hace un año>>, lo pueden revisar y ver quiénes son sus amigos, con quién se estuvo comunicando. Y esto no es especulación, existen compañías por todo el mundo que venden equipos para hacer esto, y tienen las guías de mercadeo para las agencias de inteligencia. […] Y nosotros publicamos esto a principios del año, llamado SpyFiles".*

Un grupo de investigadores del laboratorio The Citizen Lab de la Universidad de Toronto desarrolló estudios al respecto de estas compañías. Pudieron detectar tres empresas privadas dedicadas al desarrollo de soluciones y tecnologías de vigilancia, llamadas Gamma International, Hacking Team y NSO Group.

Gamma International tiene sede en Alemania y se dedica a vender equipos y software destinados a vigilancia y espionaje como, por ejemplo, FinFisher, un malware que infecta ordenadores para poder tener acceso remoto a toda su actividad en tiempo real.

Según un estudio realizado por Citizen Lab en 2013, FinFisher tiene presencia en más de 35 países, como se puede ver en la Imagen 11. Dentro de ellos se encuentran Estados Unidos, Austria, Alemania, Bulgaria, República Checa, Estonia, Lituania, Letonia, Hungría, Holanda, Rumanía y el Reino Unido.

Imagen 11 - Mapa del programa FinFisher
Fuente: https://citizenlab.ca/2013/04/for-their-eyes-only-2/

Por otra parte, Hacking Team es una compañía italiana que dispone de una amplia gama de herramientas que permiten controlar cualquier comunicación de un usuario en Internet, desencriptar archivos y correos electrónicos, grabar llamadas de Skype y de otras comunicaciones de VoIP[6], extraer contraseñas y activar remotamente micrófonos y cámaras de computadoras. Según un estudio de Citizen Lab en 2014, se calcula que los productos de Hacking Team tienen presencia en más de 20 países, como se observa en la Imagen 12, entre ellos México, Italia, Hungría y Polonia.

[6] VoIP, o Voz sobre Protocolo de Internet, es un conjunto de tecnologías que permiten el transporte de voz a través del Protocolo de Internet (IP), en lugar de hacerlo en forma analógica a través de los circuitos de la telefonía convencional.

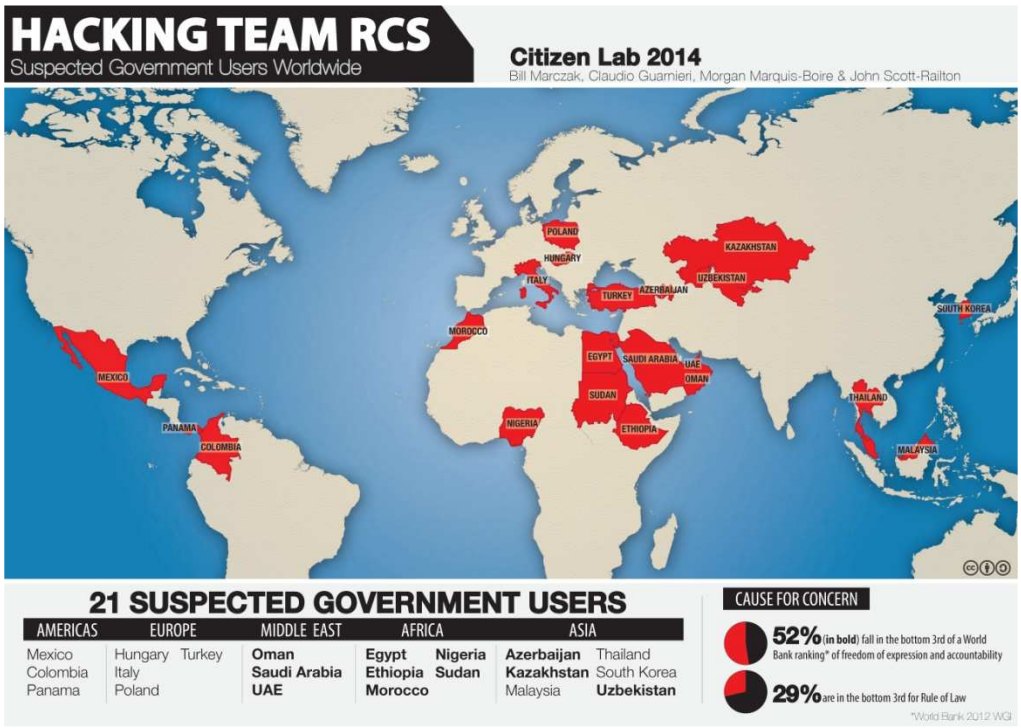

Imagen 12 - Mapa de la presencia de Hacking Team
Fuente: https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/

Otra investigación de The Citizen Lab publicada en 2018 [19], determinó que en 45 países (ver Imagen 13) se registraron evidencias de posible infección del software Pegasus que desarrolla la empresa NSO Group, una empresa israelí de desarrollo de software de ciberinteligencia. Pegasus es un spyware[7] que para que pueda ser instalado en el teléfono celular de una víctima requiere de ingeniería social, sugiriéndole a la víctima que haga clic en un enlace malicioso que se le envía. Una vez hecho el clic, Pegasus actúa para aprovechar vulnerabilidades zero-day[8] del dispositivo y luego poder hacer jailbreak del dispositivo, lo que en iOS significa poder instalar software que Apple no ha aprobado (en este caso, el spyware). Una vez vulnerado el equipo, quien opere a Pegasus puede ejecutar comandos en el teléfono celular infectado, ya sea para encender la cámara o micrófono y registrar la actividad alrededor del dispositivo, tomar capturas de pantalla o para recopilar información contenida en el dispositivo (chats y llamadas de

[7] Un spyware es un tipo de malware que actúa como espía en el equipo infectado, recopilando información de la víctima sin su consentimiento y transmitiéndosela a una entidad externa.
[8] Las vulnerabilidades zero days son aquellos agujeros de seguridad en los sistemas de los que por el momento no se conocen parches o actualizaciones de software que las solucionen.

aplicaciones de mensajería -como WhatsApp-, lista de contactos, contraseñas ingresadas, ubicación actual del GPS, datos de navegación, etc.).

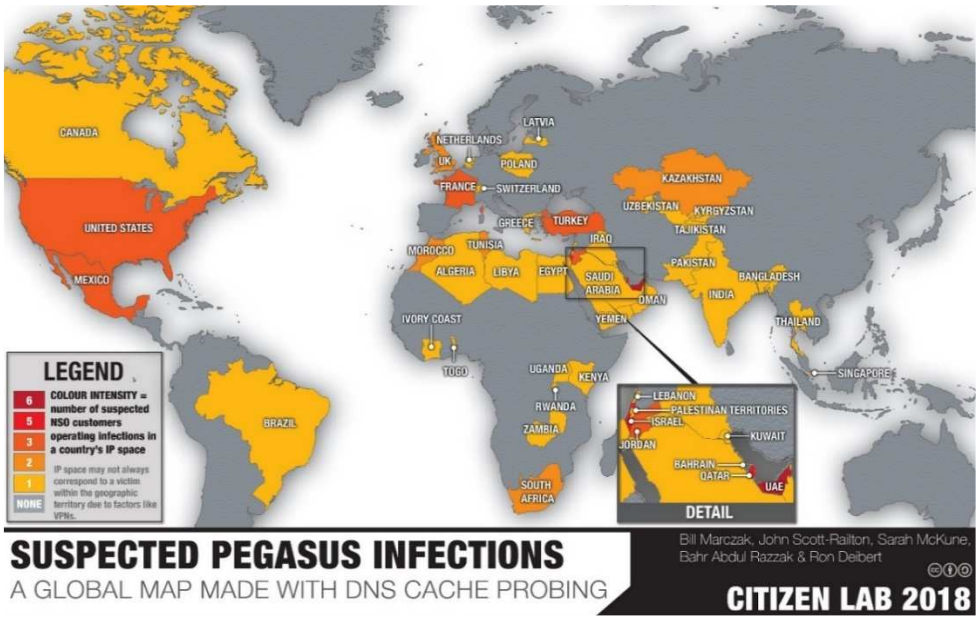

Imagen 13 - Mapa del programa Pegasus
Fuente: https://citizenlab.ca/wp-content/uploads/2018/09/Hide-and-Seek-Figure-2.jpg

Supuestamente, el objetivo del desarrollo de Pegasus es colaborar con los organismos gubernamentales a investigar a criminales y terroristas.

Un anterior informe publicado en 2016 por The Citizen Lab [20] describe como Ahmed Mansoor, un reconocido defensor de los derechos humanos oriundo de los Emiratos Árabes Unidos (EAU), fue un blanco de vigilancia del gobierno de su país. Dicho informe detalla que el gobierno emiratí contrató los servicios de NSO Group, que buscó infectar con software espía el iPhone de Mansoor al intentar explotar unas vulnerabilidades zero-day llamadas Trident, que afectaban a los sistemas iOS. Según informa The Citizen Lab, el software espía utilizado por el gobierno de EAU fue Pegasus.

A su vez, el informe destaca que Mansoor ya había sido blanco de software espía, en 2011 por parte de Gamma International y su spyware FinFisher, y en 2012 por parte del Sistema de Control Remoto de la empresa Hacking Team.

Cabe destacar que Pegasus no funciona solo para dispositivos iOS, sino que también tiene su versión para Android, llamada Chrysaor [21]. En el caso de esta última, si bien la modalidad es muy similar, no depende de explotar vulnerabilidades zero-days, sino que para poder instalar el spyware intenta

obtener acceso root al dispositivo (concepto similar al jailbreak, pero para Android). Obteniendo el acceso root, el spyware podría incluso permanecer luego de un reinicio a valores de fábrica del dispositivo.

Otro informe publicado en 2018 por el laboratorio canadiense [22] revela el intento de utilización del software Pegasus en veinticuatro periodistas mexicanos que investigaban cárteles (organizaciones criminales) por parte de clientes del NSO Group vinculados al gobierno mexicano.

Un artículo del New York Times de mediados del 2017 [23] manifiesta que el aumento de la vigilancia a defensores de derechos humanos y periodistas que exponen la corrupción en México comenzó luego de 2014, cuando estos últimos develaron escándalos del gobierno de Enrique Peña Nieto y derrumbaron la buena imagen pública que éste tenía. Y que, como represalia, comenzaron a vigilarlos y atacarlos, generando records de periodistas asesinados.

Mails filtrados por WikiLeaks en 2015 revelan el intento de parte de Nicolás Ruggiero, de la empresa argentina Tamce SRL, de adquirir el software de vigilancia Galileo, de la empresa italiana Hacking Team, para la AFI (Agencia Federal de Inteligencia) [24]. También revela supuestos intereses de la AFI de firmar un acuerdo con el NSO Group para adquirir Pegasus. Ninguna de las dos soluciones fue adquirida por el país sudamericano en esa ocasión.

Más adelante, en abril de 2018, se trató en el Congreso argentino un proyecto de reforma del Código Procesal Penal. En el artículo 30 de la reforma se planteaban nuevas “Técnicas Especiales de Investigación”, donde se habilitaba al Poder Ejecutivo, por medio de la AFI, a vigilar remotamente cualquier celular que consideren vinculado con secuestros, narcotráfico o crimen organizado. Finalmente, el proyecto no prosperó. [25]

La aprobación de esta reforma hubiera permitido la utilización del software Pegasus, supuestamente adquirido por el gobierno argentino en 2017 durante la visita del Primer Ministro de Israel Benjamín Netanyahu.

El Centro de Estudios Legales y Sociales (CELS) es una ONG argentina orientada a la promoción y defensa de los derechos humanos y el fortalecimiento del sistema democrático. Su presidente, Horacio Verbitsky, dijo que, durante su visita a Argentina en 2017, Netanyahu vino acompañado de una comitiva de empresas especialistas en ciberseguridad, algo

confirmado por el propio gobierno de Israel. Una de esas empresas fue el NSO Group. [26]

A mediados de 2019, un artículo del Financial Times [27] reveló que obtuvo documentación de venta del NSO Group que indica que a cualquier dispositivo infectado con Pegasus se le puede robar las credenciales de acceso a servicios en la nube (incluyendo a los de GAFAM[9]) que disponga el usuario y así poder acceder a los datos que almacena en ella. A pesar de esto, un portavoz del grupo israelí afirmó que "no proporcionan ni comercializan ningún tipo de software con capacidades de recolección masiva a ninguna aplicación, servicio o infraestructura en la nube".

A pesar de las fuertes acusaciones de violación de la privacidad y espionaje de políticos y activistas disidentes, Israel flexibilizó las reglas de exportación de armas cibernéticas, permitiendo ahora a empresas privadas adquirir su software espía [28]. A mediados de 2019 el Ministerio de Defensa israelí confirmó que el cambio entró en vigor hace aproximadamente un año, y mencionó que las empresas de su país que comercialicen estos programas deben cumplir con determinadas reglas y tener una licencia de exportación. Entre las compañías israelíes especialistas en armas cibernéticas se encuentran el NSO Group, Verint, y el contratista de defensa Elbit Systems, las cuales afirman cumplir con las reglas de exportación del gobierno y examinan a los clientes para garantizar que la tecnología sea utilizada con fines legítimos por gobiernos extranjeros.

El director del laboratorio The Citizen Lab de la Universidad de Toronto, Ron Deibert, dijo que era algo "desafortunado" que Israel flexibilice estas reglas.

2.2.4- Colaboración entre agencias

La NSA forma parte de la Alianza de los Cinco Ojos junto con GCHQ de Inglaterra, CSEC de Canadá, GCSB de Nueva Zelanda y ASD de Australia. Estas agencias trabajan de forma coordinada para recolectar y compartir información. No se espían entre sí, a menos que una agencia solicite a la otra recolectar información sobre sus ciudadanos.

Además de la Alianza de los Cinco Ojos, la NSA comparte información con otros países, los cuales se pueden ver en la Imagen 14.

---

[9] GAFAM es el acrónimo de las 5 empresas tecnológicas más populares a nivel mundial: Google, Amazon, Facebook, Apple y Microsoft.

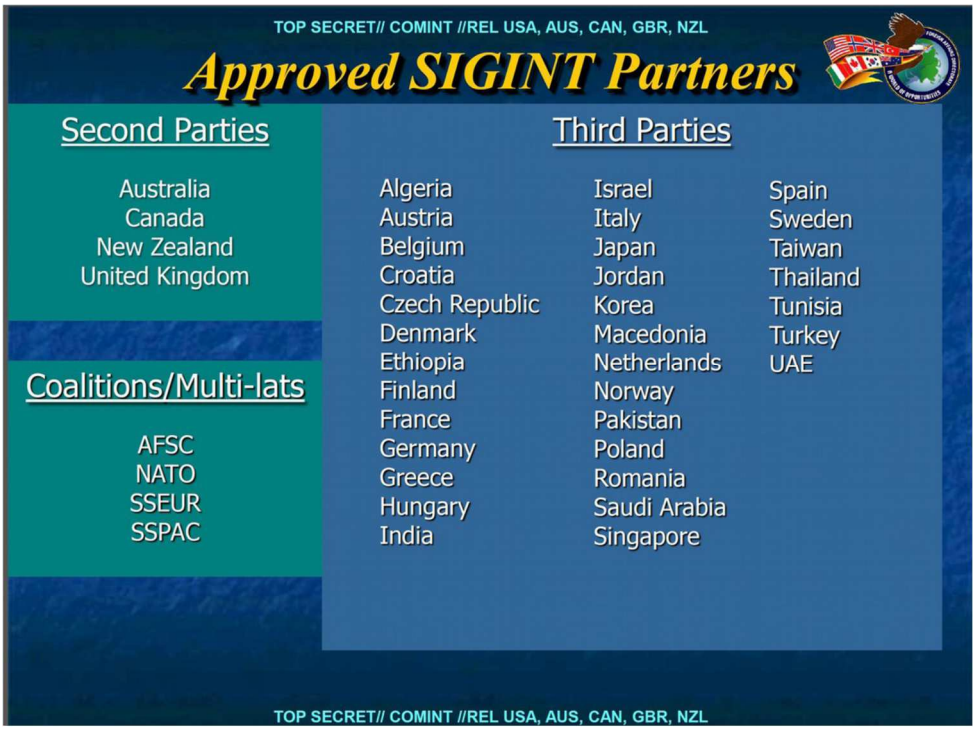

Imagen 14 - Países con los que los Cinco Ojos comparten datos
Fuente: https://edwardsnowden.com/wp-content/uploads/2014/06/fy13.pdf

Las agencias de inteligencia de distintos países europeos comparten información con la NSA, más allá de Reino Unido, principalmente en lo que respecta a datos de ciudadanos. Entre ellas se destacan las agencias de Alemania (BND), España (CNI) y Francia (DGSE). En caso de Alemania, la BND dio acceso a la NSA a dos de sus programas de vigilancia (Mira4 y VERAS) y, a cambio, la NSA le proveyó acceso a XKEYSCORE. En el caso de España, el ex presidente norteamericano George Bush ofreció en 2001 a José María Aznar, presidente de España en aquella época, compartir la red de inteligencia Echelon, supuestamente para combatir al terrorismo. Respecto a Francia, en 2012 la DGSE y la NSA firmaron un memorándum de intercambio de datos, que resulta muy atractivo para la NSA debido a que por las ciudades francesas de Penmarch y Marsella pasan cables submarinos que transportan datos entre Europa y África, los cuales son interceptados por la agencia francesa.

Por último, se encuentran aquellos países que son vigilados por Estados Unidos, pero con los que no comparte información, como sus adversarios China, Rusia, Irán, Siria y Venezuela, pero también otros países como México, Brasil y Argentina.

2.3- Análisis de los datos recolectados

En cuanto al análisis de los datos recolectados, solo hay evidencia acerca de la NSA, aunque permite dar una idea de cómo lo harían también el resto de las agencias.

El proceso de almacenamiento es el siguiente. El primer paso es definir la automatización del tráfico de datos según su tipo. Por ejemplo, el sistema Printaura (del programa PRISM), que distribuye el flujo de datos en función de si son datos de voz, texto, vídeo o metadatos, asignando tareas específicas que debe seguir el sistema. Si la recolección proviene de un tercero, el primer paso es la transferencia de datos hacia la NSA de forma encriptada, por ejemplo, usando el programa de encripción Mailorder.

El segundo paso consiste en filtrar el contenido de interés y desechar los que no son seleccionados, por ejemplo, mediante el programa Courierskill.

La NSA desarrolló reglas que permiten identificar tráfico de forma muy específica. Por ejemplo, puede filtrar por el tipo de aplicación (página web, correo electrónico, etc.), o siendo más específico se podría filtrar por ejemplo por proveedor de webmail (como Google o Yahoo!), o incluso por un usuario y contraseña determinado. Otra regla de filtrado es por alguna característica general, por ejemplo, el idioma del tráfico o su tipo de encripción. De esta forma, un analista de la NSA podría, por ejemplo, ver los mails de un objetivo de vigilancia, su historial de navegación o analizar llamadas de voz.

Otro programa es Scissors, que se utiliza en PRISM y recibe los datos según lo especifique Printaura y se encarga de formatearlos y clasificarlos de acuerdo a sus características para determinar en qué base de datos deberán almacenarse.

Luego, hay dos pasos que aplican solo a metadatos. Uno de ellos es su procesamiento, donde, de acuerdo al tipo de metadato, pasa por el programa Fallout o Fascia. Fallout es definido por la NSA como un DNI ingest processor y proporciona a los metadatos recopilados de actividades en Internet un formato común y fácilmente legible. Fascia funciona de la misma manera, pero recibe los metadatos de teléfonos y mensajes de texto.

El paso restante es almacenarlos en una base de datos intermedia. Como ejemplo, está la base de datos MAINWAY que almacena metadatos

telefónicos y de correos electrónicos y se encarga de entrecruzar ambos tipos de metadatos para obtener y almacenar vínculos entre ambos.

El último paso es el almacenamiento de los datos en bases de datos definitivas, de acuerdo a su clasificación o procedencia.

Para graficar lo anterior, la Imagen 15 es una diapositiva de la NSA que muestra el flujo de datos de PRISM. En la misma se puede ver, por ejemplo, el flujo entre los programas Printaura y Scissors y la intervención del programa Fallout para procesar metadatos.

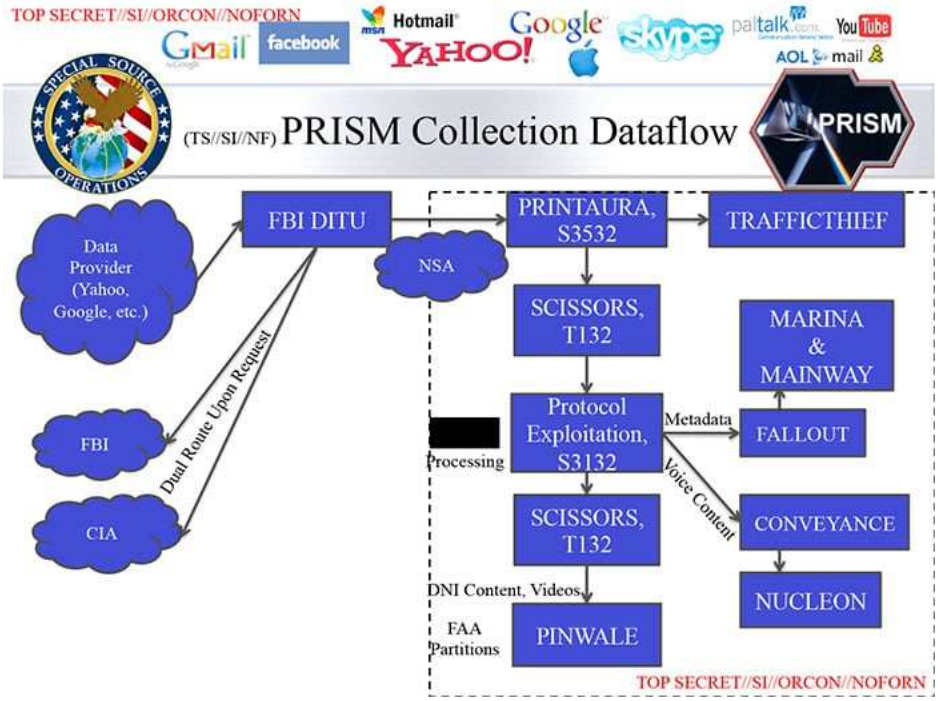

Imagen 15 - Flujo de datos del programa PRISM
Fuente: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Una vez almacenados los datos, la NSA dispone de varios sistemas integrados entre sus bases de datos para proceder a hacer búsquedas, monitoreos o entrecruzamiento de datos. También posee programas que permiten análisis de datos con una presentación visual sencilla. Uno de ellos es el software Boundless Informant, basado en la tecnología de big data[10], que permite seleccionar un país concreto y visualizar el volumen de metadatos de comunicaciones que se han recogido y almacenado. Otro de ellos es el software analítico Unified Targeting Tool (UTT), el cual sirve para seleccionar objetivos concretos para su vigilancia, mayormente personas

[10] Big data es el conjunto de tecnologías aplicadas al manejo de grandes volúmenes de datos, encargadas de obtener, analizar y realizar operaciones sobre los datos para generar nuevos conocimientos.

físicas concretas, pudiendo filtrar por nacionalidad, localización y “extensión” (por ejemplo, diplomático).

Sin embargo, la pieza clave para la NSA en el análisis de los datos es Accumulo, una gigantesca base de datos similar a BigTable de Google, pero con mayores prestaciones y un mayor nivel de seguridad. Permite categorizar cada uno de los datos que recibe, e incluso es capaz de encontrar conexiones entre datos aparentemente no relacionados (lo que se conoce como data mining o minería de datos). Además, implementa machine learning[11] y procesamiento del lenguaje natural, lo que le permite aprender conocimientos con nula o mínima intervención humana, auto-ajustarse para mejorar su rendimiento, identificar objetos a partir de imágenes, analizar e interpretar frases en un determinado contexto, inferir comportamientos futuros y analizar sentimientos para determinar reacciones. También, al alojarse en una nube de escalabilidad horizontal, cuantos más datos almacena más aumenta su rendimiento.

Accumulo se basó en Apache Hadoop, una tecnología de código abierto que permite que una base de datos disponga aún de más escalabilidad y de mucha más seguridad, logrando incluso controlar accesos a nivel de celda.

Es importante destacar que Accumulo es comercializada por Sqrrl Enterprise, comprada en 2018 por Amazon Web Services (AWS) [29], por lo que es posible que otras agencias de inteligencia también lo utilicen.

El principal programa para búsqueda de información (recolectada con algunas de las modalidades vistas anteriormente como FORNSAT, TEMPORA y TAO) es el ya descrito XKEYSCORE. Para 2008, XKEYSCORE funcionaba con 700 servidores distribuidos en 150 localidades alrededor del mundo, con MYSQL como motor de base de datos.

XKEYSCORE tiene como objetivo que los analistas de la NSA puedan buscar datos y metadatos de cualquier actividad llevada a cabo en Internet, incluso sin tener un "selector fuerte" como, por ejemplo, una cuenta de correo electrónico, un número de teléfono o una dirección IP[12]. En este caso,

---

[11] Campo de la Inteligencia Artificial que tiene la finalidad de construir máquinas que aprendan automáticamente con una mínima o nula intervención humana.

[12] Una dirección IP es un conjunto de números que identifica de forma lógica a un dispositivo que se conecta a Internet a través de una red de datos que utilice el Protocolo de Internet (IP).

los analistas también podrían utilizar "selectores suaves", como el tipo de navegador utilizado o el idioma en el que se navega, pudiendo encontrar el contenido deseado y extraer de él un selector fuerte, además de detectar mucha información que habría sido imposible de encontrar usando solamente selectores fuertes.

Una de las funcionalidades de XKEYSCORE es su sistema de obtención de correos electrónicos, el cual solo requiere que el analista ingrese la dirección de correo electrónico del objetivo, una justificación de su búsqueda y escoger el periodo de tiempo deseado. El resultado de la búsqueda le permite al analista seleccionar cuál de los mails obtenidos desea leer.

Otra de las funcionalidades de XKEYSCORE es la herramienta DNI Presenter, que le permite a un analista acceder no solo a los correos electrónicos de un objetivo, sino que también le permite leer mensajes privados de su cuenta de Facebook. Solamente es necesario que el analista introduzca el usuario de la red social del objetivo en la base de datos del programa y un intervalo de fechas en una interfaz gráfica muy simple, como se ve en la Imagen 16.

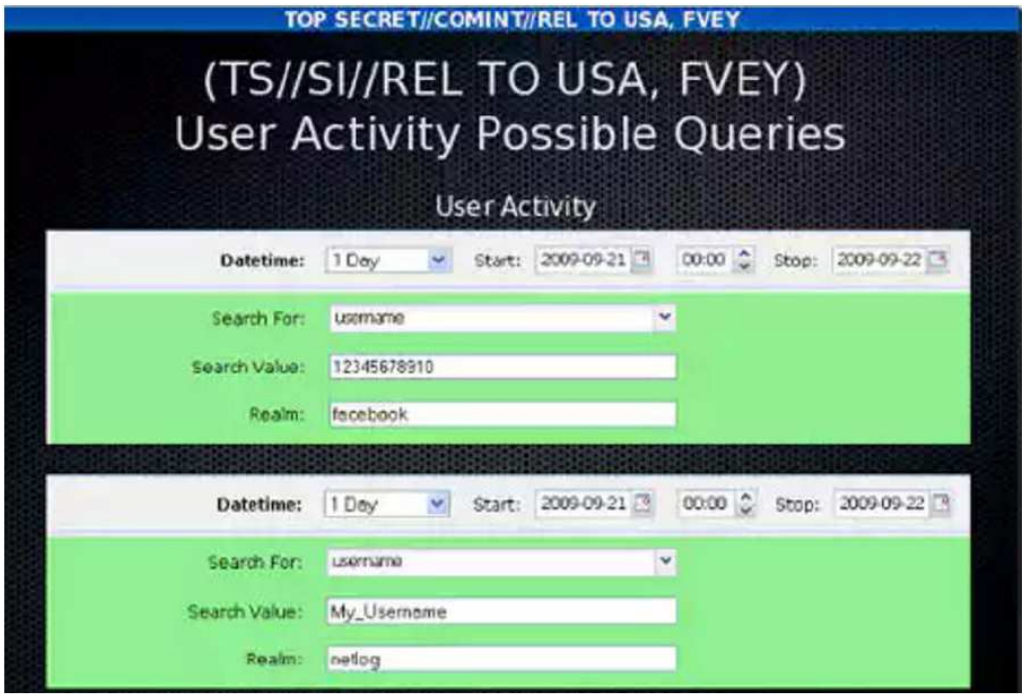

Imagen 16 - Posibles consultas sobre XKEYSCORE
Fuente: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

La NSA posee otros sistemas que permiten procesar y analizar información que se almacena por más tiempo, como MAINWAY, NUCLEON y PINWALE.

El primero almacena y procesa metadatos recolectados desde señales de telefonía y de comunicaciones en Internet, y luego de ser procesados se almacenan por un año en otro sistema llamado MARINA.

El segundo se encarga de las comunicaciones de voz recolectadas, analizándolas y permitiendo a los analistas realizar búsquedas de llamadas por voz o por IP.

Y el tercero se encarga de almacenar hasta por cinco años la información relevante que se le envíe desde XKEYSCORE, tanto datos como metadatos.

Además de recolectar información, la NSA tiene los mencionados programas para acceder de forma rápida y sencilla a ella y para procesarla. El propio Snowden afirmó en 2013 que él, sentado en su escritorio tenía la capacidad de intervenir a cualquier persona, incluso hasta el presidente, solamente disponiendo de su correo electrónico personal. [30]

Si los sitios web vigilados por la NSA no poseen implementado TLS[13] sobre HTTP (es decir, HTTPS) le resulta más simple a la agencia analizar el tráfico. Si el sitio web funcionara con HTTPS, la NSA debería buscar realizar ataques más sofisticados, o bien, por ejemplo, acceder a las llaves privadas de los certificados digitales de los blancos de vigilancia (por ejemplo, vía el programa MUSCULAR), o solo analizar metadatos del tráfico y no su contenido.

[13] TLS (Seguridad en la Capa de Transporte, por sus siglas en inglés) es un conjunto de protocolos criptográficos diseñados para contribuir con la privacidad y autenticación en las comunicaciones por redes.

3- Historia de Internet y neutralidad de la red

3.1- Conceptos y principios sobre Internet

El conocimiento e información materializados en bits[14] circulan a través de toda la estructura de Internet, la cual, tal como describe Martín Gendler [31], puede observarse compuesta por cinco niveles.

El primero de ellos es el nivel de infraestructura, el cual incluye los cables submarinos y los satélites, que transmiten datos de forma intercontinental, y los tendidos de fibra óptica, que distribuyen los datos dentro de los continentes. Todos ellos solo pueden ser instalados y mantenidos por empresas que dispongan de un gran capital. En relación a esto último, tanto los cables submarinos como los satélites se encuentran en manos de unas pocas empresas.

Otro nivel es el de hardware, donde se encuentran los Proveedores de Servicios de Internet (ISP), que son aquellas empresas encargadas de que los bits lleguen desde el nivel de infraestructura hacia cada terminal de sus usuarios a través del router o modem que cada uno de estos proveedores entrega al cliente que contrata sus servicios. También incluye a los dispositivos digitales de los usuarios (PC, smartphone, tablet, etc.), que reciben dichos bits, y los servidores físicos de las principales compañías tecnológicas que ofrecen servicios (Google, Microsoft, Facebook, etc.). Tanto estos últimos como los ISP también son oligopolios.

Un tercer nivel es el de software, donde se encuentran los programas y los protocolos (principalmente, TCP/IP) que permiten el envío y la recepción de bits en los dispositivos físicos.

Los otros dos niveles son los contenidos (lo que representan los bits cuando son procesados por los dispositivos) y las redes sociales.

Cada vez que un usuario realiza una acción en Internet a través de un dispositivo digital se generan múltiples paquetes de datos que son a su vez fraccionados, y estas fracciones (o fragmentos) pasan por un ISP y viajan a través de la capa de infraestructura hasta el servidor destino, donde se ensamblan para reconstruir los paquetes originales. Según la acción

[14] El bit, acrónimo de binary digit (dígito binario, en inglés), es la unidad mínima de información empleada en informática, con la cual se puede representar solamente dos valores o dos diferentes estados: 1 o 0.

ejecutada, el servidor destino genera una respuesta, la cual puede dirigirse al usuario original o a otro u otros usuarios.

Previo a transmitir los datos, se lleva a cabo la acción conocida como conmutación, la cual permite establecer la vía a partir de la cual se transportarán dichos datos. El tipo de conmutación más ampliamente utilizada en Internet es la conmutación de paquetes, que genera una vía por cada fragmento a ser transmitido (pudiendo variar entre los diferentes fragmentos), ya que es más eficiente y tolerante a errores (por no seguir una única ruta). No garantiza la entrega de todos los fragmentos, sino que realiza el "mejor esfuerzo" para hacerlo (si en el camino un paquete se pierde, se enviará nuevamente), por lo que no es ideal para aquellos contenidos que requieran alta calidad o necesiten hacerse en tiempo real (por ejemplo, una videoconferencia o un juego en línea). Para estos últimos casos, es conveniente utilizar una conmutación por circuitos, donde se establece un canal dedicado especialmente a la transmisión de esos datos.

Por otra parte, tal como lo explica Eduardo Bertoni [32], la arquitectura original de Internet se basó en tres principios de diseño: el de modularidad, el de estratificación y el de extremo a extremo.

El principio de modularidad establece que los componentes de un sistema deben estar lo menos acoplados posibles, es decir, que sean altamente independientes. Esto permite que el sistema se pueda dividir en módulos con solo las interdependencias necesarias. El propósito es que los componentes puedan diseñarse con la mayor libertad posible sin preocuparse por adaptarlos al resto de los componentes, de forma tal que se incrementan las posibilidades de cambios en el sistema ya que las modificaciones en capas superiores no afectan a las capas inferiores.

El principio de estratificación (o división en capas) es el encargado de restringir las interacciones entre los módulos. La idea es que cada capa ofrezca sus servicios a su capa siguiente, cumpliendo cada capa una función más compleja que su predecesora, preocupándose solo por lo que ocurre en la capa predecesora, de quien recibe información. Así, a modo de ejemplo, quien desarrolla una aplicación solo necesita saber en qué sistema operativo va a funcionar su programa, siendo el sistema operativo una capa inferior a la aplicación.

El modelo TCP/IP, que es el mayormente utilizado para las comunicaciones en redes, propone cuatro capas para dividir las funciones de la red. Así lo explica Bertoni:

> *"La capa más baja es la de «enlace», que contiene los protocolos responsables del transporte de paquetes a través de una red física (por ejemplo, la de una oficina o universidad); le sigue la capa «internet», que permite transportar paquetes a través de un conjunto de redes interconectadas, sin importar en dónde esté cada dispositivo; en seguida, está la capa de «transporte», que reparte los paquetes desde y hacia las aplicaciones de los dispositivos finales; por último, está la capa de «aplicaciones», que contiene una serie de protocolos que permiten la comunicación entre las partes (correo electrónico, world wide web, redes de pares, video)".*

Por último, el principio de extremo a extremo establece las funciones a cumplir en cada capa, sugiriendo que cuanto más complejas, específicas y cercanas a la interacción con el usuario sean más arriba deben situarse. El propósito de este principio es que las capas vinculadas a las aplicaciones (las más complejas, y por ende las de más arriba) residan en los extremos de la red (es decir, en los dispositivos de los usuarios que se conectan a la red) y que el resto de las capas sean menos especializadas y se dediquen a "servir" a los extremos. De esta forma, se puede lograr un escenario propicio para el crecimiento de Internet (ya que no dependerán de las aplicaciones por estar éstas en capas superiores) fomentando a que los desarrolladores de aplicaciones sean creativos e innovadores para adaptarse a estos cambios en la red.

Estos tres principios se complementan con la conmutación de paquetes que se utiliza en Internet, mencionada anteriormente.

Es en base a estos tres principios que se consolida el concepto de neutralidad de la red, ya que, con este diseño de la red, los propietarios de alguna parte de la red (por ejemplo, los ISP) no tienen necesidad de adaptarse o actuar a favor del contenido de alguna aplicación, ya que ésta se encuentra en alguna capa superior.

Antes de profundizar sobre la neutralidad de la red, es necesario tener presente detalles sobre el origen de Internet y su evolución.

3.2- Origen de Internet

En su libro “El enemigo conoce el sistema” [33], Marta Peirano narra el origen y la revolución de Internet y compara su infraestructura con la de las ciudades que fueron construidas por gobiernos imperiales y autoritarios. Estas últimas son estructuras amuralladas de círculos concéntricos en torno al individuo más poderoso (el gobernante), hacia donde conducen todas las calles más importantes. Estas estructuras centralizadas no están diseñadas para la eficiencia, sino para ejercer control e infundir miedo. En cambio, las estructuras del siglo XXI, como la red de redes, no están diseñadas para demostrar poder e inspirar terror, sino para disimular dicho poder y generar la confianza en la gente de que se trata de un servicio bienintencionado y eficiente. Los “imperios” del siglo XXI intentan convencer a las personas de que la red es una estructura neutral, democrática y libre.

Esta última falacia tiene un momento en el que fue cierta. En 1964, en plena Guerra Fría, el ingeniero eléctrico Paul Baran, trabajando para las Fuerzas Armadas estadounidenses, inventó la conmutación por paquetes y un diagrama de red de comunicaciones descentralizada capaz de sobrevivir a un ataque nuclear, ya que no había un único punto de fallo en el que se concentrara toda la información, como ocurría con la conmutación por circuitos que existía en ese momento. Este invento se pudo estrenar en 1969, cuando se envió un mensaje entre la Universidad de California y el Instituto de Investigación de Standford, en Menlo Park. Esta unión de los nodos de ambas instituciones constituyó la red ARPANET. En los años siguientes, ARPANET fue conectando laboratorios universitarios con bases militares y empresas tecnológicas.

En 1971, ARPANET fue ofrecida a AT&T, por aquel entonces la única compañía de telefonía estadounidense, para que la expandiera y comercializara, pero la rechazó por ser incompatible con sus redes basadas en conmutación por circuitos y su estructura, que le impedía tener un control total de la red. A su vez, el presupuesto que la Casa Blanca le destinaba era muy bajo. De esta forma, como indica Peirano, queda claro que “[…] si Internet nació como una red abierta y fuertemente descentralizada fue

porque el Gobierno estadounidense no entendió su potencial y porque la única operadora que podía comprarla dijo que no la quería".

Recién se tomó dimensión de lo que significaba ARPANET en una conferencia realizada en Washington en 1972, donde la red norteamericana fue la estrella entre otras redes de comunicación entre ordenadores presentadas por otras naciones.

Luego, surgió la necesidad de interconectar todas las redes, las cuales podían ser muy diferentes entre sí. En otras palabras, la cuestión era cómo lograr que todos los ordenadores en cada una de esas redes variadas piensen que son parte de una misma red común. Pero a su vez, la solución debía ser compatible con la administración de la infraestructura (es decir, las operadoras), que era un monopolio, y también debía ser neutral (sin beneficiar a un determinado tipo de información, servicio o usuario).

Dentro de la conmutación por paquetes, se debatieron dos versiones de tratamiento de los paquetes de datos. Una versión planteada fue el "circuito virtual", donde el recorrido de los paquetes de datos y el ancho de banda eran preasignados por la operadora (como en una llamada telefónica). La otra versión era el "datagrama", donde la responsabilidad de recalcular la trayectoria óptima de los paquetes de datos, en función del tráfico, ancho de banda disponible y nodos disponibles en ese instante, caía sobre los propios nodos. Las operadoras, como AT&T, pujaban por el modelo de circuito virtual, IBM y el resto de compañías tecnológicas por el modelo de datagrama. Tras años de debate entre científicos de laboratorios estadounidenses y europeos aliados (como Inglaterra y Francia), se optó por el modelo de datagrama, y allí surgieron los protocolos TCP/IP (Protocolo de Control de Transmisión / Protocolo de Internet), que rigen la red desde entonces.

Esta solución, con la que los científicos pretendían intercambiar sus conocimientos interdisciplinarios para beneficio de la humanidad (o, al menos, de sus aliados), fue presentada al Comité Consultivo Internacional Telefónico y Telegráfico, que establecía los estándares internacionales, el cual la rechazó. Los expertos de este comité eran todos ingenieros de telecomunicaciones de las grandes operadoras telefónicas. El modelo OSI (Interconexión de Sistemas Abiertos) si fue aceptado por el comité y tenía el

apoyo de las operadoras telefónicas, como AT&T, pero a principios de los noventa el proyecto se estancó, principalmente porque cada país armó su propia red y los sistemas de compatibilidad entre las mismas no eran eficientes. Del otro lado, ARPANET no paraba de crecer y comenzaba a transformarse en un fenómeno social (a partir de la llegada a los hogares de las computadoras personales en los años ochenta, Internet dejó de ser algo propio de laboratorios y universidades para convertirse en una tierra de oportunidades para personas y organizaciones).

Al final de 1983, la agencia DARPA (Agencia de Proyectos de Investigación Avanzados de Defensa, aunque conocida en sus orígenes como ARPA), una de las principales desarrolladoras de ARPANET, abandonó el protocolo original de ARPANET, obligando al resto de las redes a utilizar TCP/IP sino querían quedarse fuera del sistema. Ese momento, técnicamente, se conoce como el nacimiento de Internet. A finales de 1985 ya había 2.000 computadoras conectadas por TCP/IP. En 1987 eran 30.000 y en 1989 159.000. Con la ley High Performance Computing and Communication Act de 1991, bajo la presidencia de George H. W. Bush, el uso de Internet dejó de limitarse al ámbito académico y científico y se extendió a la industria, al gobierno y a la sociedad civil. Ya en 1993, bajo la presidencia de Bill Clinton, se privatiza Internet, habiendo cuatro empresas que deciden quién se conecta con quién y de qué forma, de acuerdo a sus propios intereses y alianzas: MAE-East en Washington, Sprint en Nueva York y dos particiones de AT&Y, Ameritech en Chicago y Pacific Bell en California. Con el paso del tiempo, y a escala mundial, Internet fue quedando en manos de unos cuantos monopolios, tanto la administración de cables submarinos como las redes terrestres, transformándose en un mito el hecho de que Internet sea un sistema de comunicación distribuido y neutral como lo fue en sus inicios.

Internet tampoco era para todos. Era solo para quienes sabían operar con una consola de comandos y con ella usar el correo, leer noticias o buscar información en bases de datos. Hacía falta un sistema capaz de abstraer esta complejidad y permitir una navegación apta para todos los usuarios. Este fue creado en los primeros años de la década de los noventa, cuando el científico informático Tim Bemers-Lee y sus socios presentaron la [World Wide] Web. También, inventaron el lenguaje de etiquetas HTML, para que

cada información de Internet pueda ser convertida a este lenguaje y depositada en una computadora que la comparta a Internet (servidor) de forma organizada, conformando una página web. También, crearon el protocolo HTTP, para que los usuarios que naveguen por Internet pudieran comunicarse con ese servidor, a través de un navegador que le permitiera ver gráficamente la página web.

La World Wide Web, que llevaría Internet a los hogares y negocios de millones de personas de todo el mundo, sirvió como plataforma para posibilitar e implantar cientos de nuevas aplicaciones.

3.3- Revolución sobre Internet

Intentando recuperar el espíritu original de Internet (compartir información entre pares de manera segura), Shawn Fanning y Sean Parker lanzaron Napster en 1999, el primer sistema P2P para el intercambio masivo de archivos de música. Cada usuario que accedía a la aplicación podía elegir su nombre de usuario (un nick, no necesariamente su nombre real) y su ordenador se convertía en un servidor más de la red, compartiendo con el resto los archivos de sus discos duros. La única infraestructura que tenía Napster era un servidor central que mantenía una lista actualizada de todos los archivos disponibles para compartir en cada momento, y un buscador. Cuando un usuario quería una canción, utilizaba el buscador para ponerse en contacto con otro usuario que la tuviera y el archivo pasaba directamente de un ordenador al otro. Era una red de pares, sin el control de nadie, sin prejuicios ni estructuras centralizadas en manos de multinacionales. Su arquitectura estaba pensada para intercambiar archivos de manera eficiente sin vigilar ni controlar a los interlocutores. La presión judicial por infracción masiva de copyright consiguió cerrar la plataforma en 2002.

Los sucesores de Napster fueron adoptando formas más distribuidas, prácticamente imposibles de eliminar, como Gnutella, la primera red de pares totalmente distribuida, lanzada en el 2000. Y, como estaba licenciada bajo GPL (más adelante se darán más detalles de la misma), pronto nacieron cientos de clones de Gnutella. Este movimiento a favor del libre intercambio de archivos desencadenó la creación de partidos políticos en

Europa y Estados Unidos. Y en 2010 se crea la asociación política Internacional de Partidos Pirata (Pirate Parties International o PPI), que buscaba introducir en el Parlamento el debate político sobre temas como la vigilancia masiva, la manipulación mediática, la gestión de derechos de propiedad intelectual y el manejo de datos personales. En 2012, con el apoyo de millones de personas, e incluso de Google y Wikipedia, el consorcio de partidos pirata logró frenar las leyes SOPA y PIPA que buscaban cerrar los sitios webs acusados de alojar material protegido por derechos de autor (se verán más detalles de SOPA y PIPA en la sección "Ámbito legal de la vigilancia y de la neutralidad de la red").

Primero iTunes (de Apple) y luego Spotify, ambos servicios pagos para el acceso a archivos musicales, actuaron como intermediarios entre las discográficas y los usuarios, proponiéndose como la "alternativa viable" a la "piratería del P2P", aunque por ellos circulen millones de archivos mp3 piratas.

3.3.1- Software libre

Para finales de los noventa, los programadores compartían sus líneas de código, sus ideas y consultas en los canales de comunicación y foros, como IRC, sin pensar en la propiedad intelectual, ya que el objetivo era aprender y compartir lo aprendido para cooperar en la construcción de software transparente. Richard Stallman, que comulgaba con estos principios, colaboró en este sentido para evitar caer en la comercialización y privatización del software. Para esto, Stallman creó su sistema operativo, el GNU (que, luego de la contribución de Linus Torvalds con su kernel, surgió el sistema operativo GNU/Linux, o simplemente Linux), y lo protegió con las mismas armas con las que los monopolios, como IBM o AT&T, protegían su software: con una licencia de propiedad intelectual, creada por el mismo y llamada GPL (Licencia Publica General, por sus siglas en inglés). La GPL establece que el código del software (libre) tiene que poder ser usado, estudiado, compartido y modificado. Fue la primera licencia de copyleft y es tan estricta como el copyright, pero tiene el sentido inverso: toda copia o derivado del software libre debe preservarse como software libre, no pudiendo hacer privado el código y enriquecerse a costa del trabajo de otros.

El término libre no significa necesariamente que el software sea gratis, ya que está permitido hacer distribuciones y venderlas o cobrar por su mantenimiento (el mantenimiento, a diferencia del software propietario, no es un monopolio ya que existe toda una comunidad que tiene acceso al código fuente). El término libre se refiere a libertad de expresión. Dicho por el propio Stallman, si el software no es libre entonces es el programa quien controla al usuario, y no viceversa, lo cual permite a sus desarrolladores vigilar y censurar al usuario.

El movimiento del software libre generó preocupación en los gigantes tecnológicos, que lo veían como una amenaza. Para contrarrestarlo, Microsoft consiguió que Windows se convierta en el sistema operativo por defecto en las computadoras compradas por las personas y ofreció licencias de dicho sistema operativo en gobiernos, colegios y universidades.

La competencia de Microsoft había decidido invertir en software libre. Pero el término “libre” era asociado por los ejecutivos de las empresas como algo sin valor o muy barato como para ganar dinero con él, por lo cual decidieron llamarlo software “open source”, queriendo dejar por sentado que el objetivo era dejar el código fuente del programa disponible para que la comunidad colabore en la mejora del software, y que sí se podía ganar dinero con él. Y no usarían GPL sino otras licencias más “flexibles”. Algunas de estas licencias, como la FreeBSD, permitía primero utilizar una licencia para liberar el código a la comunidad y, después de recibir los aportes de ésta, utilizar una licencia tradicional para cerrarlo al publicar una versión del software. Las dos primeras “estrellas” del open source fueron el sistema operativo BSD (Berkerley Software Distribution), derivado de Unix, y Netscape, el primer navegador web comercial. Este último, al poco tiempo fue desplazado por Internet Explorer, de Microsoft, que venía por defecto en Windows en todas las PCs. En definitiva, el open source, impulsado, entre otros, por el carismático editor de manuales de programación Tim O’Reilly y por Steve Jobs desde su vuelta a Apple a finales de los noventa, buscaba luchar contra el monopolio de Microsoft y contra el movimiento del software libre.

3.3.2- Web 2.0

La explosión de los blogs a comienzos del siglo XXI, facilitado por la baja de precios de las cámaras digitales, permitió que cada persona en el mundo

fuera capaz de contar su propio relato con testimonios, opiniones, fotos y videos, sin intermediarios ni filtros y con un acceso simple desde la comodidad de su casa. Esta batalla contra intermediarios y grandes medios por escribir la historia obtiene dos aliados. Uno es Wikipedia, un wiki[15] nacido en 2001 con licencia GPL, que consiste en una enciclopedia colaborativa donde sus contenidos resultan de las contribuciones y debates de la comunidad. Ante la consulta de cómo asegurarse de que sus contenidos fueran "verdad", uno de los creadores de Wikipedia sostuvo que la verdad es una interpretación de los hechos, y la interpretación colectiva de una comunidad tiene tanto derecho de existir como la de una institución o un medio monopólico. El otro aliado es WikiLeaks, presentado por Julian Assange en 2007 como "una Wikipedia incensurable para filtración masiva de documentos y análisis", donde las revelaciones exhibidas están respaldadas por documentación oficial.

Al igual que lo hizo con el movimiento del software libre, Tim O'Reilly capitalizó esta explosión de los blogs y generación de contenido por parte de la comunidad creando en 2004 el término "Web 2.0" para referirse al conjunto de sitios web donde se comparte información entre comunidades que contribuyen a la creación de contenidos, como los wikis, las redes sociales y los blogs. O'Reilly sostuvo que las plataformas como YouTube, Facebook y Twitter aprovechan la inteligencia colectiva para generar contenido al gestionar, comprender y responder a la cantidad masiva de datos generados por los usuarios en tiempo real, no solo a través de lo que usuario tipea sino también a través de los múltiples sensores, cámaras y sistemas de localización. De esta forma, O'Reilly sostenía que las empresas que triunfarían en la red serían las que pudieran capturar de esta forma la inteligencia colectiva, sin parecerle un escándalo que se espíe a millones de personas.

[15] Un wiki es un software para la creación de contenido colaborativo, donde distintos colaboradores contribuyen a la creación y edición de artículos en una página web con texto, documentos, imágenes, videos y animaciones sobre un tema y, a su vez, la posibilidad de adjuntar links a otras páginas.

3.4- Fin de la neutralidad y control de los Estados

El concepto de neutralidad de la red fue formulado por el estadounidense Tim Wu en 2003, y al poco tiempo pasó a tener relevancia en la política pública. Sin embargo, décadas antes en Estados Unidos ya se hablaba de que Internet no debería favorecer ninguna aplicación por encima de otra y que todo contenido (concepto de servicio universal) debe moverse igual y a la misma velocidad a través de la red (concepto de transporte común). Este debate surge por el temor que había de que si los operadores de cable, integrados a los ISP, podían añadir el acceso a Internet como un servicio, podrían excluir aplicaciones y servicios de la competencia, limitando los derechos de accesos de los usuarios y la libertad de innovación de la competencia. Poco tiempo después, este temor se hizo realidad ya que se estableció como potestad de los ISP el discriminar o no ciertos servicios y aplicaciones, y además se autorizó a los operadores móviles a discriminar aplicaciones de terceros. [32]

Que se pierda la neutralidad de la red implica que sea más costoso y menos democrático el ingreso a la competencia en el mercado de nuevas aplicaciones y servicios, ya que deben atravesar la barrera que los separa de aquellos aliados comerciales de los ISP.

La neutralidad de la red es un principio que establece que los ISP deben garantizar el acceso de los usuarios a los contenidos que circulan por Internet, sin discriminarlos por su origen o uso. [31]

Este concepto surge a comienzos de la década del 90 (aunque todavía sin el nombre acuñado por Wu), poco después de la caída del muro de Berlín, cuando comenzó a surgir la necesidad de una red confiable y veloz para el intercambio de información para garantizar la competencia y la inversión privada (premisas de la nueva economía que comenzaba en aquella época) y teniendo en cuenta la escasa penetración que tenía Internet en la población mundial de aquel momento [32]. Sin embargo, conforme fue aumentando exponencialmente esta penetración, y por consiguiente aumentando la cantidad de beneficiados por el aumento del mercado basado en Internet, la neutralidad de la red comenzó a verse con malos ojos por los principales gobiernos y empresas. Estos últimos iniciaron las tareas de

recrudecer la legislación contra la neutralidad de la red, apoyándose en factores como la lucha antiterrorista, tras los atentados del 11 de septiembre de 2001, y la avanzada de la Propiedad Intelectual que buscaba criminalizar los intercambios de contenido (música, videos, etc.), principalmente vía el auge de aplicaciones de redes Peer to Peer (P2P), como Ares y Napster.

A partir de esto, comenzaron a observarse cuatro amenazas a la neutralidad de la red a comienzos del siglo XXI: el bloqueo de aplicaciones, la tendencia a la monopolización de los ISP, la priorización de servicios o proveedores según acuerdos comerciales y la falta de transparencia.

Los ISP, por su parte, comenzaron a plantear dos ideas. Una de ellas es el bloqueo de páginas y aplicaciones "peligrosas" o violadoras de derechos de autor (descargas torrents, páginas de movimientos sociales, aplicaciones P2P, etc.). Y la restante es la cancelación de la Tarifa Plana (servicio donde, por un costo fijo mensual, el ISP permite el acceso ilimitado a todos los contenidos de Internet sin discriminación) y el otorgamiento de una conexión "Premium" a través de la cual el ISP cobre un paquete de datos mensuales limitados (por ejemplo 2 GB), como es el actual caso de los servicios de telefonía móvil. O bien, una tarifa base que requiera un pago extra para poder acceder a determinados servicios, como ocurre actualmente con el servicio de cable televisivo. Una variante de este último caso es mantener una tarifa plana pero cobrar un adicional para acceder más rápidamente a determinados contenidos (por ejemplo, Netflix).

A la vez, los ISP expresan que, debido al exponencial aumento de la demanda de servicios de Internet de los usuarios, se genera una congestión de las redes, ocasionando problemas de conexión y de velocidad en horas pico. Es por esto que incitan al Estado a que autorice el cobro diferencial de contenidos para, con ese dinero extra, poder seguir innovando en la infraestructura. Este argumento expresado por los ISP es falaz, ya que no solo los datos se transfieren de manera fragmentada principalmente por múltiples canales en la red (bajo el principio de "mejor esfuerzo"), impidiendo su congestionamiento, sino que también la infraestructura es un nivel de la red totalmente ajeno a los ISP.

Como corolario de este aspecto económico de la neutralidad de la red, se puede concluir que la alteración de dicha neutralidad pone en peligro no solo

la libertad de expresión y la libre circulación de la información, sino también el espíritu originario de Internet, pudiendo ralentizar la innovación de nuevas tecnologías y servicios al pasar a estar estos segmentados en los usuarios que puedan pagar por ellos.

Si bien este enfoque económico-comercial de la neutralidad de la red es necesario de tener en cuenta, es igual o más interesante aún prestar atención a la problemática vinculada a la vigilancia y la manipulación del tráfico.

3.4.1- Vigilancia y manipulación del tráfico

La mencionada posibilidad que tienen los ISP de filtrar y discriminar contenidos, siendo la puerta de entrada y salida de los datos que circulan hacia Internet de los dispositivos digitales de los usuarios, deja en evidencia que estos proveedores tienen acceso tanto a datos como a metadatos. En el caso de los metadatos (como la dirección del origen y el destino del paquete o su fecha y hora, el navegador web o la aplicación utilizada -por ejemplo, Twitter, Facebook, Spotify, Gmail, etc.-) es lo más sencillo de comprobar que tienen acceso, ya que es a partir de ellos que realizan filtros de contenido o que potencian o prohíben accesos. El acceso a los datos no resulta tan sencillo, a excepción de aquellos datos que se envían al interactuar con sitios web no seguros, es decir, sitios web sin HTTPS. Para los demás casos, si bien pasan por ellos los paquetes, los mismos están encriptados y se requeriría, por ejemplo, utilizar algún software de desencripción.

Esto le permite a los ISP almacenar estos datos y metadatos e incluso crear un historial de cada usuario sobre su comportamiento en Internet, el cual puede ser solicitado por el Estado, por empresas o cualquier otro interesado en obtenerlo.

El único que tiene la facultad de regular este comportamiento de los ISP es el Estado, quien podría ser cómplice de los ISP ya sea por acción, al reglamentar la obligatoriedad de este almacenamiento, o por omisión, al no tener ninguna normativa al respecto y dar vía libre al ISP de accionar con los datos y metadatos del cliente.

Los ISP no son los únicos actores en este aspecto de vigilancia. También los servidores, que soportan los sitios web con los que interactúan los usuarios, reciben tanto metadatos como datos en los paquetes que reciben de ellos.

Por lo tanto, los dueños de estos servidores (por ejemplo, Facebook, Google, Amazon, etc.) pueden también almacenarlos y luego utilizarlos o venderlos, según sea su intención. Cabe destacar que esta violación a la privacidad se hace con el consentimiento del usuario, que "acepta" los términos y condiciones de uso del servicio.

Por último, a partir de documentos filtrados, por ejemplo, por WikiLeaks y Snowden, quedó demostrado cómo las agencias de inteligencia (como la NSA y el GCHQ) recolectan tanto datos como metadatos a partir de reclamos a compañías de Internet, como Google, Facebook, Microsoft, etc., a ISPs, o bien obteniéndola desde las empresas que controlan los cables submarinos o con ataques informáticos.

También es importante hacer una mención a las empresas de telefonía móvil, quienes también atentan contra la neutralidad de la red al brindar servicios de paquetes de datos limitados (4 GB, por ejemplo), al ofrecer una conexión ilimitada y veloz a las redes sociales por un monto diario (imposibilitando acceder por medio de este pago a otros servicios o aplicaciones) y al tener que vincular los smartphones a una cuenta de email para que su sistema operativo funcione (como Gmail para Android, Icoud para Apple y Hotmail para Windows Phone). A su vez, cada aplicación que el usuario desee ejecutar desde su celular requiere de determinados permisos de acceso (por ejemplo, a la cámara, contactos, GPS, etc.), violando la privacidad del sujeto e impidiendo su funcionamiento en caso de no aceptar estas condiciones.

Por último, están las redes sociales, que tienen una lógica distinta, ya que obtienen los datos y metadatos de los usuarios de forma legal y con la voluntad de los usuarios, que son quienes suben contenido a ellas. Más allá de que las empresas que son propietarias de dichas redes sociales pueden violar la privacidad de sus usuarios al manipular estos datos y metadatos almacenados (como se mencionó anteriormente), algunas de ellas también implementan proyectos que atentan contra la neutralidad de la red, como se analizará a continuación.

3.4.2- Proyectos de Internet “abierto”

El ejemplo de alcance más masivo es el proyecto Free Basics (antes internet.org) que Facebook, en alianza con compañías de telefonía móvil,

creó en 2014 con una máscara humanitaria: permitir acceso a Internet a millones de ciudadanos sin recursos. Se trata de una aplicación que permite un acceso gratuito y de alta velocidad a determinados sitios web (como Facebook y Wikipedia) y para poder acceder al resto de los sitios se requiere un pago adicional. No solo discrimina los flujos de datos, sino que también solo aquellos usuarios que acepten voluntariamente este funcionamiento pueden utilizarla, y a su vez, por supuesto, obtiene los datos y metadatos proporcionados por el usuario durante su navegación (apropiándose de una enorme base de datos de una muy significativa cantidad de pobres en el mundo).

La decisión de qué sitios web están accesibles desde Free Basics la toman Facebook y el operador de telecomunicaciones del país donde sea instalado, con supervisión del gobierno de dicho país [34]. De esta forma, se asemeja a lo que sucede, por ejemplo, en Corea del Norte, donde los ciudadanos solo tienen acceso a una intranet local de apenas unos treinta sitios web con contenidos fiscalizados por el gobierno. Más adelante, se tratará la censura de algunos países en el acceso a la red.

Otro ejemplo es el del plan Airtel Zero, lanzado por la operadora Airtel en 2015, mediante el cual sus usuarios no consumían datos de sus tarifas por usar determinadas aplicaciones con las que se habían firmado acuerdos. [35]

El mismo trato desigual ocurre cuando operadoras de telefonía móvil ofrecen planes que incluyen el uso gratis de aplicaciones como WhatsApp o Facebook, concentrando la actividad de los usuarios en estas aplicaciones.

Lo que también es muy preocupante es que varios Estados hayan aceptado aplicar estas iniciativas bajo una consigna de "inclusión digital".

3.4.3- Control del tráfico por parte de los Estados

Los Estados, además de poder ser víctimas de las vigilancias de agencias de inteligencia extranjeras (como las mencionadas con anterioridad) ya que acceden a Internet al igual que los civiles, suelen reglamentar medidas obligando a que los ISP o servidores de empresas de servicios de Internet almacenen datos y metadatos y para poder ellos mismos accederlos cuando lo requieran. Esto representa no solo una violación a la privacidad de los

usuarios, sino que también es una forma de control social y disciplinamiento. [32]

Esta monitorización constante por parte de los Estados de la actividad de los usuarios es posible bajo el paraguas que representa la defensa de la propiedad intelectual, lo cual impulsa la lucha contra la neutralidad de la red. Y para lograrlo cuentan con el apoyo de grandes corporaciones que, como se mencionó anteriormente, ven a Internet como una gran amenaza para ellos, de forma tal que tanto los Estados como estas corporaciones se ven beneficiadas.

Un ejemplo de Latinoamérica es el Marco Civil de Internet de Brasil aprobado en 2014, en el cual sus artículos 13 y 15 establecen la obligación a los ISP y a los proveedores de aplicación (Google, Facebook, etc.) de almacenar metadatos, teniendo el Estado la potestad de solicitar acceso a los mismos [36]. Además, su artículo 19 establece que los ISP están obligados a otorgar al Estado los datos, en caso de que se soliciten vía orden judicial.

Algunos Estados controlan el uso de Internet monitoreando directamente el tráfico, ya sea interviniendo los Servidores Raíz de Nombre de Dominio o los nodos que interconectan los puntos críticos del tráfico en la red. [32]

Otros países optan por acudir a los "guardianes" de la red, como lo son los ISP y los prestadores de servicios online (como las redes sociales, servidores de correo electrónico y servicios en la nube), los cuales cooperan de forma voluntaria, obligatoria o a partir de ofertas o acuerdos con los Estados.

Una de las técnicas para lograr el control del tráfico es la Inspección Profunda de Paquetes, utilizada para monitorear el tráfico mientras pasa por algún punto de la red. Cuanto más cerca de la capa de aplicación se inspeccione el paquete, más se podrá saber acerca de ese paquete. Corresponde al nivel de inspección más alto (acceso total al paquete). Está por encima de la Inspección Superficial de Paquetes, que incluye los firewalls, que solo pueden filtrar por el encabezado de un paquete (que incluye, por ejemplo, dirección origen y destino) y no sobre la carga útil (contenido del paquete), y sobre la Inspección Media de Paquetes, que hace referencia a la utilización de proxies, que consisten en entidades (usadas en

organismos públicos y empresas privadas) por las que pasan todo el tráfico y, en base a reglas preconfiguradas, deciden cómo actuar sobre cada paquete (pudiendo acceder parcialmente a contenidos de la carga útil).

La Inspección Profunda de Paquetes le permite a un ISP discriminar el tráfico de sus usuarios. Así, por ejemplo, puede detectar aquellos usuarios que están descargando archivos de gran tamaño y luego limitar esta descarga en horas pico y normalizarla en horas de menos tráfico, para evitar congestiones de red. Sin embargo, el hecho de la capacidad de acceso al contenido de los paquetes implica que quien emplea la Inspección Profunda de Paquetes puede acceder a contenido sensible o de carácter privado del usuario, incluso hasta siendo promovido por los gobiernos.

Los usuarios utilizan todos los días los servicios que ofrecen los ISP (para la conexión a Internet) y los prestadores de servicios online, ambos conocidos como intermediarios de Internet, quienes pueden moldear las actividades de sus usuarios. Los Estados han ido diseñando e implementando fórmulas para que los intermediarios controlen la actividad online de sus usuarios con el objetivo de prevenir hechos indeseados o delitos. Esta estrategia de influir en los individuos a través de terceros, en vez de hacerlo de forma directa, se conoce como teoría del intermediario, amas de llave o guardianes, y es muy útil para el Estado, ya que existen muchas situaciones donde al Estado le resulta muy difícil o muy riesgoso hacer el control por su propia cuenta.

Sin embargo, al guardián no le afecta la posible conducta irregular de un cliente. Por ejemplo, a un ISP poco le puede importar que uno de sus usuarios descargue música ilegal. Por lo tanto, los Estados suelen hacer responsables legales a los guardianes por la conducta de sus usuarios, creando mecanismos y obligaciones que le permitan al guardián detectar una acción irregular de sus usuarios y así poder prevenirla o minimizar el impacto de la misma.

3.4.4- Censura

Uno de los propósitos de los Estados es controlar el contenido en línea con el que interactúan los usuarios. Quizás, el caso más extremo, y a su vez el más célebre, es el del gran firewall de China, que proporciona un gran filtro y bloqueo de contenidos en Internet.

El gran firewall de China consiste en un sistema de censura del contenido online, donde los ciudadanos solo pueden leer y escribir lo que el gobierno chino considere correcto. La censura de Internet en el gigante asiático comenzó a principios de la década del 2000, y se profundizó con la llegada al gobierno de Xi Jinping. [37]

Este firewall no permite la utilización de servicios como los que ofrecen Google o Facebook (por consiguiente, tampoco WhatsApp ni Instagram). A cambio de esto, el mercado chino ofrece servicios equivalentes, como Baidú, Sohu, WeChat y Sina Weibo, cuyos servidores almacenan los datos dentro del territorio nacional y tienen cientos de millones de usuarios. [38]

Una excepción es Apple, que tiene a China como uno de sus principales mercados y ha colaborado con la censura en ese país eliminando, a pedido del gobierno chino, algunas aplicaciones de su App Store, como hizo en 2019 con la del servicio de noticias Quartz, que ofrecía una amplia cobertura de los disturbios en Hong Kong. [39]

Para poder volver al mercado chino, del cual salió en 2010, Google creó el proyecto “Dragonfly”, que consistía en un buscador que se adaptara a la censura que solicitaba aplicar el gobierno chino [40]. El proyecto, que se mantenía en secreto, fue develado por The Intercept [41], que reveló que el proyecto estuvo en marcha desde 2017. Finalmente, en noviembre de 2018, otro artículo de The Intercept [42] señaló que Google cerró el proyecto Dragonfly.

Por otra parte, cuando crece alguna aplicación china y se vuelve popular, entra en el radar del gobierno y es obligada a adherirse al sistema de censura. Si la aplicación se convierte en un gigante, el gobierno envía ejecutivos a la compañía para supervisar in situ la aplicación de la censura.

Los controles sobre la red en China hacen prácticamente imposible encontrar comentarios críticos hacia el Partido Comunista e información sobre ciertos acontecimientos, como la masacre de 1989 de la Plaza de Tiananmén. [43]

Dentro del material censurado por el gran firewall de China también se encuentran aquellos que muestren abuso de alcohol o apuestas, los que promuevan el sensacionalismo de crímenes, los que involucren cualquier actividad sexual o “valores maritales malsanos” (por ejemplo, amantes o

intercambios de pareja), y aquel material que ridiculice a dirigentes históricos o actuales del régimen. [44]

Hay quienes logran saltear el firewall utilizando una red VPN (Red Privada Virtual), pero son muy pocos debido a la gran dificultad de obtener una estando dentro de China y a la restricción de su uso por parte del gobierno.

Si bien China puede ser el más emblemático, no es el único caso. Diversos informes, como el de Jack Turner [45], sostienen que Eritrea, Turkmenistán, Corea del Norte, China, Arabia Saudita, Vietnam, Irán, Cuba, Sudán, Egipto, Turquía, EAU y Rusia están entre los países que más censura poseen en la red.

En Vietnam es ilegal publicar información que afecte negativamente al gobierno y, por ley, es obligatorio controlar la actividad de los usuarios de redes públicas como las de los cibercafés.

En Egipto, hay muchos sitios web bloqueados por el gobierno y cualquier persona que visite un sitio web considerado como prohibido puede ser encarcelado hasta por un año.

En el caso de Cuba, la navegación de un usuario en la red puede ser interrumpida si se la considera en contra del comportamiento ético promovido por el Estado cubano.

El gobierno de Irán encarcela a periodistas, bloquea sitios web y mantiene un clima de miedo con hostigamiento y vigilancia (inclusive hacia las familias de los periodistas).

En Arabia Saudita, las autoridades dan rienda suelta para encarcelar a periodistas y blogueros que se desvían de la narrativa favorable al gobierno, y también utilizan tecnología de vigilancia y ejércitos de trolls y bots para en la discusión de temas delicados, como la guerra en Yemen.

En Rusia, en noviembre de 2019, entró en vigencia la Ley de Internet soberana, aprobada en abril de ese año, creada para garantizar la disponibilidad de los servicios de la red ante algún fallo global o una desconexión deliberada [46]. Se trata de una red doméstica (con infraestructura controlada por el Estado ruso), conocida como RuNet, que permitiría que Internet continúe funcionando aún sin la existencia de servidores extranjeros.

Esta ley rusa obliga a los ISP a instalar equipos especiales que le permitirán al centro de control y monitoreo del Roskomnadzor (Servicio Federal ruso para la Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación) llevar a cabo una Inspección Profunda de Paquetes y, según algunos analistas, también le permitirían bloquear de forma independiente y extrajudicial el acceso a cualquier contenido que el gobierno considera una amenaza.

Autoridades rusas sostienen que la ley no conlleva ninguna amenaza de aislamiento del país y que no se trata de un gran firewall como en el caso de China.

Otros casos, como en Alemania, Francia y Brasil, el control de contenidos se realiza para prevenir la difusión de contenidos ofensivos [32]. Los objetivos para el monitoreo del tráfico en Internet dependen de las prioridades de cada país (ya que la red se regula dentro de las fronteras de cada Estado). Así, por ejemplo, algunos países de Medio Oriente consideran inaceptable que se difunda pornografía, otros, como Estados Unidos, dicen que priorizan la lucha contra el terrorismo, y otros tantos, como Alemania, buscan prevenir que se utilicen términos o imágenes vinculadas a un pasado doloroso. Más allá del objetivo del control de contenidos, no debe perderse de vista que este espionaje sobre contenidos afecta derechos fundamentales como la libertad de expresión y la privacidad.

4- Ámbito legal de la vigilancia y de la neutralidad de la red

4.1- Aspectos legales de la vigilancia masiva

Dentro del marco legal del espionaje se destaca la Ley Patriota (Patriot Act), aprobada luego de los atentados del 11 de septiembre de 2001, que es la que cubre legalmente las actividades de vigilancia de la NSA, atentando contra los derechos humanos y las libertades civiles. [10]

Ignacio Ramonet comenta que luego de aprobada la Patriot Act, fueron abusivamente arrestados y encarcelados sin juicio previo cientos de extranjeros. Además, las autoridades manifestaron su intención de someter a interrogatorio a unos cinco mil hombres con visado de turista por el simple hecho de ser originarios de Oriente Próximo. [2]

Complementariamente, el Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos de América (FISC), bajo la Ley de Vigilancia de la Inteligencia Extranjera (FISA), es quien supervisa las solicitudes de espionaje de las agencias norteamericanas contra los sospechosos que habitan suelo norteamericano en audiencias cerradas al público. En junio de 2013 se filtró una orden del FISC, emitida ese mismo año, en la cual se exigía a la empresa de telecomunicaciones Verizon a entregar todos los registros de llamadas de sus sistemas a la NSA, incluyendo los de ciudadanos estadounidenses.

El 2 de junio de 2015, se aprueba en Estados Unidos la ley USA Freedom Act, remodelando la Patriot Act. La misma retira a la NSA la capacidad de almacenar los datos sobre las llamadas telefónicas de millones de estadounidenses y coloca estos datos en manos de las compañías telefónicas, a los cuales las agencias de inteligencia solo podrán acceder con autorización judicial. Sin embargo, cabe destacar que esta nueva ley aplica solo para ciudadanos estadounidenses, por lo que la situación legislativa para el resto de las personas en el mundo siguió siendo igual.

Si uno de los países miembros de la alianza de los Cinco Ojos no dispone de una orden judicial para vigilar a sus propios ciudadanos, serían sancionados por las normas legales. Sin embargo, este requisito no es necesario cuando se trata de ciudadanos extranjeros. Así, por ejemplo, si la NSA no tiene

permiso para interceptar las comunicaciones de la ciudadanía norteamericana, de ella se podría encargar el GCHQ británico, quien luego compartirá todos esos datos con su homólogo americano.

En Europa se destaca el Convenio Europeo de Derechos Humanos (CEDH), basado en la Declaración Universal de los Derechos Humanos y adoptado por el Consejo de Europa en 1950, el cual indica que todos los ciudadanos europeos tienen derecho a ser protegidos ante intrusiones arbitrarias o ilegales en su vida privada por parte de autoridades estatales, personas físicas o jurídicas.

En diciembre de 2013 la Organización de las Naciones Unidas (ONU) aprueba la resolución 68/167 ("El derecho a la privacidad en la era digital") para la protección en Internet de los derechos humanos, señalando que para esto los Estados deben examinar sus prácticas de vigilancia y recopilación de datos.

Además, el Informe Moraes, presentado por el LIBE al Parlamento Europeo en febrero de 2019, recomienda prohibir las actividades de vigilancia masiva, solicitando a los Estados que regulen sus actividades de inteligencia ajustándose al CEDH.

En abril de 2014, el Tribunal de Justicia de la Unión Europea anula la Directiva 2006/24/CE que obligaba a los proveedores a conservar datos de los usuarios de servicios de comunicaciones electrónicas en todo el territorio de la Unión Europea. En octubre de 2015, el mismo tribunal revoca el acuerdo de Puerto Seguro (Safe Harbor)[16], que permitía a compañías transferir datos desde Europa a Estados Unidos, al considerar que no se ofrecía una adecuada protección de los datos personales a los ciudadanos de la Unión Europea (para más detalles sobre esta revocación ver Anexos).

En junio de 2016, la UE y Estados Unidos firman el acuerdo Privacy Shield, el cual sustituye al revocado acuerdo de Safe Harbor. Este nuevo acuerdo para la protección de datos personales de ciudadanos europeos que sean transferidos a suelo estadounidense aspira a proteger dichos datos y proporcionar seguridad jurídica para las empresas, así como recuperar la

[16] Safe Harbor fue creado en el año 2000 debido a que millones de europeos empezaron a usar servicios en Internet que almacenaban información de los usuarios en bases de datos en Estados Unidos.

confianza de los consumidores en el contexto de las transferencias de datos transatlánticas.

El 27 de abril de 2016 se crea el Reglamento 2016/679, Reglamento General de Protección de Datos de la Unión Europea (RGPD o GDPR), a partir del cual se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). El objetivo del nuevo reglamento es dar más control sobre la información privada de los ciudadanos europeos en un mundo de teléfonos inteligentes, redes sociales, y homebanking.

En marzo de 2017 el Parlamento Europeo dicta la Resolución 2016/2225 [47], la cual hace referencia al big data (bajo el concepto de macrodato) e insta a que, quienes lo empleen, utilicen herramientas que permitan que los datos personales de ciudadanos que lo alimentan estén salvaguardados, para garantizar su anonimización y para asegurar que, a partir de una correlación con otros datos, no sea posible reidentificar a las personas (es decir que no se pierda la anonimización). A su vez, recomienda prohibir a los proveedores la instalación de puertas traseras en software y sugiere prestar atención a la seguridad en los softwares que se conviertan en fuentes de big data, como los de los dispositivos del Internet de las Cosas (IoT).

En una entrevista con Marta Peirano en 2019 [48], Edward Snowden asegura que países como Alemania, con la Intelligence Service Act (2016), Reino Unido, con la Investigatory Powers Act (2016) y Australia, con la The Assistance and Access Act (2018), han legalizado la vigilancia. De esta forma, afirma que “[…] la respuesta a los escándalos sobre vigilancia no ha sido hacer que los servicios de inteligencia se ajusten a la ley, sino hacer que la ley se ajuste a los servicios de inteligencia”. Por otra parte, sostiene que la cuarta enmienda en Estados Unidos limita las capacidades del gobierno y del Estado, pero no de las empresas privadas, sabiendo que gran parte de los datos de inteligencia del Estado provienen de estas compañías.

En otra entrevista, el mismo Snowden ha manifestado que la ley de vigilancia británica Investigatory Powers Act, aprobada en 2016 por el Parlamento británico, legaliza “la vigilancia más extrema de la historia de la democracia occidental”. Según esta ley, las compañías de telecomunicaciones deberán registrar información sobre las actividades de sus clientes (en todos los dispositivos, desde computadoras personales

hasta smartphones) durante al menos un año, para que los servicios de inteligencia puedan examinarla cuando lo requieran. [49]

Por otra parte, Ramonet menciona que en 2015 en Francia se aprobó la ley Renseignement, la cual, yendo en contra de la posición de la Unión Europea de no espiar masivamente a personas sin indicios de que sean sospechosas, permite llevar a cabo una vigilancia masiva sin requerir autorización judicial: solo hace falta la decisión del Primer Ministro. Esta ley ha sido muy cuestionada por su violación al derecho de vida privada y familiar, por no garantizar el secreto profesional de abogados, por la no protección de las fuentes periodísticas, por su ausencia de transparencia y por los métodos intrusivos de vigilancia. [2]

A su vez, Francia cuenta con un sistema para obtener y almacenar masivamente datos personales, llamado PNCD (Plateforme Nationale de Criptanalyse et de Décryptement), alojado en la agencia de inteligencia francesa, la DGSE. Este sistema contribuye al objetivo de la ley Renseignement y permite almacenar las comunicaciones en todo el mundo durante los últimos cinco años, de forma tal que si una persona se vuelve sospechosa se pueda reconstruir su red de relaciones. Por último, comparte la información que recopila con sus homólogos NSA y GCHQ.

4.2- Aspectos legales de la neutralidad de la red

En 2011, en Estados Unidos se lanzaron dos proyectos de ley para censurar aquellos sitios web con contenidos que violaban derechos de autor, conocidas como ley SOPA (Ley de Cese de la Piratería Online, por sus siglas en inglés) y PIPA (Ley de Protección de Direcciones IP, por sus siglas en inglés). Estos proyectos buscaban que los servidores DNS, que resuelven las URLs tipeadas por los usuarios en los navegadores (por ejemplo, google.com) a su dirección IP (la cual permite el acceso al servidor que hospeda a dicho sitio web), no funcionen para aquellos sitios web que albergan contenidos violatorios de derechos de autor. Esto impediría a los usuarios a acceder a estos sitios, y además impedirían a los buscadores indexarlos en sus búsquedas y a las compañías de publicidad o de pagos online hacer negocios con ellos. Estos proyectos han tenido un rechazo muy

importante, tanto por organizaciones civiles y activistas, como Aaron Swartz, como por intermediarios de Internet, como Google y Wikipedia, y otras tantas páginas que cerraron temporalmente en señal de protesta. Esto llevó a que varios congresistas estadounidenses se opongan a estos proyectos, los cuales no llegaron a ser aprobados. [32]

En diciembre de 2017, la administración de Donald Trump, a través de la Comisión Federal de Comunicaciones de Estados Unidos (FCC, por sus siglas en inglés), derogó las normas de neutralidad de la red creadas por la administración de Obama [50]. Estas normas impedían a los ISP manipular el tráfico de Internet (bloquear contenidos, ralentizar servicios, favorecer cierto tráfico de aplicaciones a cambio de una contraprestación). Con esta abolición, ahora los ISP solo tienen la obligación de trasparentar cómo gestionan la red. A pesar de esto, los Estados pueden aprobar sus propias reglas que promuevan la defensa de la neutralidad de la red dentro de sus límites.

A diferencia de Estados Unidos, en Europa entraron en vigencia en el año 2016 las primeras normas para proteger la neutralidad de la red [51], donde el Organismo de Reguladores Europeos de Comunicaciones Electrónicas (BEREC) presentó una serie de reglas para que los reguladores de cada país de la Unión Europea las adopten formalmente e indiquen las penalizaciones por no cumplirlas. Señala como únicas excepciones la existencia de órdenes judiciales, la congestión en la red o el combate de ataques cibernéticos, en cuyos casos el control del tráfico debe ser transparente, no pudiendo demorarse más que el tiempo necesario para solucionar el inconveniente. Sin embargo, un estudio en enero de 2019 de la organización Epicenter demuestra que 17 de los 31 países examinados no han definido las penalizaciones por incumplimiento [52].

Holanda fue el primero de los países europeos en incorporar leyes de neutralidad de la red en diciembre de 2012. En el caso de América Latina, en 2010 Chile fue el primer país a nivel mundial es establecer una ley a favor de la neutralidad de la red. En 2014, en Argentina se sancionó una ley al respecto que prohíbe a los ISP "bloquear, interferir, discriminar, entorpecer, degradar o restringir la utilización, envío, recepción, ofrecimiento o acceso a cualquier contenido, aplicación, servicio o protocolo salvo orden judicial o

expresa solicitud del usuario" [53]. En 2014, en Brasil aprobó el Marco Civil de Internet, que protege algunos aspectos de la neutralidad de la red.

Más allá de estos intentos de regulación, Eduardo Bertoni menciona:

> *"Aun en los países con regulación en la materia, las prácticas de los proveedores indican que es poco o nada lo que el Estado hace para evitar que se viole la neutralidad de la red. Esto puede deberse a muchas causas: el regulador no tiene fortaleza para intervenir o no cuenta con la capacidad para documentar las irregularidades; el proveedor del servicio no tiene incentivos suficientes para cumplir, o el usuario en general no exige un servicio en términos acordes con la neutralidad".* [32]

5- El negocio de los datos personales

5.1- Fuentes de datos personales

Tal como menciona el coronel y experto estratega español Pedro Baños, los teléfonos móviles “[…] son nuestra ventana al mundo, pero también son la ventana del mundo hacia nosotros” [38]. Distintas aplicaciones, preinstaladas o descargadas por el usuario, por más inofensivas para aparenten ser, requieren permisos de acceso, por ejemplo, al GPS para saber la localización actual del usuario en todo momento. Una vez recolectada, esta información de los usuarios pasa a estar disponible para las empresas a las que pertenecen estas aplicaciones. Incluso, admitido por Google, estando desactivado el GPS, los dispositivos basados en Android permiten recoger la ubicación del usuario a partir de la triangulación de señales de las antenas de telefonía a las que se conectan los usuarios.

Por otra parte, las GAFAM acumulan una colosal cantidad de información sobre sus usuarios, sus perfiles, mensajes y patrones de conducta. A su vez, los asistentes de voz de estas compañías (Home y Assistance de Google, Siri de Apple, Echo y Alexa de Amazon, Cortana de Microsoft) escuchan todo el tiempo las conversaciones de sus usuarios, por más que éstos no les estén hablando, registrando los contenidos de estos diálogos.

En diciembre de 2018 una investigación de The New York Times [54] reveló que durante los últimos años Facebook le dio a más de 150 empresas, dentro de ellas algunos gigantes tecnológicos como Amazon, Microsoft, Yahoo, Spotify y Netflix, más acceso del que se sabía a información personal de sus usuarios (el producto más preciado de la era digital), sin su consentimiento.

Se trató de una serie de acuerdos, algunos que datan desde 2010, donde se establecían intercambios que beneficiaba a todos. Facebook incrementó su cantidad de usuarios e ingresos publicitarios, mientras que las otras empresas mencionadas pudieron mejorar sus servicios.

Con este acuerdo, Microsoft logró que su motor de búsqueda, Bing, tuviera acceso a prácticamente todos los amigos de cada usuario de Facebook, y tanto Netflix como Spotify pudieron leer los mensajes privados de los usuarios de la red social. Por otra parte, Facebook permitió que Amazon

obtuviera los nombres y la información de contactos de los usuarios a través de sus amigos, y Yahoo! pudo, hasta mediados de 2018, ver las publicaciones de amigos de los usuarios.

Tal como comenta Eva Mejías Alonso, existen distintas fuentes de las cuales pueden proceder los datos de las personas, las cuales se destacan a continuación. [10]

Generados por las personas: correos electrónicos, mensajes por WhatsApp, estado y likes en Facebook, tweets, consultas en Google. Son cosas que se hacen a diario y que crean nuevos datos y metadatos que pueden ser analizados.

Transacciones de datos: facturaciones, llamadas, transacciones bancarias. Pueden convertirse en datos relevantes, como una acción llevada a cabo en una fecha y un momento determinado, en un lugar concreto y entre unos ciertos usuarios registrados.

E-marketing y web: interacciones con cualquier sitio web, como los movimientos de ratón (que se quedan grabados en mapas de calor) o los registros de cuánto tiempo se pasa en cada página web y cuándo y por qué se la visita.

Biométrica: datos generados por lectores biométricos como escáneres de retina, huellas digitales o patrones de voz. El propósito de estos datos es proporcionar mecanismos de seguridad para el acceso a dispositivos, como, por ejemplo, a smartphones. Sin embargo, estos datos pueden ser registrados por el dispositivo.

Además, tal como lo explica un artículo del portal web Infobae [55], los dispositivos de IoT (Internet de las Cosas, por sus siglas en inglés), que mucha gente incorporó a sus hogares, como cámaras de monitoreo y electrodomésticos inteligentes, suelen ser fabricados sobre una arquitectura de seguridad con pocos recaudos, conteniendo vulnerabilidades en su firmware[17] o en los protocolos de comunicación que implementan. Si alguien aprovechara estas vulnerabilidades podría tener acceso a datos desde el interior de un hogar.

[17] El firmware es un conjunto de instrucciones grabadas en una memoria no volátil (ROM, flash, etc.) que establecen la lógica que controla los circuitos electrónicos de un dispositivo.

Ya en 2015, durante una charla TED, Marta Peirano explica las formas de vigilancia a la que las personas están expuestas [56]. Indicaba que, desde 2008, la Unión Europea exige a las compañías telefónicas con más de diez mil clientes retener datos de sus clientes un mínimo de seis meses y un máximo de dos años. Esa información (con quién mantiene llamadas y de cuánta duración, con quién se intercambia mensajes y qué mensajes) se puede entrecruzar con otro tipo de información de un usuario en particular. Por ejemplo, el registro de la ubicación actual del usuario a partir de su teléfono celular, los registros de navegación en su computadora personal, las cámaras de vigilancia de los espacios públicos y privados, los radares en las rutas y los distintos chips o tarjetas de identificación, como el DNI, el carnet de conducir, la tarjeta del transporte, las tarjetas de débito y crédito o las tarjetas de descuentos de supermercados. Al pasar estas tarjetas por los distintos lectores, el usuario se identifica y deja una huella de todas las actividades que realiza todos los días (a dónde viaja, qué come, cuánto dinero gana, cuándo se enferma, etc.). Incluso, para hacer un análisis del contexto en el que se desenvuelve un usuario y así elaborar un perfil más completo, se puede analizar a otros usuarios que interactúan con él y que también registran el mismo tipo de información. Estos perfiles se generan de forma automática y existen a pesar de que sean de usuarios que actualmente no revistan importancia para quienes los vigilan. Y, si el día de mañana se convierten en alguien importante, este perfil se transforma en sus antecedentes.

Ignacio Ramonet también remarca que con algoritmos cada vez más perfeccionados y con una innumerable cantidad de dispositivos se registran y analizan la información que las personas generan sobre sí mismas [2]. Satélites, drones, cámaras infrarrojas, cámaras de video, son algunos ejemplos de estos dispositivos. Ramonet, al igual que Peirano, también recalca la importancia de considerar las tarjetas con chips de identificación por radiofrecuencia (RFID), que se utilizan cotidianamente, como las tarjetas de bonificaciones de los grandes supermercados, que describen el perfil de los consumidores a partir de su uso.

A su vez, se ha generado un gran mercado en el que los datos personales se transformaron en una mercancía valiosa con el crecimiento del consumo

en línea. Las cookies[18] de los usuarios van generando un perfil de consumidor a partir de las búsquedas que realizan. Estos perfiles son vendidos a distintos anunciantes que, a partir de ese perfil, le muestran en pantalla a esos usuarios publicidad que supuestamente les es de interés.

5.2- Vigilancia de empresas de tecnología

Marta Peirano detalla cómo las empresas tecnológicas recolectan masivamente información sobre sus clientes [33]. Comenta que tanto la CIA como la NSA contribuyen al financiamiento de la investigación universitaria de ciencias computacionales, para lograr que exista la tecnología necesaria para la vigilancia, como sistemas de reconocimiento de patrones (para identificar personas con comportamiento sospechoso o no deseado) y sistemas de gestión eficiente de bases de datos masivas. Así ocurrió con el buscador Google, lanzado en 1998, cuyos creadores, Serguéi Brin y Larry Page, fueron financiados por el proyecto MDDS (Massive Digital Data Systems Project), liderado por dichas agencias estadounidenses.

La empresa de Brin y Page arrasó al resto de los buscadores. Otro éxito fue su servicio de correo electrónico, Gmail, cuyos términos de uso le permiten almacenar el contenido de los correos, incluso de aquellos borrados. Lo mismo ocurre con Google Drive, su servicio de almacenamiento en la nube, con el cual la empresa dispone eternamente de cada archivo que el usuario haya subido alguna vez. En 2003, Google lanza Adsense, un método que permite al dueño de un sitio web ganar dinero al habilitar banners que se cargan con publicidad, la cual es escogida de acuerdo a los contenidos del sitio web y a los datos del usuario que lo está visitando. Estos datos del usuario se forman con lo que Google sabe sobre el usuario. Y Google cada vez sabe más sobre sus usuarios.

Con Google Chrome, el navegador lanzado en 2008, la empresa de Brin y Page puede registrar los gustos del usuario: temas sobre los que busca, links a los que hace clic, servicios en los que inició sesión, etc. Esta

[18] Una cookie es una porción de información que el programador de un sitio web genera en el equipo (smartphone, computadora, tablet, etc.) de un usuario que accede a dicho sitio, con el propósito de almacenar información sobre la actividad del usuario y sus preferencias, de forma tal que se intente mejorar su experiencia mientras navega en Internet.

información con estadísticas sobre la navegación la generan los servidores web, en los que se alojan los sitios web visitados, y la almacenan en una cookie en el navegador del usuario. Esta cookie queda adherida a cada solicitud posterior que el usuario hace a un servidor web. Las cookies fueron creadas por la empresa de Netscape en 1994, cuando los programadores buscaban que el listado de compras virtuales quede asociado al usuario que las realizó, como si se tratara de un carrito de compras virtual, con la inocente intención de que el portal web cambie su aspecto de acuerdo a las preferencias del usuario. Luego, en 1996, una empresa llamada DoubleClick, dedicada a publicidad y anuncios en Internet, crea unas cookies que permitían registrar información sobre el usuario que navegaba en todas aquellas páginas web en donde DoubleClick tenía banners con publicidad. Google compra DoubleClick en 2007.

En la misma línea, Ramonet sostiene que Google, quien cuenta con más de mil millones de usuarios, dispone de muchas herramientas para espiar el comportamiento de los internautas que utilizan sus servicios. Su motor de búsqueda, Google Search, le permite saber dónde está localizado el usuario, qué busca y en qué momento. Su navegador, Google Chrome, captura y envía a Alphabet (empresa matriz de Google desde 2015) datos sobre la navegación del usuario. La herramienta Google Analytics elabora estadísticas sobre la navegación de los usuarios. Google Plus (la red social de Google que cerró por falta de éxito en abril de 2019) recogía información complementaria de los usuarios. Youtube (servicio de alojamiento de videos adquirido por Google en 2006) registra los videos que consumen sus usuarios. La aplicación Google Maps permite identificar la ubicación actual del usuario y registra todo su itinerario. [2]

Continuando con lo que comenta Peirano, Google cuenta con Android, el sistema operativo más utilizado mundialmente en los smartphones, los cuales poseen cámaras, micrófonos, múltiples sensores y sistemas de geolocalización, todas ellas herramientas muy poderosas para extraer datos de los usuarios. Sobre la geolocalización, Peirano comenta:

> *“Cualquier espía te dirá lo mismo: el dato más valioso sobre una persona no son sus correos personales sino su posición geográfica. Sabiendo dónde está en cada momento de su vida sabremos dónde*

vive, dónde trabaja, cuántas horas duerme, cuándo sale a correr, con quién se relaciona, a dónde viaja, cómo se transporta de un sitio a otro, cuál es su terraza favorita. Frente qué escaparates se para, en qué tienda del mercado compra, si recicla, si se droga, si toma anticonceptivos o si va a la iglesia. Si va a conciertos al aire libre o prefiere los DJ, si come en restaurantes de comida rápida o es más bien gourmet. Sabemos quién le gusta y a quién intenta evitar, con quién come y cena, cuánto tiempo pasa con cada uno y a dónde va después. Sabremos si tiene un amante, si se hace el enfermo, si apuesta, si bebe. Sabremos cosas que la propia persona no sabe, como sus rutinas inconscientes y sus correlaciones sutiles. Un smartphone le cuenta todas esas cosas a las aplicaciones que lleva dentro, una mina de oro sin fondo para la industria de la atención".

Todos los smartphones tienen un servicio de geolocalización, siendo el GPS estadounidense el que está presente en prácticamente todos ellos, aunque muchos países planean competirle con sus propios sistemas, como es el caso del Beidou chino.

Aparte del GPS, hay otras maneras de geolocalizar un teléfono móvil. El bluetooth, cuando está activado, emite señales de radio de corta frecuencia hacia otros dispositivos dando información sobre el terminal. Cuando un teléfono móvil tiene una tarjeta SIM emite señales a las antenas de las operadoras, las cuales pueden calcular la distancia hacia el dispositivo y en base a triangulaciones determinar con cierta precisión su localización, como ya se ha mencionado anteriormente. Otra forma es mediante el uso de los dispositivos StingRay (cuyo uso es ilegal), los cuales se hacen pasar por antenas para rastrear los móviles a su alrededor y suelen ser empleados por la policía en camionetas y helicópteros para determinar quiénes están en un lugar y momento determinado.

StingRay es capaz de reunir datos de miles de celulares en un área determinada e interceptar llamadas sin intervenir el equipo. Un ejemplo de ellos es el Gossamer (ver Imagen 17), un dispositivo parecido a un teléfono que tiene un costo en el mercado negro de países como México, Brasil y Argentina de unos 20.000 dólares. [57]

Imagen 17 - Dispositivo Gossamer
Fuente: https://resources.infosecinstitute.com/cellphone-surveillance-the-secret-arsenal/#gref

El StingRay es solo un ejemplo de sistemas de vigilancia que utilizan receptores IMSI (Identidad Internacional del Abonado Móvil, por sus siglas en ingles), que efectúan un ataque Man in the Middle (MITM)[19] actuando como una torre celular móvil falsa que se encuentra entre el teléfono móvil del objetivo a vigilar y las torres reales del proveedor del servicio. [58]

Los smartphones tienen diversidad de sensores. Uno de ellos es aquel que registra la orientación del teléfono, determinando cuándo se lo utiliza para escribir o navegar y cuándo se lo rota para tomar una foto, jugar o ver un video. El acelerómetro mide la velocidad y el sentido en que el usuario se mueve, con lo cual puede determinar si lo está haciendo a pie o en algún medio de transporte. Otro sensor determina cuándo el usuario apoya su oreja en la parte superior del dispositivo (para una llamada telefónica o para escuchar un audio), para apagar la pantalla en ese momento. Otro sensor mide el grado de exposición a la luz ambiental, el cual permite autoajustar el brillo de la pantalla.

Las cámaras y los micrófonos (los ojos y oídos de los móviles) permiten la obtención de datos personales aún más sensibles. Algunas aplicaciones,

[19] Un ataque Man in the Middle, o ataque de hombre en el medio, es un tipo de ataque informático en el cual un tercero, de forma desautorizada, actúa de intermediario en un intercambio de datos entre otras dos entidades, manipulando los paquetes de datos que entre ellos se envían.

como los asistentes de voz, requieren estar en escucha constantemente. Sobre los asistentes de voz de los gigantes tecnológicos, Peirano comenta:

> *"Además de venir instalados por defecto en los dispositivos de sus respectivas empresas, como los iPhone y los Android y los Echo y los Dots, los gigantes pelean ahora por colonizar con sus algoritmos el resto de consolas, vehículos, televisores, webcams, lámparas, tablets, electrodomésticos y hasta aplicaciones «inteligentes» de otras marcas. El de Google está integrado en videocámaras domésticas de Nest, pantallas de Lenovo, despertadores como iHome, televisores de Philips, altavoces de Onkyo, LG, Klipsch, Braven y JBL y hasta en el asistente de estilo del gigante japonés Uniqlo, que utiliza la tecnología de Mountain View. Alexa viene por defecto en al menos ciento cincuenta productos diferentes, incluyendo estrellas del mercado como la barra-altavoz de Sonos Beam y los microondas de Whirlpool. Naturalmente, Tesla tiene su propio asistente para sus coches. Pronto será imposible comprar tecnologías que no escuchen lo que hacemos en nuestra casa, vehículo, oficina, todo lo que ocurre a su alrededor y envíen toda clase de datos a las mismas cinco compañías, sin que podamos saber para qué los usan ni durante cuánto tiempo ni con quién más".*

Las aplicaciones que tienen permiso de acceso a las cámaras pueden en cualquier momento encenderlas, tomar fotos y videos y enviarlas a servidores para procesarlas más adelante.

Por otra parte, todas las aplicaciones de identificación biométrica (utilizadas para desbloquear los móviles) recogen, analizan y almacenan los datos biométricos de los usuarios. Los algoritmos de reconocimiento facial permiten identificar personas, incluso contra su voluntad, debido a que las características físicas de una persona son prácticamente inalterables a lo largo de su vida. Amazon tiene su algoritmo, Amazon Rekognition, fruto de su relación con las agencias de inteligencia y capaz de identificar a más de cien personas en una sola imagen. También Facebook tiene el suyo, DeepFace, que tiene un porcentaje de acierto prácticamente igual que el del ojo humano.

Tanto Android como iPhone ofrecen sistemas de reconocimiento facial para desbloquear el teléfono, pero, también, cualquier aplicación con permiso para acceder a la cámara puede utilizar software de reconocimiento facial. Los populares filtros de Snapchat e Instagram o la conocida aplicación FaceApp, que permite a un usuario ver cómo sería a una determinada edad, son claros ejemplos. Cada vez que se utilizan estas aplicaciones o se suben fotos a la nube, se contribuye al entrenamiento de estos algoritmos, los cuales actúan contra la privacidad de aquellas personas que no desean ser identificadas por un software.

Estudios han demostrado que la mayoría de las aplicaciones, con conocimiento o no de sus desarrolladores, comparten información con Google o con aplicaciones vinculadas a Amazon, Facebook, Apple o Microsoft.

5.3- Persecución al sospechoso, ausencia de privacidad y control social

Ramonet indica que tanto el terrorismo yihadista como la amenaza de movimientos sociales insurgentes han hecho que las autoridades de varios países, como Estados Unidos, pongan el foco en perfeccionar su tecnología de vigilancia. Como ejemplos están los mencionados drones, escáneres biométricos (de iris, huellas dactilares, voz, rostro, etc.) y cámaras de vigilancia de cada vez más alta definición, que permiten registrar facciones y datos biométricos de las personas. Esta tecnología se desarrolla cada vez más en los espacios urbanos, llegando incluso a adentrarse en los hogares de los ciudadanos, invadiendo su vida privada. Esto último se ha profundizado con los dispositivos IoT, como los televisores inteligentes que graban todo lo que los espectadores consumen a través de él. De esta forma, los fabricantes de estos televisores pueden recopilar esta información sobre los gustos de sus clientes y venderla a empresas publicitarias. [2]

Una de las situaciones más insólitas y perversas de este sistema de vigilancia masiva es que los ciudadanos sean vigilados y al mismo tiempo vigilantes. Existen soplones civiles que voluntariamente aceptan trabajar para los servicios de la policía a cambio de recompensas económicas en

caso de buenos desempeños. Un ejemplo es la operación TIPS (Sistema de Información y Prevención del Terrorismo, por sus siglas en inglés), lanzada en Estados Unidos en 2002 bajo la presidencia de George W. Bush, dirigida a trabajadores con acceso a las casas de la gente, como cerrajeros, carteros, empleados domésticos y jardineros, para que se contactaran con la policía en caso de advertir señales sospechosas.

Otro ejemplo es el del Internet Eyes en el Reino Unido, un servicio presentado como un "juego" en el que los voluntarios deben analizar las imágenes en tiempo real de cámaras de vigilancia colocadas en comercios y calles y detectar posibles infracciones.

El aumento de éxodos migratorios y el incremento de la xenofobia plantea un escenario propicio para que el número de estos confidentes voluntarios no merme.

A este aumento de la vigilancia masiva, una parte de la opinión pública manifiesta estar dispuesta a limitar sus libertades y su privacidad para poder luchar contra el terrorismo y otros crímenes. Incluso, muchas personas gustan de exhibir su vida privada, compartir su intimidad y publicar sus pensamientos y sentimientos, gusto que ha emergido con el apogeo de Internet, y se ha acentuado con la aparición de las webcams y las redes sociales. Con total despreocupación, y a cambio de minutos de fama, desahogo personal o diversión, muchas personas están dispuestas a contarlo todo, mientras por detrás hay máquinas y algoritmos que recogen toda esa información.

El riesgo de falsos positivos aumenta al dejar todo en mano de los algoritmos. Y con ello sube la posibilidad, por ejemplo, de confundir a un ciudadano inocente con un delincuente, ya sea porque el algoritmo determina que sus rasgos faciales o sus comportamientos son similares, o porque haya detectado que ambos estuvieron físicamente en el mismo lugar en el momento en que el delincuente cometió un delito. Como caso extremo, existen drones armados con cámara de reconocimiento facial capaces de disparar contra aquellos que “identifique” como insurgentes o terroristas en lugares como Afganistán. [33]

En el documental Citizenfour [7], Jacob Appelbaum, periodista e investigador de Seguridad Informática, explica cómo se logra la vigilancia:

"Cuando desean ir por alguien, pueden recrear con exactitud los pasos que hizo dicho individuo, por ejemplo, con los registros de una tarjeta de un banco y la tarjeta del metro. Saben lo que compra (por la tarjeta del banco), con quien se comunica (vinculando los datos del individuo con otras personas con planes de viajes similares), donde está físicamente (obteniendo la ubicación del celular del individuo), etc. Esta información se conoce como metadatos agregados, los cuales cuentan una historia sobre nosotros a partir de hechos concretos pero que no es necesariamente cierta, ya que, por ejemplo, si ese individuo estaba en el mismo lugar en que se cometió un delito no significa necesariamente que sea el culpable".

En una entrevista con Marta Peirano [48], Snowden indica que las comunicaciones no reflejan exactamente cómo somos, ya que las personas suelen cambiar de opinión, cometer errores o incluso mentir hasta a aquellas personas más queridas. Pero manifiesta que agencias como la NSA toman decisiones, incluso de bombardear con misiles a sospechosos, en base a los metadatos recopilados de las comunicaciones.

Por otra parte, en el mismo documental antes mencionado, Snowden se refiere a cómo se comportan las personas cuando se sienten vigiladas:

"Al saberse vigiladas, las personas dudan de hacer donativos a causas políticas o de hacer ciertos comentarios en una comunicación […] Incluso, muchas personas tienen cuidado en la forma en que realizan sus consultas en Internet porque saben que se registra, lo cual limita las fronteras de su exploración intelectual".

Es fundamental tener en cuenta que las personas vigiladas alteran su comportamiento ante la expectativa de poder estar siendo observadas en cualquier momento. A propósito de esto, un estudio de la Universidad de Oxford en 2016 [59] afirma que la sola existencia de la vigilancia genera miedo y asfixia a la libertad de expresión.

Enrique Amestoy traza un paralelismo entre el control y vigilancia a los que están sometidos los usuarios con el Panóptico de Bentham [60]. El panóptico era una arquitectura carcelaria ideada por el filósofo utilitarista Jeremy Bentham, que tenía como objetivo que el guardián de una cárcel, ubicado en

una torre central, pudiera observar a todos los prisioneros en cada una de sus celdas sin que ellos pudieran notar que estaban siendo vigilados.

En este mismo sentido, durante una charla TED, Glenn Greenwald remarca que hay decenas de estudios psicológicos que demuestran que cuando las personas se sienten vigiladas su comportamiento se vuelve conformista y complaciente con las expectativas de los mandatos de la ortodoxia social [61]. Dice que esto lo refleja el Panóptico de Bentham, cuyo diseño arquitectónico no permitía a los prisioneros ver el interior del Panóptico para saber en qué momento eran vigilados, por lo cual asumían que se los vigilaba permanentemente, lo que generaba que los prisioneros cumplieran con el comportamiento deseado por los encargados de la prisión. Greenwald también sostiene que la vigilancia masiva actúa como el Panóptico de Bentham moderno, de una forma mucho más sutil y efectiva, y crea una prisión en la mente que hace que las personas que se sienten vigiladas actúen conforme a la ortodoxia social establecida.

Greenwald indica que esta sensación de vigilancia que tienen las personas es la situación que anhela un tirano para ejercer el control social, y que el objetivo principal de dicha vigilancia es detectar a aquellos disidentes que desafían al poder político que la ejerza, el cual considera que quienes no son inofensivos ni sumisos están haciendo “cosas malas”.

Durante la misma charla, Greenwald habla sobre por qué importa la privacidad, cuando hay gente que dice que no tiene miedo a la vigilancia masiva porque no tiene nada que esconder. Greenwald sostiene:

> *“Hay cosas que estamos dispuestos a hacer solo si nadie nos está vigilando […] Todos, no solo los terroristas y criminales, tenemos cosas que esconder. Hay todo tipo de cosas que hacemos o decimos que solo estamos dispuestos a decirle a nuestro médico, nuestro psicólogo, nuestro abogado, nuestra pareja o nuestro mejor amigo porque nos mortificaría si el resto del mundo lo supiera”.*

Sobre este tema, Edward Snowden ha manifestado:

“Argumentar que no te preocupa el derecho a la privacidad porque no tienes nada que esconder es lo mismo que decir que no te preocupa la libertad de expresión porque no tienes nada para decir”[20].

Greenwald afirma que las personas que dicen que la privacidad no es importante toman acciones que van en contra de esa creencia. Por ejemplo, ponen cerradura en las puertas de sus casas o contraseñas en sus cuentas de redes sociales, medidas destinadas a evitar que otras personas accedan a su espacio privado. A su vez, menciona el caso de Mark Zuckerberg, quien en una entrevista en 2010 dijo que la privacidad ya no era una “norma social” y a los pocos años no solo compró una casa en Palo Alto sino que también compró las cuatro casas adyacentes para asegurarse disfrutar de privacidad.

5.4- Sistema de crédito social chino

El jurista norteamericano Richard Posner decía que la privacidad obstaculiza el capitalismo al interrumpir el libre flujo de información y generar ineficiencia bursátil. Tanto los Estados como las grandes corporaciones de Internet, un grupo concentrado de corporaciones, recopilan datos privados de las personas, con herramientas cada vez más intrusivas, como el Internet de las Cosas. Lucas Malaspina sostiene que, teniendo solo que negociar con ese grupo reducido de empresas, los gobernantes de esta época tienen la capacidad de analizar datos a gran escala para controlar a la población [62].

Un ejemplo extremo de esto es el sistema de crédito social chino, con el cual el comportamiento de ciudadanos y personas jurídicas en China es calificado y rankeado por el Estado, independientemente de su voluntad. Algo similar, aunque a mucho mayor escala, que lo que sucede con la aplicación norteamericana Peeple: una app muy polémica, lanzada en marzo de 2016 [63], que permite puntuar a las personas en los planos personal, profesional y sentimental.

Cuando alguien calificaba a una persona en Peeple (etiquetando su nombre) dicha reseña era permanente y no podía ser eliminada, por más que se tratara de un comentario negativo sesgado y no representativo de la realidad

[20] “Saying you don't care about privacy because you have nothing to hide is like saying you don't care about free speech because you have nothing to say”.

[64]. Peeple nunca prosperó y tuvo una pésima calificación tanto de los usuarios como de muchos medios de comunicación.

Para implementar el sistema de crédito social, el gobierno chino precisa de grandes empresas, como Alibaba, el Amazon chino, Didi, el Uber chino, y Baidu, el Google chino, ya que poseen gran cantidad de información sobre los ciudadanos.

Alibaba explica que se tomarán en cuenta una serie de factores, como el historial crediticio (por ejemplo, si el ciudadano abona a tiempo sus facturas de electricidad o teléfono), la capacidad del usuario para cumplir con sus obligaciones contractuales y el comportamiento de su entorno más cercano (una especie de “dime con quién andas y te diré quién eres”).

Ant Financial, una empresa afiliada a Alibaba, es la creadora de la plataforma de pagos digitales Alipay, utilizada por millones de personas, ya que en Asia las tarjetas de crédito nunca llegaron a popularizarse. Al disponer de una gigantesca cantidad de datos de ciudadanos chinos, Ant Financial fue la encargada de crear para el sistema de crédito social chino el Sesame Credit: un sistema que le da a cada usuario registrado una puntuación en base a datos como compras realizadas, atrasos en los pagos o, incluso, quienes son sus amigos. [65]

Para que este sistema pueda funcionar, también se requieren cientos de millones de cámaras con reconocimiento facial que vigilen en tiempo real a la población. A su vez, cada dispositivo que utilizan los ciudadanos poseen sensores, micrófonos, cámaras y software instalado que también forma parte del sistema de vigilancia del gobierno. [33]

Según se dio a conocer en 2018, más de 30 agencias militares y del gobierno chino desplegaron en al menos cinco provincias unos drones en forma de paloma (llamados Dove, “paloma” en inglés), los cuales, imitando el 90% de los movimientos de esta ave (incluyendo el aleteo), disponen de una cámara de alta definición, antena GPS, sistema de control de vuelo y conexión de datos con capacidad de conexión a satélite [38]. Ese mismo año, la policía china comenzó a utilizar gafas de reconocimiento facial, las cuales están conectadas a bases de datos policiales para acelerar el reconocimiento de vehículos y personas sospechosas [66].

El sistema de crédito social chino surge del documento “Esquema de planificación para la construcción de un sistema de crédito social”, publicado por el gobierno del país asiático en 2014. A partir de ese momento, los ciudadanos chinos se han ido inscribiendo libremente en él, algunos presumiendo sus buenos resultados en sus redes sociales. [67]

El objetivo del sistema es valorar la confianza que otorga cada ciudadano en base a su comportamiento. Cada comportamiento será evaluado como positivo o negativo, en un valor determinado. A su vez, el sistema ofrece consejos y recomendaciones para mejorar la puntuación y aconseja a los ciudadanos a no ser amigos de gente con puntuación baja.

El lema del sistema de crédito social chino es algo así como: “Los buenos ciudadanos caminarán libres bajo el sol y a los malos ciudadanos se les dificultará dar pasos”. Todos los ciudadanos chinos van a sumar o restar puntos de acuerdo a cómo se portan [33]. Cada persona que estacione mal su auto, pase un semáforo en rojo, critique al gobierno en una conversación, se atrase en el pago de facturas, robe o realice alguna otra acción u omisión mal vista por los gobernantes podría perder su seguro médico, perder su empleo, no poder tomar un avión o no poder acceder a determinados servicios o promociones. También hay acciones que suman puntos, como donar sangre, hacer donaciones a beneficencia, obtener buenas calificaciones, hacer horas extras en el trabajo o participar en actividades organizadas por el gobierno.

En concreto, se valoran 5 áreas: crédito económico, capacidad de cumplir con obligaciones, información personal, comportamientos y preferencias, y relaciones personales. [67]

Dentro de los posibles beneficios por obtener un puntaje alto están poder pedir un crédito online, conseguir check-in VIP en el aeropuerto de Pekín o poder solicitar un viaje sin documentos justificativos.

Como consecuencias por obtener un puntaje bajo, un ciudadano puede ver reducida su velocidad de Internet, tener acceso restringido a locales de ocio, perder la posibilidad de viajar libremente al extranjero o quedar excluido de la posibilidad de conseguir algunos empleos.

El mal comportamiento de un ciudadano chino podría llevar a que una imagen suya se exhiba en pantallas de su ciudad, para mostrarle al resto de la población que “se ha portado mal”. [65]

Otro punto crítico sobre el Sesame Credit es que es una especie de red social, por lo que el puntaje que el usuario tiene es visible para todo el mundo. [68]

El gigante chino Tencent también está experimentando con sistemas de crédito social. Su aplicación de mensajería WeChat, que posee un servicio de reconocimiento facial (permitiendo vincular a cada individuo con la aplicación), está en los planes del gobierno chino para que se convierta en una forma de identificación oficial.

5.5- El negocio de la nube

De las GAFAM, Amazon ha sido el más discreto y el que más alejado de polémicas está [33]. Sin embargo, en sus servidores está almacenado aproximadamente un tercio de los contenidos de Internet. Además de almacenamiento, AWS vende servicios de software e infraestructura, y tiene entre sus clientes a Netflix, Unilever, Uber, Tesla, Airbnb, Pinterest, la NASA y el servicio de mensajería recomendado por Snowden, Signal. Su único competidor es Alibaba, que domina el continente asiático, ya que Microsoft Azure, Google Cloud e IBM Cloud lo siguen muy de lejos.

La nube más voluminosa, la primera capaz de contener un yottabyte (1024 bytes) de datos, es la que mantiene la NSA en el desierto de Utah, una construcción protegida por extremas medidas de seguridad.

La nube ha dejado de ser solo el almacén de la web. Cada día está siendo más explotado por el big data y la inteligencia artificial (IA), vía algoritmos de aprendizaje automático (machine learning) y profundo (deep learning[21]). Cuanta más información procesa el algoritmo, más poderoso se vuelve.

[21] Deep learning es un subcampo del machine learning que, potenciado por el uso de unidades gráficas de procesamiento (GPU) o unidades de procesamiento tensorial (TPU), permite a una máquina realizar tareas como identificar imágenes y reconocer voces de forma similar al cerebro humano. La máquina no aprende a través de un conjunto de instrucciones, sino que lo hace a partir de imágenes, texto o sonido que se le brindan como ejemplos

Tanto AWS como Azure tienen relación con el Pentágono y los servicios de inteligencia estadounidenses. Ambos han pujado por firmar el contrato con el Pentágono para el proyecto JEDI, que pretendía centralizar en la nube los datos del Departamento de Defensa por al menos diez años. El concurso por dicho contrato fue ganado por Microsoft [69], en parte por el involucramiento personal de Trump, que consideró al contrato como uno de los más grandes de la historia, debido a su públicamente conocido enfrentamiento con Jeff Bezos. Amazon, a su vez, posee en AWS un centro de datos exclusivamente para clientes del sector público, llamado GovCloud, con el cual firmó en 2013 un contrato con la CIA.

5.6- El negocio de las empresas de tecnología y los data brokers

Todos los datos que recolectan los principales gigantes tecnológicos acerca de sus usuarios son materia prima del big data, con el que estas empresas crean información sobre usos, gustos y costumbres de sus usuarios [60]. Luego, esta información es vendida a empresas, que luego envían publicidad a la gente vía correo electrónico o con anuncios en redes sociales con temas sobre los que les gustaría leer, saber o comprar.

A esta información recolectada también se le pueden dar muchos usos políticos. Con la información que recolectaron de un potencial presidente desde que era chico es posible potenciarlo o hacer que no tenga posibilidades de ganar. Otro tipo de uso es distribuir masivamente noticias falsas (fake news), desacreditando políticamente a determinados candidatos, como se verá más adelante.

Marta Peirano señala que, en el caso de Google, con Adsense y DoubleClick, su nuevo negocio era ofrecer información sobre las preferencias de sus usuarios a los patrocinadores que el gigante tecnológico tenía como clientes para que, en vez de que hagan los mismos anuncios a todo el mundo con el objetivo de convencer a solo unos cuantos, enfoquen anuncios direccionados a los usuarios de acuerdo a sus gustos. Con las cookies de Google, cada usuario es identificado y se registra su navegación

en millones de sitios web, quedando asentado qué lee, qué compra, cuánto tiempo pasa en cada sitio, etc. [33]

En ambos casos el objetivo era el mismo: vender sus usuarios (sus datos personales y preferencias) como productos a empresas que paguen por ellos.

En 2012, Facebook, ante su deseo de conocer más acerca de sus usuarios (principalmente información comercial), firmó acuerdos con tres data brokers: Acxiom Corp., Epsilon Data Management y Epsilon. Ese mismo año compró Instagram.

El trabajo de las empresas conocidas como data brokers consiste en aglutinar toda la información dispersa que existe sobre cada persona; de ser necesario las compran en el mercado negro. Como menciona Peirano, buscan reunir “nombre completo, dirección, teléfono y número de la Seguridad Social” con “los datos de su tarjeta, matrícula, seguro médico, los informes de su empresa, las liquidaciones de su banco, las compras con sus tarjetas, viajes, suscripciones, multas, tarjeta del casino, factura del veterinario, licencia de armas, currículum académico, series favoritas, antecedentes penales, afiliación religiosa, estado civil, pruebas de ADN, etcétera”. Luego, los trabajan, generando grupos de personas con determinadas características en común, para que le resulte útiles a determinadas compañías. Tal como indica Peirano, algunos ejemplos de estos grupos son adolescentes hijos de padres divorciados con problemas de autoestima y alto poder adquisitivo y aquellos jubilados con antecedentes cardíacos y alto poder adquisitivo que consumen mucha carne roja.

En 2012, al momento de salir a la bolsa, Facebook registraba la cantidad de datos suficiente como para segmentar a un tercio de la población mundial por edad, raza, estado civil, barrio o estatus socioeconómico o separarlos por sus valores, miedos, preferencias sexuales y grado de satisfacción laboral.

Con los altavoces inteligentes, que están siempre escuchando, las empresas tecnológicas tienen una herramienta para llevar la vigilancia masiva al interior de un hogar. Estos altavoces conectados a Internet suelen ser usados para controlar o interactuar con otros dispositivos o plataformas, por

ejemplo, a la hora de reproducir música, ver series o consultar cómo va a estar el clima. [70]

En el caso de Google, Alphabet obtiene más del 80% de sus ingresos por publicidad. Por lo tanto, el asistente de voz Google Home le resulta una buena manera de obtener información privada de sus usuarios para venderla a los anunciantes.

Facebook y Google, entre otras empresas, ante el objetivo de la ONU de erradicar la pobreza extrema, han manifestado su intención de lograr que Internet sea accesible a todo el mundo con distintos proyectos que permiten el acceso a Internet de forma gratuita al utilizar sus servicios, como el ya mencionado Free Basics de Facebook. Sin embargo, teniendo en cuenta que el negocio de este tipo de empresas es vender los datos de sus usuarios a los anunciantes publicitarios, si pueden conseguir que todos los habitantes del planeta utilicen sus servicios sus ganancias se incrementarían de forma proporcional a este aumento. [2]

Jorge Majfud comenta que los gerentes de poderosas compañías de gaseosas, tabaco o comidas rápidas tienen como principal objetivo que el volumen de ganancias crezca sin parar, sin importarle si el tabaco, el azúcar y las grasas recicladas matan a cientos de miles de personas por año [71]. Y sostiene que lo mismo pasa con compañías como Facebook. Al respecto piensa:

> *"Zuckerberg es un buen muchacho, realiza donaciones millonarias […] No obstante, su equipo de ingenieros y psicólogos trabaja día y noche para maximizar las ganancias maximizando el número de los nuevos clientes sin importar que para ello deban desarrollar estrategias de dependencia psicológica, sin importar que varios estudios insistan que Facebook produce depresión, sin importar que varias investigaciones hayan mostrado el carácter adictivo de esta actividad[…] Como el alcohol, el consumidor compulsivo satisface una necesidad creada mientras niega el problema y presume de su libertad".*

5.7- Adicción a las redes sociales y Capitalismo de la Vigilancia

En su libro “El enemigo conoce el sistema” [33], Marta Peirano compara la industria de producción de comida con la de la producción tecnológica. Sostiene que muchos de los productos de las empresas alimenticias buscan que el consumidor se sienta embriagado de dopamina, neurohormona vinculada al placer, pero nunca satisfecho, provocando que siga comiendo de forma frenética. Luego, establece la comparación entre las dos industrias mencionadas:

> *“Estamos todos entregados a la noria del consumo irresponsable de productos inadecuados que nos engordan y nos enferman sin alimentarnos, cabalgando a lomos de nuestra culpa y nuestra vergüenza, impidiendo que podamos estar del todo satisfechos comiendo lo necesario o al menos tener el cuerpo de un ángel de Victoria’s Secret. Pero preferimos pensar que somos unos tragaldabas sin un gramo de disciplina a creer que una de las industrias más poderosas y tóxicas del planeta mantiene equipos de genios extraordinariamente motivados con salarios exorbitantes y laboratorios con lo último en tecnología cuyo único propósito es manipularnos sin que nos demos cuenta. Es exactamente lo que nos pasa con el móvil, con las redes sociales y con las plataformas más exitosas y adictivas de la red. Son las ruedas que hacen funcionar la gigantesca y destructiva economía de la atención”.*

Citando como ejemplo a la empresa Facebook, una de las cinco empresas de las GAFAM, indica que las distintas herramientas que posee no tienen el objetivo de facilitar o hacer más eficiente la vida de los usuarios, sino que cada una de ellas posee un funcionamiento diseñado por expertos para generar adicción, y con esto lograr que cada vez más usuarios, y con más frecuencia, las utilicen. El objetivo de estos servicios es obtener la mayor cantidad posible de información sobre el usuario y sus amigos. Peirano afirma que el objetivo de Facebook es “convertir a cada persona viva en una celda de su base de datos, para poder llenarla de información” y que su política es “acumular la mayor cantidad posible de esa información para vendérsela al mejor postor”.

Facebook no es un caso excepcional, sino solo un ejemplo. La adicción que generan estos servicios es tal que muchas veces ni siquiera la persona se acuerda de para qué revisó su smartphone, ni tampoco de lo que ha visto en las aplicaciones que utilizó recientemente, actuando prácticamente "de memoria". Y la violación a la privacidad de los datos es posible debido al contrato legal vinculante que surge de la aceptación por parte del usuario de los Términos y Condiciones de Uso de un servicio o aplicación, los cuales suelen ser muy extensos y la gran mayoría de las personas no tienen los conocimientos técnicos y legales para comprenderlos.

Un motivo que empuja a millones de personas a utilizar determinados servicios o aplicaciones es el deseo de ser aceptados socialmente (o el temor de ser rechazados socialmente). En otras palabras: el deseo de estar al día con las novedades y no quedarse fuera de onda. A su vez, los desarrolladores se esmeran para que estas aplicaciones sean fáciles de encontrar y simples de utilizar, es decir, que estén muy a mano y que sean amigables al usuario. Los desarrolladores también fomentan a que los usuarios las utilicen lo más seguido posible, ya sea generando un ícono llamativo en el escritorio o enviando notificaciones con cierta frecuencia y con contenido de interés (comentarios nuevos, vistas de perfil, productos con descuentos, posteos de fotos de personas conocidas, etc.).

Cuando la notificación logra su cometido y el usuario accede al servicio, el mismo encuentra sus "recompensas" (ve los likes, comentarios, mensajes, retuits, etc.), que lo recargan de dopamina, haciéndolo sentir mejor y con deseo de tuitear o escribir algún estado ingenioso. El incentivo social es poderoso. En cada red social se puede comparar la "popularidad" de cada usuario, ya sea por el número de seguidores, likes y comentarios que recibe. Cada usuario puede compararse con otro, y si ve que tiene menos popularidad, la reacción natural será pensar que es menos importante o menos querido, produciéndose una gran ansiedad y motivación para poder incrementar su popularidad usando las distintas herramientas que ofrece el sistema. Y así con todos los usuarios, generándose una adicción en cadena.

Esta adicción va generando una rutina en los usuarios, que miran una y otra vez el smartphone, no tanto por el contenido que pueda haber, sino por la propia rutina que le genera actuar "de memoria". Y hay otro truco, que les

permite a las aplicaciones atrapar por más tiempo al usuario: el scroll infinito, al deslizarse incesantemente con el mouse hacia abajo para leer nuevos contenidos.

Este sistema de generar adicción en los usuarios y transformar a cada uno de ellos en materia prima de la cual extraer datos personales, para luego poder manipular su comportamiento, se conoce como Capitalismo de la Vigilancia.

Un estudio publicado en 2017 respalda con solidas evidencias que se puede obtener información de una persona, e incluso predecir su comportamiento, sin que esta tenga una red social en la que esté activa [72]. Esto se logra a partir de la constante interacción entre usuarios, los cuales llegan a revelar en las redes información de otras personas, inclusive no usuarios de redes sociales, sin su consentimiento (e incluso sin su conocimiento previo ni posterior). Los perfiles de personas armados a partir de información no suministrada por ellas mismas a las redes sociales se conocen como “perfiles ocultos” o “perfiles sombra” (shadow profiles, en inglés).

Sean Parker, primer presidente de Facebook, sostuvo en 2017 que siendo conscientes de que con el sistema de los “me gusta” que producen descargas de dopamina “explotaban una vulnerabilidad en la psicología humana” continuaron con el algoritmo de fomentar la interacción y con el modelo de negocios de venta de perfiles de sus usuarios a agentes publicitarios. [73]

Marcelo Colussi afirma que las redes sociales tienen, al menos, dos características que las hacen tan atractivas [74]. Una de ellas es el efecto de las imágenes masivas, las cuales fascinan a los usuarios, pero a la vez no dan mayores posibilidades de reflexión. En general, el usuario prefiere el significado resumido y fulminante de la imagen sintética en lugar del razonamiento y la reflexión.

El segundo aspecto es el hecho de que, al estar conectado, se genera la posibilidad de la interacción constante, la sensación de conocer todo lo que está aconteciendo y la capacidad de opinar y hacer comentarios que jamás se podrían hacer estando cara a cara.

Colussi concluye que si la tecnología no está al servicio de la causa del ser humano “sigue siendo un mecanismo de dominación”.

6- Manipulación de la opinión pública

6.1- Debilidades humanas y filtro burbuja

Tal como sostiene Peirano, el "hambre infinita de satisfacción inmediata" combinado con el alto nivel de distracción que tienen los ciudadanos les hace revisar constantemente sus dispositivos con acceso a Internet y allí consumir la propaganda. Leyendo solo titulares o contenidos fragmentados, debido a que su capacidad de atención promedio es corta, el ciudadano piensa que está actualizado acerca de las noticias. Sin embargo, el acto de pensar requiere de pausa y paciencia, algo que en el acelerado mundo de la televisión y redes sociales es improbable de conseguir. [33]

A su vez, Peirano se refiere al sesgo de los seres humanos al momento de consumir contenidos:

> *"Los seres humanos tenemos sesgos cognitivos, puntos ciegos en nuestro razonamiento que crean una distorsión. […] El primero es la tendencia que tenemos todos a favorecer la información que confirma lo que ya creemos y despreciar la que nos contradice, independientemente de la evidencia presentada. El segundo es que tendemos a sobreestimar la popularidad de nuestro punto de vista, porque nuestras opiniones, creencias, favoritismos, valores y hábitos nos parecen de puro sentido común".*

Luego, habla sobre cómo este sesgo afecta a la visión de la realidad:

> *"Los grupos generan un entorno de consenso permanente, aislado del mundo real, donde la credulidad dentro del círculo es máxima, y fuera del círculo es nula. El rasgo de pertenencia se arremolina en torno al rechazo a «el otro» y su deriva es racismo, genocidio, exterminio y deshumanización. […] Las plataformas de publicidad segmentada ofrecen distintas versiones de la realidad a diferentes grupos políticos, socioeconómicos, étnicos, geográficos, culturales o religiosos, pero los usuarios no se dan cuenta de que son diferentes. El afroamericano que desayuna cada día con titulares sobre brutalidad policial, esclavitud, agravios culturales y racismo institucional no sabe que su odiado vecino blanco amanece con titulares de bandas criminales hondureñas de caras tatuadas, negros detenidos por violar y matar*

misionarias o vender crack a adolescentes. […] No existe la posibilidad de diálogo porque están viviendo realidades paralelas cuya «verdad» es mutuamente excluyente, y los dos piensan genuinamente que el otro miente o manipula la realidad".

El odio se fabrica, ya que no es espontáneo. Para lo cual requiere, por un lado, aislar a las personas, ya que el contacto genera afecto, empatía y comprensión con el prójimo (permite ver a la persona y no a la idea preconcebida que existe sobre esa persona), y, por otra parte, la existencia repetitiva y sin descanso de mensajes que deshumanizan a esas otras personas, de forma que se genere una visión de que los odiados tienen menos rasgos humanos.

Con la facilidad ofrecida por las redes sociales y otras aplicaciones web, cualquier persona tiene un espacio para expresarse, realizar una denuncia, dar opiniones sobre determinados temas, convocar manifestaciones, compartir música o hacerse famoso. Como el algoritmo que corre detrás de las redes sociales está diseñado para priorizar las interacciones, cuantas más visitas, reproducciones, likes, retuits o referencias externas tenga una publicación, más impacto tiene en la red (se vuelve más "viral"), sin valorar si la publicación es buena o mala. Muchas de estas publicaciones son injurias o expresiones violentas contra minorías étnicas o religiosas o están basadas en noticias falsas que pueden ser utilizadas para fines políticos o comerciales, sin que los dueños de las plataformas reciban infracciones o sanciones, debido a que no hay una ley que los responsabilice por estos contenidos. No hay nada que incentive más a las personas a viralizar un contenido que las sensaciones de miedo y odio.

Vía redes sociales resulta sencillo sembrar odio. Y tiene mayor impacto en aquellos países pobres donde funcionan proyectos como Free Basics, con acceso gratuito a determinados servicios de Internet pero que solo permiten leer gratis los titulares de videos y noticias, y si se accede al link se cobran los datos consumidos. De esta forma, resulta más sencillo manipular la opinión pública con campañas de odio y desinformación.

Los algoritmos de las redes sociales saben todo sobre el usuario, así que tienen la capacidad de ajustar los contenidos que le presenta en su portada de inicio en función de su perfil e ideología. Peirano habla al respecto:

“Los dos mil trescientos millones de personas que leen Twitter y Facebook a diario lo hacen como si ambas redes fueran la portada de un periódico en el que salen «todas las noticias que es apropiado imprimir», con un enfoque en los temas que a ellas les interesan y recomendaciones de un círculo de elegidos. No lo leen como si fuera un contenido diseñado a su medida por empresas de marketing y campañas políticas”.

Esto es lo que se conoce como filtro burbuja, una situación en la que un usuario de Internet encuentra solo información y opiniones que se ajustan y refuerzan sus propias creencias.

Por su parte, Jorge Majfud, analizando los posibles efectos de las redes sociales (además de la adicción y las depresiones), escribe:

“Los usuarios (¿individuos?) suelen eliminar con un solo click un <<amigo>> molesto. Esto, que parece muchas veces lo mejor, tiene un efecto acumulativo: hace que los individuos se rodeen de gente que piensa como ellos. Así se crean sectas, burbujas, mientras el individuo se vuelve intolerante ante la discrepancia o la opinión ajena. El producto, el nuevo pseudo-individuo, no sabe debatir. El insulto y el odio afloran a la velocidad de la luz. Así, las redes se convierten en fábricas de odio y de seudo amistades […] El diálogo, antes probable cuando se estaba cara a cara con un café mediante, desaparece y aflora el amor propio, el Ego herido por cualquier punto y coma de más”.[71]

Paradójicamente, en el caso de Facebook cuantos más datos circulen en la red social, menos pluralismo habrá, ya que el filtro burbuja que generan los algoritmos de su plataforma se perfecciona al alimentarse de mayor información. Por lo cual, será más difícil que un usuario encuentre contenido que no vaya en línea con sus ideas. [75]

6.2- Manipulación psicológica

Según Alexandre de Marenches, ex director del servicio de inteligencia francés, una de las claves para lograr aumentar o mantener la posición de privilegio en el conflicto internacional es el control psicológico de la población

con la ayuda de los medios de comunicación y la desinformación. Esto lo decía en 1986, mucho antes de la explosión de Internet y las redes sociales, que han permitido elevar exponencialmente la manipulación psicológica de las masas. [76]

Y aunque exista una jurisdicción internacional con el objetivo, por ejemplo, de evitar esta manipulación, los más poderosos siempre encuentran una manera de sortearla (basándose en su poder y en su capacidad de influencia) aunque, eso sí, velando por que se aplique con rigor y firmeza al resto.

Siempre resulta primordial conquistar la opinión pública. Una manera de hacerlo es repetir insistentemente una idea hasta que quede impregnada en la mente y los corazones de una gran parte de la sociedad, sin importar que se trate de mentiras. Esto se aprecia en la frase atribuida al ministro para Ilustración Pública y Propaganda de la Alemania nazi, Joseph Goebbels: "Miente, miente que algo quedará; cuanto más grande sea la mentira, más gente se la creerá".

Sobre la orquestación de esta propaganda, Goebbels afirma que la propaganda debe limitarse a un número pequeño de ideas y hay que repetirlas incansablemente, presentadas una y otra vez desde diferentes perspectivas, pero siempre convergiendo sobre el mismo concepto, sin fisuras ni dudas. Y también sostiene que la propaganda debe ser renovada constantemente, con nuevos argumentos, a un ritmo tal que cuando el adversario responda, el público esté ya interesado en otra cosa.

El escritor francés Sylvain Timsit definió una serie de estrategias para la manipulación mediática. Una de ellas consiste en desviar la atención del público de los problemas importantes y de las decisiones políticas y económicas, concentrándose en generar información sobre temas menos importantes. Por ejemplo, en Occidente el deporte se ha convertido en la principal distracción. Otra estrategia consiste en crear problemas para generar reacciones en la gente y así ésta exija medidas que los dirigentes deseaban aplicar, como aumentos en las fuerzas de seguridad, retrocesos en las prestaciones sociales o privatizaciones de empresas públicas. Timsit también esgrime la estrategia de dirigirse al público en un tono cuasi infantil cuando se desea engañar al espectador, empleando un lenguaje básico y

comprensible hasta por las personas menos instruidas, por ejemplo usando metáforas. De esta forma se esperaría una respuesta también infantil y desprovista de críticas. La estrategia de la autoculpabilidad también es destacable, con la cual se busca hacer creer al individuo que él es el único culpable de su propia desgracia por ser poco inteligente, tener pocas capacidades o no esforzarse lo suficiente, así la persona se resignará y no se rebelará contra un sistema injusto.

Con las nuevas tecnologías, las sociedades quedan más expuestas a un lavado de cerebro producto de la cuantiosa información sin analizar y sin contextualizar que reciben de los medios y redes sociales, creándose un alto nivel de desinformación. Y cuando se recibe una verdad irrefutable que daña la imagen de alguien importante, afectando intereses, se reacciona atacando a la fuente y no dándole prioridad a su contenido. Un claro ejemplo es lo que sucede con las revelaciones de WikiLeaks.

Sostiene Pedro Baños que lo que nos muestran los medios pocas veces reflejan la realidad objetiva, y suelen mostrar un escenario artificial hipnotizante del que es difícil salir y que impide ver lo que en verdad ocurre a espaldas de los ciudadanos.

El tercer presidente de Estados Unidos, Thomas Jefferson, dijo en una carta fechada el 14 de junio de 1807: "[…] la persona que nunca mira un periódico está mejor informada que la que los lee; ya que quien no sabe nada está más cerca de la verdad que aquel cuya mente se ha llenado con falsedades y errores". Estas palabras de Jefferson son cada día más ciertas, más aún teniendo en cuenta el exponencial incremento de la información que reciben las personas hoy en día (sobre todo con la explosión del uso de las redes sociales) en comparación a la fecha de esta frase (a mayor volumen de "información", más desinformación).

Un ejemplo de este tipo de propaganda ocurrió en el siglo XX en Estados Unidos durante la presidencia de Reagan, donde, a partir de documentos desclasificados, se pudo develar la existencia de programas para influir en la opinión pública con determinados objetivos, entre ellos superar los resultados de la guerra en Vietnam en los ciudadanos estadounidenses y contrarrestar la propaganda soviética convenciendo al mundo de las bondades de la política exterior de Estados Unidos.

Un ejemplo más cercano en el tiempo surgió a partir de un artículo publicado en 2015 por el periodista Adrian Chen. El mismo trata sobre la empresa rusa Internet Research Agency (IRA), aparentemente bajo órdenes del Kremlin, que, a partir de cientos de trolls y mediante sofisticados montajes de videos e imágenes y clonación de páginas web de importantes medios, lograron difundir masivamente información falsa en Internet y redes sociales perjudicando a Estados Unidos.

Pedro Baños comparte la idea de Freud de que los pensamientos, costumbres y gustos que constituyen gran parte de la cultura de una sociedad han sido impuestos a la mayoría de la población por una minoría que supo adueñarse de los medios de poder, agregando que se puede marginar y perseguir socialmente a quienes intenten poner en tela de juicio estas ideas impuestas. De esta forma, ya sea por seguir estas tendencias predominantes de la mayoría o por temor a ser perseguidos y aislados socialmente (miedo innato de las personas), quienes tienen pensamientos contrarios a los dominantes suelen optar por no compartirlos al público.

En los últimos años, los medios de comunicación más influyentes del mundo se han concentrado en unas pocas manos, dándoles un inmenso poder con capacidad para, incluso, derribar gobiernos. Las principales agencias de noticias del mundo (prácticamente todas estadounidenses, inglesas o francesas) tienen una gran influencia en el mensaje final que llega a la ciudadanía, ya que de ellas se alimentan la mayor parte de los medios de comunicación del planeta que se limitan a retransmitirlas a sus audiencias sin hacer un análisis profundo de ellas, debido a la necesidad de dar noticias con rapidez. Al hablar sobre la labor de los periodistas en los medios de comunicación, Baños sostiene:

> *"Cada vez son menos frecuentes las investigaciones y los análisis independientes. La mayor parte de los medios de comunicación dependen de fuentes de información de dudosa solvencia y habitualmente condicionadas por determinados intereses. Salvo honrosas excepciones, en lugar de realizar verdadero periodismo, emplean informaciones sin contrastar, emiten imágenes sensacionalistas sin análisis ni contenido y dan preferencia a los titulares más llamativos en detrimento del rigor".*

Por otra parte, en el ambiente periodístico existe la presunción de que muchos periodistas y medios de comunicación de distintos países (incluso de países sin un gran peso internacional) reciben información clasificada filtrada por los servicios de inteligencia (nacionales o internacionales) para, en base a ellas, elaborar grandes investigaciones periodísticas a cambio de otros favores, como transmitir al público información favorable a los intereses del gobierno al que pertenecen dichos servicios de inteligencia. Alguien que intentó sacar a la luz estas presuntas relaciones fue el destacado periodista alemán Udo Ulfkotte, que a partir de 2014 reveló que tanto él como muchos otros periodistas de distintos países eran sobornados o recibían información clasificada de servicios de inteligencia, como el BND alemán o la CIA, a cambio de publicar noticias falsas que beneficiaran a Washington o a otros países occidentales. El mismo Ulfkotte cuenta, como ejemplo, que agentes de la BND le presentaron un informe sobre El Gadafi y la situación en Libia con datos secretos obtenidos por la agencia, y lo único que tuvo que hacer es poner la firma, quedando el artículo publicado a su nombre.

Cables de WikiLeaks han mostrado la estrategia del gobierno de Arabia Saudita para neutralizar o atacar periodistas que difundan información que afecte negativamente al gobierno, de forma tal que se mantenga una imagen internacional positiva de Riad.

Los grupos extremistas también hacen uso de los medios de comunicación (por lo general, con la difusión de videos en Internet) para hacer apología de su lucha y ganar adeptos y para atemorizar y desprestigiar a sus enemigos.

6.3- Dominio cultural

La expansión y consolidación de los imperios a lo largo de la historia no se consiguió solo con la fuerza sino también con la imposición de la cultura (idioma, religión, estilo de vida, hábitos, etc.). Hoy en día, una de las formas en que se busca la influencia cultural es a través de los medios de comunicación, las redes sociales y el arte. Por ejemplo, en las películas estadounidenses es habitual que aparezcan dos de sus símbolos patrios, el himno y la bandera, para incentivar el espíritu patriótico. Otro ejemplo es el otorgamiento de becas a estudiantes destacados por parte de instituciones

culturales que distintos países, como Francia y China, tienen diseminados en todo el planeta, para que estos jóvenes estudien en centros educativos de esos países de forma tal que vayan incorporando los valores y costumbres del país en cuestión. [38]

La dominación por medio de la cultura es principalmente indirecta. En 2018, según el Observatorio Audiovisual Europeo, los productos cinematográficos estadounidenses ocuparon casi el 70% del mercado mundial [76]. Detrás de esta ficción, se filtran valores americanos sobre su estilo de vida y sobre quiénes son los "buenos" y los "malos" en el mundo. Además, en 2017 se dieron a conocer documentos desclasificados que revelaron que el Pentágono, la NSA y la CIA influyeron en los argumentos de unas 800 exitosas películas y unos 1000 programas de televisión, para evitar rigurosas críticas al servicio militar y a los servicios secretos norteamericanos y para promover las guerras en el exterior [77]. Si a esta situación se le suma la magnificación del miedo en los ciudadanos (arma psicológica por excelencia del Estado para manipular al pueblo), como ocurre cuando se establece al terrorismo o a algún país enemigo como amenaza a la seguridad nacional, prácticamente no hay oposición social a sacrificar libertades y derechos (por ejemplo, permitiendo vigilancia masiva a costa de privacidad) ni a incrementar esfuerzos bélicos fuera del territorio nacional.

Estados Unidos tiene una dominación cultural a nivel mundial, principalmente a través de sus programas de televisión, series y películas, su música, hábitos alimentarios, vestimenta, idioma y tecnología. [38]

Rusia ha tenido un auge en su cine y series de televisión ultranacionalistas.

Por su parte, China viene invirtiendo en productoras y distribuidoras de cine y televisión estadounidenses, como AMC Entertainment, Lionsgate y Universal, a través de empresas del gigante asiático como Dalian Wanda, Alibaba y Perfect World Pictures. Tal como señala Baños “Hollywood tiene lo que le faltaba a China: capacidad para contar historias”. Esto le permite a China extender sus historias, que, por ejemplo, resalten el patriotismo chino, y, a su vez, contrarrestar la propaganda norteamericana.

6.4- Guerra de la comunicación

Imponerse en los medios de comunicación es hasta más importante que ganar en el ámbito militar, ya que si no se le brinda una imagen positiva al pueblo éste podría quitarle apoyo y dejarlo debilitado ante sus enemigos. Para lograr conquistar la mente y los corazones de su gente, los gobiernos pugnan entre sí para controlar (y difundir) las percepciones de la realidad, los relatos y las imágenes, por más que no se apeguen demasiado a la realidad. En este sentido, Baños afirma que si se logra influir en la forma en que los individuos entienden la realidad se les podrá “hacer creer lo que se quiera y convencerlos incluso del candidato o partido por el que deben votar”. [38]

Este control de la comunicación para influir en las percepciones no es nada nuevo. Por ejemplo, Napoleón Bonaparte construyó su propio mito magnificando sus victorias ante la prensa y el arte para captar más apoyo de su pueblo y generar pánico en sus aliados. Y, por el contrario, sus rivales (como Inglaterra y España) difundían caricaturas y panfletos ridiculizando a Napoleón para desprestigiar su imagen.

Otro caso particular es el de los grupos extremistas, como el Estado Islámico. Éstos, a través de difusión de videos sanguinarios, el envío de mensajes amenazadores a ciudades del mundo y el empleo de atentados para generar terror en los adversarios, sumado a los mensajes persuasivos que envían a su gente (diciendo que sus enemigos buscan acabar con su religión y modo de vida y prometiendo la victoria), buscan el impacto mediático que les permita contrarrestar su inferioridad tecnológica y bélica.

Los medios de comunicación históricamente han demostrado una gran eficacia para moldear la opinión pública, ya sea para crear o destruir movimientos sociales o políticos, justificar guerras o convencer a la población con relatos falaces.

Otra forma de manipulación mediática es la impulsada por empresas comerciales que llevan adelante técnicas de marketing psicológicas para incrementar sus ventas. El objetivo es hacer creer a la gente que si no adquieren sus productos o servicios están destinados a ser infelices o vivir en condiciones adversas. Aprovechando el actual contexto en el que los

usuarios de redes sociales, especialmente Instagram, solo postean fotos y vídeos de sus mejores momentos, las empresas se ven beneficiadas de que las personas aspiren a disfrutar de bienes materiales para alcanzar esa “felicidad” que exponen estos usuarios o de un mundo que se presenta como paradisíaco en propagandas en la televisión o en Internet.

Por otra parte, si una determinada realidad no aparece en los medios o no se replica masivamente en redes sociales o servicios de mensajería es como si no existiera, y si una persona se entera de esta situación es probable que desconfíe de su verosimilitud por no haberla recibido de uno de los principales medios de comunicación o redes sociales. Son ejemplos las muertes en conflictos armados en países como Yemen y Siria que, por intereses a los que responden los grandes medios de comunicación, no son difundidas masivamente.

Las noticias falsas (fake news) son más bien relatos disfrazados de noticias, habitualmente mezclando la verdad con la mentira de forma sutil (pocas veces son completamente falsas), lo que hace más difícil todavía conocer la realidad. Esta situación amenaza acabar con la esperanza de saber qué ocurre en realidad, y así imponer el instinto humano de la comodidad de consumir una verdad (relato) antes que el desafío de enfrentar las contradicciones.

La desinformación ha estado presente desde que el hombre empezó a comunicarse, pero el término “fake news” fue popularizado por Donald Trump en 2016, para descalificar una participación suya en un reality show americano. De esta forma, el término está más asociado al mundo de la política que a otros ámbitos.

No solo lo que se lee puede ser falso, sino también lo que se ve y escucha. La tecnología permite actualmente la generación de videos con imágenes y audios alterados que muestren a una persona conocida haciendo o diciendo cosas que nunca ha manifestado. Además de lo rápido que se difunde este tipo de material, por más que luego se intente mostrar que el video era falso, la desmentida llega a muy pocas personas y el daño ya está causado.

Para fines de 2018 ya se preveía que el Deepfake sería una tendencia. Se trata de una tecnología basada en IA que hace posible crear videos falsos de personas con un gran realismo, ya sea generando diálogos con la voz de

una persona o generando sus movimientos faciales y corporales característicos y montándolos en un vídeo que nunca sucedió en la realidad [78].

Deepfake es un acrónimo de deep learning y fake news. La técnica de deep learning utilizada para la generar estos videos falsos se conoce como Redes Neuronales Generativas Adversarias (GANs, por sus siglas en inglés). En Anexos se pueden ver más detalles sobre estas redes.

Los deepfakes están evolucionando increíblemente rápido, siendo cada vez más fácil y barato de crear y, a su vez, más difícil de comprobar su veracidad tanto para el ojo humano como para las herramientas de análisis forense.

Cuanto mayor sea la cantidad de datos con los que se alimentan las redes GAN, más difícil será determinar que no son reales los videos. Por lo que las personas famosas, que tienen muchos contenidos (imágenes, audios, videos) en Internet, son las más afectadas. [79]

Una vez ingresados los datos de la persona objetivo se puede, por ejemplo, crear discursos de ésta desde cero, que nunca existieron en la realidad.

Un artículo de Nobbot [80] define al deepfake como “un salto de calidad y peligrosidad en el <<arte de la desinformación>>” y sostiene que “en la sociedad de la imagen en la que vivimos, el poder de un vídeo o una foto es mucho mayor que el de un texto escrito”.

Un artículo de 2018 del New York Times [81] indica que, luego de la aparición de un videomontaje de la ex primera dama Michelle Obama, creado mediante un programa llamado FakeApp, los videos generados por software ya no son algo que solo disponen las grandes industrias cinematográficas y las investigaciones de punta. La comunidad de desarrolladores ya ha creado aplicaciones que permiten realizar montajes realistas, como la mencionada FakeApp.

Los deepfakes son un arma muy susceptible de ser utilizada para difamación de políticos, crear pornografía vengativa (pornovenganza) o tender trampas a personas para culparlas de crímenes.

Ejemplo de demonización

Pedro Baños menciona que la concentración de los medios de comunicación en unas pocas manos le facilita al poder el control de la difusión de la información, ya que en el peor de los casos deberá ejercer presión sobre

unos pocos objetivos. Para desacreditar y demonizar a los medios disidentes se los suele, en el más suave pero efectivo de los casos, acusar de difundir noticias falsas, carecer de objetividad o ser antipatrióticos.

Un ejemplo de cómo se demoniza a un enemigo en la fase previa a su ataque, con el objetivo de lograr el apoyo de la opinión pública, es la operación mediática llevada a cabo en 2011 contra Gadafi, el por entonces líder de Libia. Dos semanas antes de la ofensiva sobre el país norteafricano un artículo del periódico Daily Mail, el segundo periódico británico más leído, afirmaba que Gadafi tenía armas químicas y estaba dispuesto a utilizarla contra su propio pueblo, además de dar detalles de los terribles efectos que provocaban sobre los seres humanos. Asimismo, citando como fuente a un antiguo ministro de Justicia libio, aseguraba que Gadafi contaba con armas biológicas como ántrax, sarín y hasta el virus de la viruela modificado genéticamente, y, por si fuera poco, que disponía de mil toneladas de polvo de uranio que le permitirían fabricar una bomba atómica. Hay que decir que Libia no usó ninguna de estas armas, ni contra la población ni contra las fuerzas internacionales que la atacaron. [76]

También se supo, a partir de los correos electrónicos filtrados de Hillary Clinton durante su campaña presidencial en 2016, que, para continuar con la demonización de Gadafi y lograr el apoyo de la opinión pública occidental, se hicieron correr rumores (que se extendieron por todos los medios de comunicación occidentales) de que las fuerzas del dirigente libio recurrían a violaciones masivas, lo cual fue desmentido por varias organizaciones, incluyendo a Amnistía Internacional.

Este tipo de operación con participación de servicios secretos estadounidenses ha tenido éxito (y seguramente lo continúe teniendo) en muchos países, buscando deshacerse de una persona arruinando su prestigio, por más alto poder o imagen positiva que tenga en la sociedad, y mucho más hoy en día a través del perverso uso de redes sociales y la televisión.

Propaganda vs Desinformación

De acuerdo a lo que cada votante quiera oír, la industria de la manipulación política le contará una determinada historia para inducirlo a votar al candidato que la emplea [33]. Malcom X, activista norteamericano y defensor

de los derechos de la población afrodescendiente, decía: “Si no estás prevenido ante los medios de comunicación, te harán amar al opresor y odiar al oprimido”.

Luego de las campañas del referéndum para el Brexit en Gran Bretaña y de la presidencial de Donald Trump se puso de moda la palabra “posverdad”, para referirse a las circunstancias en las cuales los hechos objetivos son menos influyentes en la opinión pública que las emociones y las creencias personales.

La manipulación de la opinión pública se puede llevar a cabo vía propaganda o desinformación. Como menciona Peirano, la principal diferencia entre ellas es que la propaganda usa los medios de comunicación de maneras “éticamente dudosas” para convencer a la población de un mensaje, y con la desinformación el mensaje es un invento basado en documentos alterados, datos fabricados o material sacado de contexto para crear una visión alterada de la realidad. Las campañas de desinformación comienzan identificando las grietas preexistentes en la sociedad con el fin de alimentarlas y llevarlas al extremo. Estas armas de la comunicación son ejemplos de herramientas de la Guerra Híbrida o Guerra de 5ª Generación (tema abordado en el capítulo Contexto geopolítico del presente trabajo).

En el caso de Rusia, el gobierno de Putin ha financiado agencias de noticias internacionales para que brinden una interpretación de la realidad alternativa a la versión occidental y anglosajona, y agencias de desinformación, como la Internet Research Agency que, además de crear noticias falsas, recibe material de grupos de hackers rusos (como Fancy Bear) y agencias de espionaje. Incluso IRA generaba, a través de cuentas falsas en redes sociales, comunidades en Estados Unidos en torno a una lucha o ideología (a favor y en contra del derecho a portar armas, a favor y en contra del matrimonio homosexual, a favor y en contra de los derechos para los inmigrantes, etc.), a las cuales les enviaba noticias falsas y convocaba a manifestaciones. El objetivo de IRA era, justamente, amplificar las mencionadas grietas ideológicas y así dividir a Estados Unidos (divide y vencerás), al hacer enfrentar a su población.

6.5- Fact checking

Con el objetivo de combatir las fake news han surgido iniciativas de comprobación de hechos [38], o fact checking, que se tratan de prácticas periodísticas que buscan comprobar a posteriori informaciones que circulan en los medios de comunicación o en redes sociales, y alertar el hecho a través de su sitio web de modo que cada información falsa quede desmentida. Algunos ejemplos son Maldito Bulo (España), Pagella Politica (Italia), Chequeado (Argentina) y BBC reality check (Reino Unido).

Sin embargo, es muy poco probable que una verificadora de hechos sea completamente neutral. Por un lado, porque cada uno de sus periodistas o investigadores tiene sus propias opiniones sobre los hechos que debe analizar y, por otro lado, porque muchas de estas organizaciones son impulsadas por grandes medios que querrán imponer sus condiciones.

Además, tal como comenta Esther Miguel Trula [82], los analistas sugieren que, cuanto más divisivo sea un tema (aborto, inmigración, etc.), las personas tienden a apoyar más fuertemente su propia creencia, aunque se les muestre evidencia que refutan sus ideas. Esto permite que muchos partidos políticos opten por decir muchas mentiras que luego obtienen más visualización mediática al ser analizados por fact checkers, lo que genera más apoyo público ya que, como se mencionó anteriormente, por más que las mentiras sean refutadas no se afectan las creencias.

6.6- Manipulación de encuestas y seguidores

Un informe de Trend Micro [83] explica que una de las formas más efectivas de influir en la opinión pública es manipulando encuestas en redes sociales u otros sitios online. Un ejemplo es la empresa rusa Siguldin, capaz de manipular casi cualquier sistema de votación en Internet y pasar por alto controles de seguridad como la detección de la dirección IP origen, los captchas, los mecanismos de autenticación en redes sociales, el registro en los sitios, entre otros. Los potenciales clientes reciben una prueba gratuita de 10 a 20 votos ingresados fraudulentamente, y el pago comienza luego del voto número 50.

El informe también destaca que existen otras herramientas de países de habla inglesa, como Quick Follow Now, que ofrecen aumentos en visualizaciones en videos de YouTube (de acuerdo al paquete contratado) e incremento de seguidores o likes en Instagram, Facebook y Twitter. Esto permite una mayor repercusión de determinados contenidos.

6.7- Influencias de Grupos y ONGs

Existen grandes grupos de presión que, manipulando la opinión pública en los medios de comunicación, logran influir fuertemente en los procesos electorales de diferentes países [76]. Un ejemplo son las ONGs localizadas en decenas de países del magnate húngaro-americano George Soros, de cuyas Fundaciones para una Sociedad Abierta (OSF, por sus siglas en inglés) se filtraron, en 2016, documentos internos que revelaron cómo Soros intervino en el cambio de Gobierno en Ucrania en 2014. Para tal fin, utilizó una de las OSF, la ONG ucraniana Fundación por el Renacimiento Internacional (IRF, por sus siglas en inglés). El objetivo era hacer llegar al gobierno ucraniano a Petró Poroshenko, en contra de los intereses de Rusia, y mantenerlo en el poder. Para esto Soros afirmaba, en estos documentos, que también era necesario poner a la opinión pública europea en contra de Rusia y a favor de Poroshenko, principalmente en Grecia (muy ligada culturalmente a Moscú), donde el magnate propuso hacer campaña en periódicos, radios, televisión y redes sociales.

La Casa Blanca ha logrado convencer a la mayoría de los líderes de los países europeos (y éstos, a su vez, a la opinión pública de sus respectivos países) de la maldad de los rusos, posiblemente por el temor de una amalgama entre Rusia y Europa, que, tal como dice el experto en geopolítica George Friedman, representaría una potencia difícil de contrarrestar.

Soros ha apoyado y financiado campañas de varios candidatos demócratas en Estados Unidos, entre ellos a Hillary Clinton en 2016. El jefe de esa campaña de Hillary Clinton fue John Podesta, quien junto con su hermano Anthony son dueños de la firma lobista Podesta Group que, tal como muestran documentos revelados por The Intercept [84], firmó acuerdos con el gobierno de Arabia Saudita, uno de los principales donantes de la

fundación Clinton. Es más, según confirmó Julian Assange, Anthony Podesta es un agente del gobierno de Arabia Saudita para representar los intereses de ese país en Washington.

6.8- Diplomacia y espionaje

La diplomacia, entendida desde finales del siglo XVIII como la gestión de negociaciones entre naciones a partir de funcionarios estatales, desde los turbulentos años del siglo XX se convirtió en otro instrumento (uno de los más importantes) de los países más poderosos para ejercer influencia en otros países del mundo. Un diplomático con gran poder de persuasión y personalidad arrolladora, y más aún si representa a un país con una fuerza (capacidad para intervención militar o para sanción económica) que genere intimidación a los demás países, tendrá muchas posibilidades de conseguir beneficios para su nación, sobre todo si el país con el que negocia no tiene la suficiente autoridad o tenacidad para imponer condiciones. A la potencia no le alcanza con lograr las alianzas con el país que negocia, sino que debe también realizar una campaña vía medios de comunicación y redes sociales para generar una opinión favorable sobre ella en la población local, y así esta reaccione favorablemente a los intereses del poderoso. La influencia de las embajadas vía redes sociales es cada vez más habitual, ya sea ofreciendo una imagen positiva del país que representa o dañando la reputación de sus rivales. [38]

Hay una relación muy estrecha entre la diplomacia y los servicios de inteligencia, siendo muy común que trabajen coordinadamente, ya que comparten un objetivo en común: obtener información. Para esto, ambos tienen que conocer en profundidad a los líderes (políticos, sindicales, religiosos, periodísticos, etc.) y a la historia e idiosincrasia del país en el que actúan para ser más efectivos en sus negociaciones, e incluso para intentar predecir sus acciones.

Es habitual que existan agentes de inteligencia que, camuflados de diplomáticos, llevan a cabo operaciones para intervenir en la economía o en la política, ya sea financiando a miembros de la oposición (con la esperanza de que lleguen al poder y así este nuevo gobierno sea más afín a sus

intereses), interviniendo en los procesos electorales o manipulando a figuras de los medios de comunicación para que influyan en la opinión pública de forma favorable a sus intereses.

Hoy en día los servicios de inteligencia de un país son tanto o más importantes que su fuerza militar, ya que están permanentemente siendo utilizados en nuevas misiones a nivel global (neutralización de agresiones o intentos de robo de información por parte de otros Estados, espionaje de países de interés –enemigos o aliados-, vigilancia de población local, etc.), con escenarios nuevos, como el ciberespacio, pero con los mismos objetivos de siempre. Además de la comunidad de inteligencia (compuesta por organismos públicos que producen inteligencia y por empresas privadas que contratan los gobiernos para estos fines), existe un componente extra llamado reserva de inteligencia, formado por especialistas procedentes del mundo académico o empresarial que aportan conocimientos de gran valor a los servicios de inteligencia sin pertenecer a ellos.

6.9- Lawfare

A partir de un ensayo en 2001 de Charles J. Dunlap, por entonces coronel de la fuerza aérea de Estados Unidos, comenzó a tomar notoriedad el concepto de "lawfare" o "guerra jurídica", donde se refería a la manipulación que ejercían los talibanes en Afganistán sobre las leyes internacionales con el objetivo de poner fin a los bombardeos que recibían por parte de Estados Unidos. Es decir, ponía a Estados Unidos como “víctima” de un lawfare que frenaba los intentos norteamericanos de bombardear libremente al país afgano. [76]

El concepto de lawfare hace referencia al uso (o abuso) del derecho como sustituto de medios militares para alcanzar un objetivo operacional. La estrategia de los Estados consiste en ampararse en la legalidad de un principio aceptado por la comunidad internacional (principalmente, el de proteger a los ciudadanos que sufren violaciones de un determinado gobierno), la cual tergiversan al máximo para legitimar sus acciones (incluyendo, de ser necesario, una intervención militar). Suele ocurrir que cuando un país no puede justificar una intervención militar por amenaza a la

seguridad nacional, recurre a estas razones humanitarias. De una u otra manera, ha quedado demostrado que, cuando hay voluntad política de intervenir, se encuentra alguna justificación, de ser necesario retorciendo las leyes nacionales o internacionales.

Pedro Baños sostiene que es absolutamente razonable, y legitimado por las Naciones Unidas, la intervención humanitaria desde otros países en un Estado para salvar a su población cuando el propio Estado no puede (o no quiere) proteger a sus ciudadanos, o bien si es el mismo quien violenta sus derechos. Sin embargo, no resulta objetivo que la decisión de qué situaciones amenazan a la paz y seguridad internacional sean decididas por los miembros del Consejo de Seguridad de las Naciones Unidas. Esta decisión dependerá de sus propios intereses políticos y económicos. Acá es donde entra en juego la estrategia del lawfare, con la cual se desarrollan intervenciones militares con la finalidad de conseguir y mantener influencia y poder de determinados países, y el resto de los países necesitados ni siquiera serán mencionados en los principales medios de comunicación. Lo que termina prevaleciendo son los intereses de las potencias, en lugar de centrarse en lo primordial: la protección de la población civil.

El lawfare se ha convertido en uno de los mayores peligros para la democracia en todo el mundo y, en especial, en América Latina [85]. En este último caso, ha implicado la designación de jueces que representen determinados intereses para que puedan llevar adelante el uso indebido de elementos jurídicos para desprestigiar o perseguir a un adversario (por lo general, político). El proceso es apoyado por una amplia cobertura de medios de comunicación concentrados (incluso, sosteniendo los medios la culpabilidad de la víctima cuando no hay una sentencia judicial), también afines a los mencionados intereses, para manipular la opinión pública y dejar a la víctima vulnerable a acusaciones sin pruebas y con menos apoyo popular [86].

En 2019, el Papa Francisco, hablando sobre el lawfare, indicó que “es fundamental detectar y neutralizar este tipo de prácticas, que resultan de la impropia actividad judicial en combinación con operaciones multimediáticas paralelas”. [87]

El lawfare también se sirve del abuso del espionaje ilegal de servicios de inteligencia (nacionales o extranjeros) para facilitar información vinculada a la víctima a periodistas o fiscales, quienes la utilizan para iniciar o profundizar el proceso judicial.

Ejemplo de lawfare en Argentina

En marzo de 2019, el juez federal de Argentina Alejo Ramos Padilla reveló una red de espionaje político y judicial en el país. La investigación se inició cuando en enero de ese mismo año el empresario Pedro Etchebest denunció que fue extorsionado (una exigencia de 300.000 dólares) por Marcelo D'Alessio, quien decía actuar como enviado del fiscal federal Carlos Stornelli (distintas pruebas que se han hecho públicas han demostrado el estrecho vínculo entre ambos), para no ser involucrado judicialmente en la llamada "Causa de los Cuadernos". Dicha causa investigaba supuestos casos de corrupción en la obra pública durante la presidencia de Cristina Fernández de Kirchner y estaba a cargo de Stornelli. Etchebest proporcionó pruebas de audio e imagen de la extorsión. En algunas grabaciones pertenecientes a la investigación D'Alessio se presenta como un representante regional de la Administración para el Control de Drogas de Estados Unidos (DEA, por sus siglas en inglés). [88]

Ramos Padilla comunicó que, luego del primer allanamiento, se dieron cuenta que no se trataba de un caso aislado. Lo que se estaba investigando era una organización de agentes o ex agentes de inteligencia (nacionales e internacionales, orgánicos o inorgánicos), con vínculos con agencias nacionales e internacionales, que estaba llevando adelante operaciones de espionaje ilícitas vinculadas con la actividad de los poderes judiciales, los ministerios públicos (nacionales y provinciales), las fuerzas de seguridad (nacionales y provinciales), los poderes políticos y los medios de prensa. D'Alessio tenía en su poder informes de inteligencia con el sello de la embajada de Estados Unidos.

Durante la investigación, la empresa de telefonía a la que pertenecía la línea de teléfono que D'Alessio tenía agendada como "Patricia Bullrich", y con quien intercambiaba mensajes de algunas de las operaciones que llevaba adelante, pertenecía efectivamente a quien fuera Ministra de Seguridad durante la presidencia de Mauricio Macri [89]. A su vez, D'Alessio se jactaba

de su acceso a algunos medios de prensa para operar contra la víctima y lo utilizaba como parte de las extorsiones. Daniel Santoro, periodista de Clarín, fue el principal operador desde el sector mediático en contra de las víctimas. Ramos Padilla afirmó que la metodología empleada por la organización constaba de la "recopilación de información, la producción de inteligencia y el almacenamiento de datos sensibles de manera paralela a las causas judiciales que se utilizaban para luego llevar a cabo acciones coactivas intimidatorias y extorsivas con la finalidad de influir en causas judiciales". En mayo de 2020, Federico Pinedo, ex senador del partido de Macri, afirmó en un programa de radio que es normal e institucional que el poder ejecutivo hable con jueces para advertirles sobre los fallos que deben dictaminar.

Ejemplo de lawfare en Brasil

El medio internacional The Intercept, creado por Glenn Greenwald, filtró en junio de 2019 [90] material (incluyendo chats privados de Telegram, grabaciones de audio, videos y fotos) que evidencia que Sergio Moro, el entonces juez del caso Lava Jato (el mayor escándalo de corrupción de Brasil), hizo consultas y asesoró a procuradores federales del caso (cuando legalmente deben guardar distancia institucional) sobre la estrategia para las investigaciones contra el ex presidente de Brasil Lula Da Silva, con las cuales terminó dictando el encarcelamiento del ex mandatario (sin sentencia firme), imposibilitándolo de participar en las elecciones presidenciales del 2018 [91].

Algunos mensajes filtrados sugieren que Deltan Dallagnol, fiscal del Lava Jato y supervisor de la acusación contra Lula, tuvo dudas respecto a cuán contundente era la evidencia contra el ex presidente[22]. Otras conversaciones indican que los procuradores discutieron estrategias para que Lula no pudiera dar una entrevista a medios de comunicación desde prisión antes de la elección, por temor a que eso favoreciera al PT (Partido de los Trabajadores), fundado por Lula. En parte de una conversación, Moro critica a Dallagnol por la lentitud en el avance de la investigación, sugiriéndole: "¿No es demasiado tiempo ya sin una operación?".

[22] La acusación contra Lula era por recibir un departamento frente al mar por parte de la empresa constructora OAS como un soborno a cambio de facilitar millones de dólares en contratos a Petrobras, pero carecía de pruebas documentales sólidas para demostrar que el departamento era de Lula o que éste alguna vez facilitó algún contrato.

Los grandes medios de comunicación de Brasil mostraron un gran apoyo a Sergio Moro durante la investigación del Lava Jato, generando en la opinión pública una imagen muy positiva del juez. Según Glenn Greenwald [92], los grandes medios “no estaban informando sobre el Lava Jato, estaban trabajando para el Lava Jato”, sosteniendo que los periodistas “dejaron de investigar y cuestionar al Lava Jato” y solo se limitaban a “publicar lo que el grupo de tareas quería que ellos publicaran”. Luego de las filtraciones, Greenwald comenta que, a excepción de la cadena Globo, los grandes medios “informaron sobre el material de forma más o menos justa, con la gravedad que merece”.

El juez Moro reconoció la veracidad de los mensajes, pero sostuvo que no demuestran que él actuó de manera inapropiada.

Es de público conocimiento que el Departamento de Justicia de Estados Unidos colaboró con el juez Moro en la causa Lava Jato. Incluso, en agosto de 2019, miembros del Congreso estadounidense enviaron una carta firmada al fiscal general de Estados Unidos, William Barr, exigiendo respuestas sobre posibles colusiones ilegales y violaciones de la ética en la colaboración del Departamento de Justicia de Estados Unidos con el grupo de trabajo de la causa Lava Jato [93].

Con Lula preso y el PT estigmatizado, Jair Bolsonaro logró ganar las elecciones en 2018, nombrando posteriormente a Moro a cargo de los ministerios de Justicia, Seguridad y Lucha contra la Corrupción.

6.10- Ingeniería social

La ingeniería social consiste en, estrategias psicológicas mediante (como la persuasión y la sugestión), extraer información de una persona (ya sea claves de acceso a sistemas como información personal), sin que esta sea consciente de ello, para luego utilizarla en perjuicio de la víctima. Quienes aplican ingeniería social se aprovechan del exceso de confianza, buena fe o inocencia de las víctimas, que les brindan información ya sea personalmente, telefónicamente, vía mail, servicios de mensajería o simplemente realizando publicaciones en redes sociales acerca de su personalidad, actividades, ideologías, entornos familiares, etc. A partir de

esta información recolectada, el victimario comienza a trabajar con los datos para manipular a su víctima, por ejemplo, haciéndose pasar por una persona de confianza para obtener información más crítica (número de tarjeta de crédito, claves de acceso, etc.). [38]

Otra finalidad de la ingeniería social es la creación de perfiles psicológicos y sociales de las víctimas, a partir de los datos recolectados, para venderlos a entidades que los emplearán para hacer publicidades direccionadas (de acuerdo al perfil de la persona) y así persuadir a las víctimas para que adopten determinadas posturas, como sucedió con la empresa Cambridge Analytica en las elecciones presidenciales estadounidenses de 2016.

6.11- Máquina de propaganda automatizada

Berit Anderson y Brett Horvath explican cómo funciona la máquina de propaganda automatizada y qué consecuencias puede tener [94].

El profesor Jonathan Albright de la Universidad de Elon se refiere a esta máquina de propaganda:

> *"Está dirigida a las personas, de manera individual, para reclutarlos en torno a una idea. Es un nivel de ingeniería social que nunca se había visto antes"*[23].

Cambridge Analytica ha sido el ejemplo más poderoso de este tipo de máquinas de propaganda basadas en inteligencia artificial, las cuáles parecen haberse convertido en un nuevo pre-requisito para el éxito político en un mundo de polarización, aislamiento, trolls y publicaciones invisibles (dark posts en inglés), todo lo cual será explicado más adelante.

El caso de Cambridge Analytica

SCL Group era una consultora británica especializada en operaciones psicológicas (“psyops”) en países como Pakistán y Afganistán, proporcionando análisis de datos a gobiernos y organizaciones militares en todo el mundo. Esta consultora fue la casa matriz de la estadounidense Cambridge Analytica (CA), creada en 2013, cuyo principal accionista fue Robert Mercer, uno de los financiadores de la campaña de Donald Trump de

[23] "It’s targeting people individually to recruit them to an idea. It’s a level of social engineering that I’ve never seen before".

2016. A su vez, Steve Bannon, quien fuera director ejecutivo de la mencionada campaña de Trump, fue co-fundador de CA junto con Mercer. [33]

CA trascendió por su rol en las elecciones presidenciales de Estados Unidos en 2016 y por su influencia en el referéndum por el Brexit (salida del Reino Unido de la Unión Europea), también en 2016. Sin embargo, operó en más de 100 campañas políticas en el mundo, y en América Latina trabajó en Argentina, Brasil, Colombia y México. [95]

Todo empieza cuando, en 2013, Michal Kosinski (psicólogo y especialista en psicometría y minería de datos) junto a sus colegas en la Universidad de Cambridge publicaron una aplicación, llamada “MyPersonality”, que les permitía identificar el género, la sexualidad, las creencias políticas y los rasgos de personalidad de un individuo a partir de correlacionar "likes" en Facebook con calificaciones del test de personalidad OCEAN[24]. [94]

Según Das Magazine de Zurich:

> *"[…] con solo diez likes como insumos, su modelo podría evaluar el carácter de una persona mejor que un compañero de trabajo promedio. Con setenta, podría ‘conocer’ un tema mejor que un amigo; con 150 likes, mejor que sus padres. Con 300 likes, la máquina de Kosinski podía predecir el comportamiento de un sujeto mejor que su pareja. Con aún más likes, podría exceder lo que una persona piensa que sabe acerca de sí misma".*

Poco después, Kosinski rechazó una oferta de SCL Elections (una subsidiaria de la compañía SCL Group, al igual que CA, que afirmaba ser especialista en manipular elecciones) para replicar su método.

Tal como declaró Christopher Wylie, ex empleado de CA, Alexandr Kogan, un profesor de Cambridge del Departamento de Psicología y colega de Kosinski, diseñó una aplicación llamada “This is your digital life”, una réplica de la aplicación “MyPersonality” y también basada en el sistema de evaluación psicológica OCEAN [33]. Dicha réplica consistía en un test de personalidad disponible en Facebook para aquellos usuarios habilitados para

[24] También conocido como el test de los Cinco Grandes o Big Five, por cada una de sus siglas en inglés (Openness - apertura a nuevas experiencias, Conscientiousness - ser consciente o responsabilidad, Extraversion - extroversión, Agreeableness – afabilidad o amabilidad, Neuroticism - inestabilidad emocional).

votar en las elecciones de Estados Unidos del 2016. Al realizar el test los usuarios aceptaban ceder los datos de su usuario para "fines de investigación académica" [96]. Su test constaba de 120 preguntas y ofrecía entre dos y cuatro dólares a quien lo completara en plataformas de micropagos como Turco Mecánico, de Amazon, y Qualtrics. También se podía completar en Facebook, donde los test estaban de moda.

Facebook le permitía de forma precisa, barata y remota obtener una base de datos para generar perfiles psicométricos, es decir, conocer las preferencias, gustos y emociones de las personas a través de sus interacciones en la red, además de otros datos adicionales como edad, ciudad donde vive, nivel socioeconómico, etc. [33]. Kogan logró convencer a unas 270 mil personas para que completaran el test. Sin embargo, Facebook mantenía una Interfaz de Programación de Aplicaciones (API) con los desarrolladores de aplicaciones externas para que estos pudieran interactuar con la plataforma de la red social y, a través de esta API, los desarrolladores externos tenían acceso a los datos de los usuarios que instalaban sus aplicaciones y a los de sus amigos[25]. Lo mismo aplicaba para los test, ya que sus desarrolladores podían acceder a los datos de los usuarios que hacían el test (edad, localización, estado civil, religión, afiliación política, preferencias) y también a los de todos sus amigos (sin necesitar que estos últimos lo acepten). Y no se trataba de una vulnerabilidad de la plataforma, sino que era una función deliberadamente elegida por Facebook para atraer anunciantes.

Como sostiene Lucas Malaspina [97], este asunto no se trató de una filtración, sino que dejó expuesto el principal negocio de Facebook (y de las demás redes sociales): ofrecer datos de los usuarios a terceros, los cuales dispondrán de información sobre el perfil y gustos de los usuarios y así podrán publicitar en la red social sus productos o servicios con mayor efectividad. Con respecto a esto último, sentencia:

> *"[…] los usuarios son la materia prima de Facebook, y los clientes son los anunciantes. Para ganar más, necesita exprimir más la materia prima y multiplicar los anunciantes".*

[25] Dicha API fue cerrada por Facebook recién en abril de 2014 (reemplazándola por una más restrictiva), habiendo durado cinco años, mucho tiempo para que los desarrolladores hayan podido extraer gran cantidad de datos de los usuarios.

Facebook calculó que se habrían obtenido datos de al menos 78 millones de usuarios. Hasta ese momento, nada de lo que había hecho Kogan era ilegal. De hecho, usar tests para recopilar los datos de los usuarios de Facebook y de sus amigos era una práctica conocida de cientos de miles de agentes desde al menos 2009, a costa de la privacidad de dos mil millones de personas. [33]

Sin embargo, el acuerdo de desarrolladores (que Kogan aceptó al subir el test a la red social en 2012) decía que los datos de los usuarios no podían comercializarse. Y Kogan, a través de su empresa, Global Science Research, vendió a Cambridge Analytica la base de datos que recolectó con su aplicación "This is your digital life" [97].

CA, además, compró a varios data brokers cientos de bases de datos para perfeccionar los perfiles de los usuarios[26] y así poder influir en las búsquedas en Google y en la portada de inicio de Facebook, que se pueden comprar como parte de una campaña.

Peirano sostiene que el escándalo Cambridge Analytica "hizo estallar la nueva industria del marketing político online entre los partidos políticos". Esta nueva forma de marketing superó en capacidad a la llevada a cabo por Obama en 2008, en la cual se utilizó Internet no solo para distribuir los mensajes de campaña, sino que también se encargaron de poner en contacto a sus seguidores. Esto último, inspirándose en la filosofía Open Source, les permitió que sus partidarios pudieran contribuir a la campaña de manera activa, tanto en la red como en las calles, juntando firmas y fondos para la campaña o realizando investigaciones y denuncias contra la competencia. Y todo quedaba centralizado en la página de la campaña: My.BarackObama.com.

Alexander Nix, directivo de CA, explicó que su receta secreta era, a partir de todos los datos recolectados, inferir la personalidad de las personas en base a sus motivaciones psicológicas para entender cómo se comportan y cómo toman decisiones, lo que se conoce como microtargeting conductual. [94]

Según un estudio del IICS (Instituto Internacional de Seguridad Cibernética por sus siglas en inglés) [57], en una elección solo un 40% tiene definido su

[26] Los algoritmos predictivos son tan buenos como lo sean la cantidad y la calidad de las bases de datos que los alimentan.

voto, un 35% se mantiene indeciso y el restante 25% puede ser condicionado a lo largo de la campaña electoral.

Usando los perfiles psicográficos, CA podía identificar aquellos votantes aun inseguros del candidato al que van a votar para poder modificar su comportamiento, publicando luego anuncios diseñados en base a los rasgos de personalidad individuales. [94]

CA recibía un feedback de este anuncio casi instantáneamente de parte del votante y el algoritmo elaboraba una rápida respuesta. Por ejemplo, si el votante accedía al anuncio (mostrando interés), el algoritmo le serviría más contenido que enfatice la causa. Si no mostraba interés, el algoritmo intentaba con un título diferente, quizás uno que enfatice sobre otro rasgo distinto de su personalidad.

Gran parte de esto se hace a través de publicaciones invisibles de Facebook (dark posts), que solo son visibles por aquellos votantes que se utilizan como objetivo. Debido a que las publicaciones invisibles solo son visibles para los usuarios específicos a los que se dirigen, no había forma de que alguien fuera de CA o de la campaña política a la que está apoyando rastreara el contenido de estos anuncios.

Al igual que Wylie, quien también denunció esta actividad de CA fue Brittany Kaiser, quien trabajó como directora en CA entre 2015 y 2018. Como se puede ver en el documental The Great Hack, estrenado en 2019, Kaiser declara como arrepentida sobre cómo CA influyó en los votantes de las elecciones de 2016 de Estados Unidos y del Brexit.

El caso de Cambridge Analytica, con su influencia en las elecciones presidenciales de Estados Unidos y en el Brexit como sus dos casos más emblemáticos, ilustra muchos de los riesgos de que el big data sea mal utilizado. Por una parte, pone de manifiesto la amenaza a la privacidad, así como la falta de legislación al respecto. Por otra parte, demuestra su influencia en la manipulación de la información, la desinformación y la formación de opiniones políticas. [96]

Elecciones presidenciales en Estados Unidos en 2016

Mucho se habló de la injerencia rusa en las elecciones presidenciales de Estados Unidos en 2016, en la que no se sabe si Trump conspiró con Putin ni si lo hizo su equipo por iniciativa propia. Las comunicaciones del partido

Demócrata con el jefe de campaña de Hillary Clinton, John Podesta, fueron filtradas a través de WikiLeaks y la página de filtraciones llamada DCLeaks. Esto originó una campaña de desprestigio contra Clinton, que también había hecho trampa para ser candidata, ya que algunos de los mails filtrados sugerían que hubo un complot interno en el Comité Nacional Demócrata (DNC) para asegurarse de que ganara Hillary Clinton la elección primaria.

La investigación del fiscal especial Robert Mueller reveló en 2018 que fue Roger Stone, asesor de la campaña de Trump, quien organizó la entrega de los documentos a la “Organización 1”, que, al parecer, era WikiLeaks. Julian Assange confirmó que, al igual que su organización hace con todos los documentos que filtra, recibieron los documentos sin rastro del remitente (para proteger a sus fuentes de una probable persecución policial) y, antes de filtrarlos, comprobaron su veracidad.

En una entrevista [98], Assange afirma que la publicación de dichos mails no fue para favorecer a Trump sino porque le aseguraron a sus fuentes que serían publicados en el momento de mayor impacto. Al igual que la mayoría de los analistas, Assange creía que iba a ganar Clinton, sabiendo que Trump tenía en contra a los bancos, a los principales medios, a los políticos, a la CIA y a los gigantes de Silicon Valley (como Google).

Para poder obtener estos mails alguien debió haber realizado un ataque al servidor de correo del DNC, acto que se adjudicó un presunto hacker rumano llamado Guccifer 2.0, que al poco tiempo se supo que ni siquiera hablaba ni entendía el idioma rumano. En este sentido, la investigación de Mueller concluyó que Guccifer 2.0 era un oficial del Departamento Central de Inteligencia ruso (GRU) y que DCLeaks había sido creada y gestionada por dos agentes de inteligencia rusos.

Sin embargo, el informe de Mueller concluye que no hubo colusión, es decir, que no hubo miembros de la campaña de Trump que coordinaran o conspiraran con el gobierno de Rusia en sus actividades de interferencia en las elecciones. [99]

Hay (al menos) un país adicional donde también se operaba en Internet para favorecer a Trump, aunque con otro motivo. Se trata de la ciudad de Veles, en Macedonia, en la cual el salario medio era muy bajo (unos 320 euros) y los muy virales artículos (sensacionalistas o directamente noticias falsas) a

favor del candidato republicano le permitieron al centenar de sitios web que los redactaban cobrar hasta 5000 euros al mes, al tener Adsense de Google para publicidad.

Por otra parte, tanto Peter Thiel, miembro del consejo directivo de Facebook, como Robert Mercer, quien fue propietario de Cambridge Analytica hasta su cierre en 2018, dieron su apoyo público a Donald Trump para las elecciones de 2016. Thiel es conocido como el mentor de Mark Zuckerberg al ser uno de los primeros inversores de Facebook (fundada en 2004) al igual que la CIA que, a través de su fondo de capital riesgo, In-Q-Tel, puso millones de dólares. A su vez, Thiel es cofundador y mayor accionista de Palantir Technologies Inc., una compañía de software especializada en big data, que desarrolló el programa XKEYSCORE para la NSA y luego tuvo diversos contratos no solo con la NSA sino también con otros organismos estadounidenses como el FBI, la CIA y la Marina. Siendo ya para 2016 una de las mayores contratistas del gobierno norteamericano para el espionaje y la vigilancia masiva, Palantir (recordando que Thiel es directivo de Facebook) colaboró con Cambridge Analityca durante la campaña presidencial de Trump para la explotación de los datos de los usuarios de Facebook. [33]

Hillary Clinton invirtió mucho más dinero que Donald Trump para la campaña en Facebook, sin embargo, la propaganda del republicano, a pesar de ser menos seria que la de Clinton, tuvo más visibilidad porque era mucho más viral. Era comentada y compartida tanto por sus seguidores (con likes y comentarios a favor) como por sus detractores (con comentarios negativos), pero todos servían para su viralización. Así lo menciona Peirano:

> *"La plataforma de Facebook es igual que la de Google, pero en lugar de comprar por palabras, el anunciante compra determinadas audiencias. El precio del anuncio depende de la cantidad de gente que pincha, comparte o comenta el anuncio. Cuanto más viral es el anuncio, más veces aparece, y consigue más impresiones por el mismo dinero. Si el algoritmo calcula que el contenido de un anunciante va a generar cinco o diez veces más interacciones que el de otro anunciante, entonces sus anuncios aparecerán cinco o diez veces más que los del competidor".*

Las plataformas digitales permiten decirle a cada grupo exactamente lo que quiere oír, y sin que los demás lo sepan, ya que la propaganda es direccionada (a través de dark posts) de acuerdo a un perfil psicográfico elaborado a partir de los datos recolectados.

El objetivo de CA en las elecciones estadounidenses era encontrar aquellos entre dos y cinco millones de ciudadanos más susceptibles de ser convencidos en determinados estados donde se necesitaban algunos votos a favor de Trump para poder ganarlo[27]. Contando, además, con las operaciones rusas, los sitios web de Veles, Macedonia, y las acciones llevadas a cabo por su equipo de campaña.

Operaciones en Argentina

Tras ser filmados por cámaras ocultas en diversas reuniones por empleados del noticiero británico Channel 4 News [100], que se hicieron pasar por políticos de Sri Lanka deseosos ganar las elecciones en ese país, directivos de Cambridge Analytica, entre ellos Alexander Nix, contaron diversos detalles de su forma de actuar. Un ejemplo es el uso de mujeres para implicar a candidatos opositores en un escándalo sexual. Otra estrategia es filmarlos mientras se les intenta ofrecer dinero como soborno para luego acusarlos de corrupción. También, utilizar espías del Reino Unido o Israel para recopilar información personal sobre el pasado de contrincantes políticos. Todo, por supuesto, operando “desde las sombras”.

A su vez, durante los encuentros, los representantes de Cambridge Analytica alardean de haber trabajado en unas 200 campañas políticas alrededor del mundo, entre ellas, en Argentina, Kenia y Nigeria.

En 2018, el CEO de Cambridge Analytica, Alexander Nix, dio su testimonio ante el Parlamento Británico de que su empresa planificó llevar adelante en Argentina una campaña “anti-Kirchner”. [101]

Ha quedado demostrado en Argentina que, durante esos años y a través de numerosos trolls en redes sociales (principalmente en Twitter), se han creado y difundido noticias falsas o amenazas sobre distintas personalidades que se manifestaban en contra del por entonces oficialismo. Estas publicaciones se basan principalmente en sembrar odio hacia dichas

[27] En las elecciones de 2016 en Estados Unidos, unos setenta mil votantes en tres estados definieron la elección.

personalidades, y, como ya se ha mencionado anteriormente, el odio es uno de los principales medios para viralizar contenidos. Dada su viralización en redes sociales, muchas de estas noticias falsas han llegado a ser tratadas por programas de televisión de alta audiencia, generando una difamación de mayor impacto [102].

Estas noticias falsas, amenazas y demonizaciones continuan viralizándose en la actualidad en Argentina vía cientos de trolls, orquestados principalmente desde organizaciones políticas que responden a determinados intereses, con el apoyo de ciertos personajes mediáticos que las fogonean y con la participación de seguidores reales que están en linea con ciertos ideales. Algunas de las modalidades de difusión de estos contenidos son hacer tendencias algunos hashtags provocativos, responder tweets de forma agresiva y con argumentos poco sólidos a personas que manifiesten ideas opuestas a los intereses que ellos representan, convocar manifestaciones con consignas grotescas o basadas en manipulaciones de la realidad, compartir datos inexactos o noticias falsas publicadas por importantes medios y responder favorablemente (comentarios positivos, likes y retweets) a mensajes de cuentas que exhiban contenidos alineados a sus intereses.

La campaña de Bolsonaro

Como menciona Marta Peirano, la victoria de Jair Bolsonaro en las elecciones brasileñas del 2018 parecía improbable [33]. Por un lado, por su publica postura como racista, machista, homofóbico y defensor de la dictadura militar que tuvo lugar en Brasil entre 1964 y 1985. Y, por otra parte, por el hecho de que desde 2015 el dinero público de la campaña y el espacio en prensa, radio y televisión se distribuye de manera proporcional al número de asientos que tiene el candidato en el Congreso, y el Partido Social Liberal, al que pertenecía Bolsonaro, tenía solo ocho diputados (de un total de 513). A su vez, el acuchillamiento que recibió en su abdomen en septiembre de 2018 le sirvió para no asistir a los debates.

Quien luego sería jefe de gabinete, Onyx Lorenzoni, aseguró que la campaña fue ejecutada a través de WhatsApp, Facebook y Twitter. El servicio de mensajería WhatsApp, que Facebook compró en 2014, no se responsabiliza por lo que se haga entre los usuarios que se comunican, ya

que, teóricamente, luego de la implementación del cifrado de extremo a extremo en 2016, no puede acceder a las conversaciones. Y en Brasil casi la mitad de la población utilizaba WhatsApp como principal fuente de información electoral, por lo que era muy difícil que las fact checking pudieran combatir con eficacia la desinformación que en ella se produjera, como si es posible, por ejemplo, en Facebook o Twitter.

El equipo de campaña de Bolsonaro creó cientos de miles de chats, que recibían miles de mensajes diarios (en su mayoría noticias falsas o información sacada de contexto para desprestigiar a su competidor, Haddad), que primero llegaban a activistas locales y regionales que luego los difundían a otros grupos cuyos miembros, crédulos, los diseminaban a sus propios contactos personales. El servicio de "listas de difusión" que posee WhatsApp le dio la posibilidad de tener mayor llegada a los ciudadanos, ya que, a diferencia de los grupos, permite que cada destinatario vea que los mensajes que reciben de forma individual, generándose un chat separado para cada destinatario.

A inicios de 2019, WhatsApp ha tomado la medida de limitar a cinco la cantidad de canales (no de personas) a las que se pueden reenviar mensajes de manera simultánea. Pero, tal como destaca Peirano "[…] los grupos pueden tener hasta doscientos cincuenta y seis participantes […] Si cada una de esas personas pueden reenviar el mismo mensaje a otros cinco grupos, el contenido puede llegar a millones de personas en pocos minutos con un coste cero".

6.12- Origen de las fake news, bots y trolls

Para las elecciones de Estados Unidos en 2016, el profesor Albright rastreó 306 páginas web de noticias falsas y encontró como resultado una red de 23.000 páginas y 1,3 millones de hipervínculos, los cuales están conectados con frecuencia a los principales medios de comunicación, redes sociales y recursos informativos [94], como se puede ver en la Imagen 18.

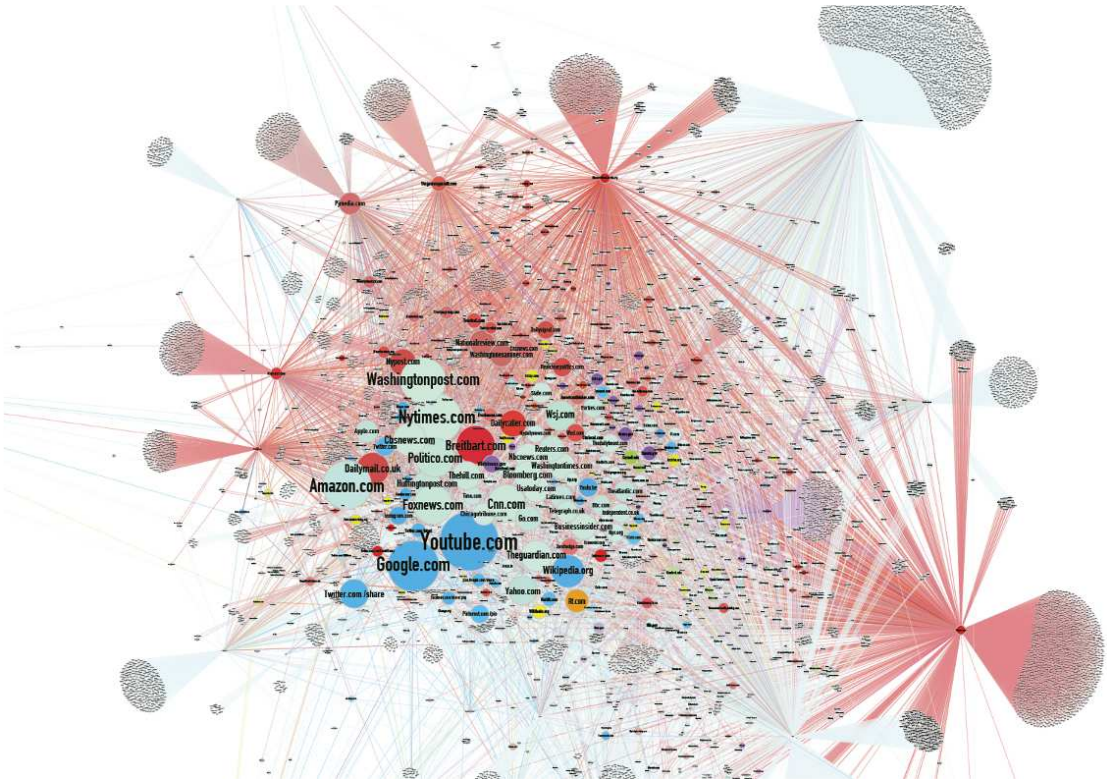

Imagen 18 - Fuentes vinculadas a noticias falsas encontradas por el profesor Albright
Fuente: https://scout.ai/story/the-rise-of-the-weaponized-ai-propaganda-machine]

Estos sitios no son administrados por una entidad individual, pero juntos han sido capaces alcanzar un alto posicionamiento en los buscadores, aumentando la visibilidad de las noticias falsas y sesgadas cada vez que alguien en Google busque un término relacionado con las elecciones. Esta red de noticias falsas creó una poderosa infraestructura para que compañías como Cambridge Analytica puedan rastrear a los votantes y refinar sus modelos de análisis de personalidad.

Además de las noticias falsas en sí mismas, existe una red internacional de gobiernos, consultorías (muchas veces integradas por directivos a solo un grado de distancia de los actores oficiales del gobierno) y personas que construyen y mantienen redes masivas de bots (conocidas como botnets[28]) o perfiles falsos en redes sociales (trolls) para distribuir y amplificar la propaganda de los actores políticos, difamar a sus oponentes y silenciar o intimidar a aquellas personas que expresen una ideología contraria.

[28] Una botnet es una red de máquinas “zombies” (bots), es decir, de máquinas infectadas con algún programa malicioso, las cuales recogen y ejecutan instrucciones de un tercero que las controla.

No todos los bots se crean de igual manera. Por ejemplo, el bot de Twitter es un robot habitualmente programado para retuitear determinadas cuentas y así contribuir a popularizar ciertas ideas, y también suelen responder de forma automática a aquellos usuarios que utilizan determinadas palabras clave o hashtags, a menudo con insultos o amenazas preconfiguradas.

En cambio, los bots de gama alta son operados por personas reales que emplean identidades falsas. Se encargan de responder a otros usuarios de forma específica, cuestionando su punto de vista, para intentar cambiar sus opiniones o la de sus seguidores. Al ser perfiles no automáticos y al tener amigos o seguidores, es mucho menos probable que sean descubiertos (y de que sus cuentas sean desactivadas) por Facebook o Twitter. Una sola persona podría crear y mantener más de un bot: se estima hasta unos 400 en Twitter y entre 10 y 20 en Facebook. En julio de 2018, Twitter había detectado más de 70 millones de cuentas falsas entre sus usuarios.

Las botnets de alta calidad se usan a menudo para múltiples campañas políticas. Por ejemplo, durante el referéndum del Brexit, una red de bots, previamente utilizada para influir en la conversación sobre el conflicto israelí-palestino, fue reactivada para luchar por la campaña a favor de la salida de la Unión Europea (campaña *Leave*). Es decir, los perfiles individuales se actualizaron para reflejar el nuevo debate.

Anderson y Horvath sostienen que la máquina de propaganda basada en big data y en Inteligencia Artificial está dando recién sus primeros pasos, y representa una gran ventaja para aquellos actores políticos que la utilizan mediante la recopilación de datos, la creación de mejores test de personalidad, el uso de inteligencia artificial y la contratación de más trolls. Concluyen que en las campañas políticas futuras el ganador será aquel candidato cuyo equipo use mejor los datos recolectados (ya que todos tendrán posibilidad de acceder a utilizar el big data) para refinar los algoritmos de machine learning (aprendizaje automático), el cual les permite inferir la personalidad de cada votante que sea objetivo de la propaganda y en base a ella distribuir un mensaje personalizado.

Cambio en los algoritmos de Google

Con el auge de las fake news, en 2017 Google (y algo similar sucedió con Facebook) anunció que modificó sus algoritmos de búsqueda para “hacer

emerger contenido más autorizado" y así dificultar el acceso a noticias falsas. [34] Luego del cambio en el algoritmo de búsqueda de Google, algunos sitios como WikiLeaks, Amnistía Internacional, The Intercept y varios medios independientes experimentaron bajas en las visitas a sus sitios, creando la sospecha de que Google se haya aliado con los medios tradicionales potentes para discriminar a medios alternativos e independientes [103]. Y, tal como lo demostró el estudio del profesor Jonathan Albright hecho en 2016, las principales fuentes de noticias falsas no son los medios alternativos sino las grandes corporaciones mediáticas (Google, CNN, The Washington Post, Amazon, Fox News, etc.), que dicen combatir la difusión de falsedades.

Así, Google se transforma en gran editor periodístico mundial, no solo con influencia política sino también comercial. En 2017, la Comisión Europea multó a Google con más de dos mil millones de euros por utilizar su motor de búsqueda para aventajar a su propio servicio de compras, Google Shopping.

6.13- Otras estrategias para influir en elecciones

Las empresas privadas tienen acuerdos con actores políticos, pero, dentro de la mayoría de los países, violaría la ley que un partido político transfiera dinero a una empresa privada con fines electorales. Por lo tanto, se recurre a acuerdos previos entre los privados y los posibles futuros gobernantes y legisladores que si logran ganar las elecciones impulsarán planes y proyectos para favorecer a quienes contribuyeron al éxito electoral. [57]

Los partidos políticos suelen usar distintas estrategias en los medios tradicionales. Una de ellas es comprar espacios publicitarios en aquellas zonas donde se identificó una menor intención de voto, pagar al medio para que éste realice publicaciones con opiniones positivas o bien pagar para promover una investigación para descalificar a otros candidatos o partidos políticos. Otra estrategia posible consiste en intervenir en canales de televisión para cambiar la agenda de los temas sobre los que quieren y sobre los temas que no quieren que se hable, ofreciendo dinero y contratos de publicidad oficiales, o bien dando bonos a periodistas y líderes de opinión como recompensa por su "buen comportamiento". También un partido

político puede utilizar el espionaje a periodistas opositores o a aquellos que no son fáciles de sobornar para amenazarlos y ejercer influencia sobre sus informes e investigaciones. Una última estrategia a mencionar es el uso de anuncios y carteles en aquellas zonas geográficas detectadas por la vigilancia masiva con un mensaje a medida según el perfil identificado de las personas de ese lugar, atrayendo la mirada de muchas personas.

Los gobiernos podrían utilizar la información obtenida de la vigilancia masiva para limitar la libertad de expresión y beneficiar solo a las personas del poder que gobierna. Algunos ejemplos son: formar un grupo de elite donde sus miembros alternen los mandatos (eliminando la posibilidad de analizar otros proyectos de nación), espiar a quienes están en desacuerdo para accionar contra ellos y así reducir la oposición y ganar mayor gobernabilidad, crear una falsa oposición donde sus mismos partidarios las conforman, vigilar a la oposición para anticiparse a sus acciones y arrestar a personas que representan una amenaza política para el gobierno.

6.14- Historia de la interferencia en procesos electorales

La influencia en procesos electorales no es algo nuevo. Según un estudio del analista político Dov Levin, entre 1946 y 2000, Estados Unidos interfirió en 81 elecciones realizadas en 45 países (desde las campañas de Filipinas de la década de 1950 a las nicaragüenses de 1990), sin incluir los golpes de Estado o los intentos de cambio de régimen cuando resultaba electo un candidato contrario a los intereses de Washington. El modus operandi incluía desde distribución de propaganda hasta ayudas económicas. [76]

El estudio de Levin también indica que Rusia también intentó influir en procesos electorales en 36 ocasiones. Además, se conoce el caso de la segunda vuelta de las elecciones francesas del 2017 cuando se filtraron por redes sociales correos electrónicos del candidato Emmanuel Macron, apoyado mayoritariamente por la prensa europea y por el ex presidente norteamericano Barack Obama, con el objetivo de perjudicarlo en beneficio de su contrincante Marine Le Pen, apoyada por Rusia. Hay quienes sostienen que esta operación, conocida como "Macron Leaks", respondería a una maniobra del Kremlin.

7- Contexto geopolítico

En este capítulo se pretende dar algunos detalles del contexto geopolítico dentro del cual se suscitan los hechos y situaciones narrados anteriormente.
En su libro "Así se domina el mundo" [76], Pedro Baños describe las estrategias llevadas a cabo por los distintos países en su afán de poder y dominio (que tienen su origen en tiempos pasados, pero con una notable vigencia), a partir de su experiencia y de una recolección de ideas de diferentes pensadores y actores políticos y sociales muy reconocidos a nivel mundial.
Luego, en su libro "El dominio mundial" [38], que complementa a "Así se domina el mundo", Baños detalla los instrumentos empleados para lograr dicho dominio.
Este capítulo está basado en las dos obras mencionadas, complementado con otras citas con aportes de otros autores.

7.1- Tipos de países y estrategias

Según Baños, se puede considerar que existen dos tipos de países, los dominadores y los dominados. Esta dominación puede ser más o menos directa y de diversas formas (económica, cultural, tecnológica, militar, etc.).
Aquellos países que no se sienten poderosos procuran cobijarse bajo el paraguas de alguno que si se sienta (por ejemplo, alguna de las potencias nucleares, que se pueden ver en la Tabla 1) para que, al menos teóricamente, le brinde seguridad a cambio de determinados negocios. O bien pueden buscar asociaciones con otros países para ganar peso.

País	Misiles nucleares disponibles (estimación)	Ensayos nucleares realizados	Máxima potencia alcanzada
Estados Unidos	6450	1032	15 Megatones
Rusia	6850	715	50 Megatones
Francia	300	210	2,6 Megatones
China	280	45	3,3 Megatones
Reino Unido	215	45	1,8 Megatones
Pakistán	140 - 150	2	0,04 Megatones
India	130 - 140	5	0,04 Megatones
Israel	80	0	-
Corea del Norte	10 - 20	6	0,06 Megatones

Tabla 1 – Datos de las potencias nucleares

Fuente: Pedro Baños, "El dominio mundial" (2018) y "Así se domina el mundo" (2017)

Teniendo en cuenta que los intereses son cambiantes, las relaciones internacionales varían permanentemente. En ocasiones las naciones deciden aliarse con otras para conseguir fines concretos, más o menos temporales, que pueden ir desde los económicos a los de seguridad o puramente bélicos. Incluso, muchas de estas relaciones son contra natura por las diferencias ideológicas, pero se unen en pos de un enemigo en común o de algún beneficio mutuo.

Si los países asumidos débiles, que también buscan obtener para su nación el mayor beneficio o el menor perjuicio posible, se dejan arrastrar por las potencias pueden ingresar en aventuras bélicas ajenas a sus propios intereses. Y lo que pueden terminar ganando es que se produzcan atentados en su propio territorio (si el conflicto bélico fue con grupos que entre sus tácticas está el terrorismo) o que el descontento de su pueblo lleve al derrocamiento del gobierno responsable de elegir participar en el conflicto.

Existen algunas excepciones a esta distinción entre dominadores y dominados. Algunos (muy pocos) países, como actualmente lo es Corea del Norte, no encaja en ninguno de los dos tipos, pero deben defender su supervivencia sin ayuda de otros países. Y, por último, hay un reducido grupo de países (como Ucrania, Egipto, Turquía e Irán) que tienen una

relevancia por su ubicación geográfica o por su capacidad de influencia, y mantienen una relación ambigua con las potencias mundiales.

Como se detalla a continuación, Baños refleja cómo es la estrategia de los Estados, tanto de los más poderosos como de los menos, para luchar por una posición de privilegio (en cuanto a riqueza y poder), con prácticas propias de la ambición y el egoísmo.

Por un lado, los Estados más poderosos aspiran a mantener su posición de privilegio ya sea a través de enfrentamientos armados (prácticamente todos ellos surgen principalmente por motivaciones económicas; ver ejemplos en Anexos) o interviniendo en la actividad económico-financiera de otros países[29] para controlar sus riquezas (hidrocarburos, agua dulce, minerales estratégicos, etc.) y así salir lo más favorecido posible, muchas veces a través de negocios con grandes empresas. Además de buscar mantener esta posición de privilegio, operan para impedir a otros países poner en práctica algunas medidas (muchas de las cuales en su momento llevaron a los privilegiados a su actual posición de dominio), ya sea como parte de una negociación o mediante prácticas de intimidación. Otras operaciones consisten en fomentan la ruptura de alianzas entre países si es que de alguna manera representan una amenaza a sus intereses, o apoyar (por ejemplo, financieramente o proveyendo armas) a organizaciones rebeldes de algún país para que luchen contra el gobierno local. De hecho, desde tiempos de la Guerra Fría, Estados Unidos y algunos de sus aliados (como Reino Unido, Arabia Saudita y Qatar) han financiado grupos radicales islamitas, lo que permitió el surgimiento de grupos terroristas como Al Qaeda y el Estado Islámico, para avanzar con los intereses occidentales en Medio Oriente. Luego, ambos grupos terroristas, siguiendo sus propios intereses, han declarado la guerra tanto a países de Oriente Medio como a Occidente.

Un ejemplo de operación política con inclusión de actividades de inteligencia es lo sucedido en Irán en la década de 1950. A mediados del siglo XIX, los pozos de petróleo de Irán eran disputados por la Unión Soviética, Estados

[29] Uno de los ejemplos que señala Baños es cuando el Ejército de Estados Unidos elaboró un informe sobre Afganistán (luego de su invasión en 2001) donde concluyó que la producción de algodón sería muy rentable para el país asiático y así les haría una gran competencia a los americanos, entonces estos últimos pusieron todos los impedimentos posibles para que su producción no se pusiera en marcha.

Unidos y Gran Bretaña, logrando los británicos una importante supremacía. Cuando el democráticamente electo primer ministro de Irán Mohamed Mossadeq decidió que se tenía que nacionalizar el petróleo (lo cual hubiera generado que los británicos dejaran de controlarlo) se llevó a cabo la Operación Ajax, denominada así por la CIA y reconocida luego por la administración de Barack Obama. La misma, orquestada por Gran Bretaña y Estados Unidos, se inició cuando los británicos boicotearan el petróleo iraní, logrando que nadie se atreviera a comprarlo. Al poco tiempo, la economía del país persa se hundió, generando una situación propicia para un golpe de Estado, que ocurrió en 1953. Para acelerar el derrocamiento de Mossadeq, Estados Unidos y Gran Bretaña fomentaron la demonización del primer ministro iraní en la población local, a la vez que tanto la CIA como el servicio de inteligencia exterior británico, el MI6, promovieron disturbios en las calles.

Por parte de los restantes Estados, los menos poderosos, Baños sostiene que buscan la forma de ganar poder para tener más riqueza o ganar mayor riqueza para tener más poder, ya sea asociándose con otros países o aprovechando determinadas características que tienen a su favor, por ejemplo, canales de navegación por los que circulan embarcaciones de diversos países o la disposición de recursos naturales en su territorio.

7.2- Colonialismo de las democracias

Durante la Guerra Fría, Rusia fomentó en diferentes países los movimientos nacionales contra el colonialismo, las dictaduras y los gobiernos de derecha, y apoyó la implantación de democracias populares con el objetivo de expandir su ideología en todo el planeta.

En esos tiempos, y especialmente durante el mandato de Ronald Reagan (1981-1989), Estados Unidos implementó una doctrina de pensamiento que sostenía que los regímenes prosoviéticos eran totalitarios (y que buscaban controlar los pensamientos de la población y ejercer influencia en países vecinos) y que las dictaduras proestadounidenses eran autoritarios (y solo se limitaban a controlar la conducta de la población). Sostenían que estas últimas con el paso del tiempo podían, pacíficamente, convertirse en

democracias, pero que para las primeras solo podría lograrse a través de la violencia. De esta forma, desde Washington se apoyaron las dictaduras y los gobiernos anticomunistas en países como Afganistán, Argentina, Filipinas, Angola y Nicaragua.

Poco ha cambiado esta situación. En los últimos años varios gobiernos han sido removidos (o han intentado lograrlo) con mayor o menor apoyo desde el exterior, incluso aunque hubiesen sido elegidos mediante votaciones legítimas, de acuerdo a los intereses que hayan tenido las grandes potencias y los beneficios que le signifique un cambio de gobierno.

7.3- Neocolonialismo

El comercio mundial depende mayoritariamente de los océanos (el 80 % de las mercancías transitan por mar). Una de las principales bases estratégicas de Estados Unidos es la Armada, siendo este país (por escándalo) la principal potencia naval, contando ya a finales de 2018 con once de los doce portaaviones de propulsión nuclear del mundo y con más de setenta submarinos de propulsión nuclear.

El continente africano es una gran fuente de recursos naturales (petróleo, gas natural, uranio, diamante, oro, etc.), lo que lleva a ser codiciado por grandes potencias (principalmente, China, Francia y Reino Unido) y empresas multinacionales, a la vez que posee muy altos índices de pobreza y subdesarrollo, acompañados de violentas guerras y corrupción. Se trata de un proceso neocolonizador, en varios casos tan perjudicial como lo fue su colonización en tiempos anteriores a la Primera Guerra Mundial, donde las potencias se siguen haciendo con los recursos de sus antiguas colonias a raíz de acuerdos con dirigentes corruptos.

Otras regiones en disputa son el Ártico y la Antártida que, a raíz del calentamiento global y el consecuente deshielo, comienzan a ser más factibles de explorar y explotar, además de abrirse nuevas rutas marítimas que podrían abaratar costos. Se estima que el Ártico tiene grandes reservas de petróleo, gas natural y diversos minerales, además de una importante fauna. Por su parte, el continente antártico tiene la mayor reserva de agua

dulce del planeta, además de importantes recursos minerales (plata, cobre, hierro, etc.).

7.4- Estrategias en el ciberespacio

Para Baños, se vive en un estado de guerra permanente, donde ahora el ciberespacio es un nuevo escenario de confrontación y resultan claves los servicios de inteligencia (públicos y privados), la diplomacia y los medios de comunicación (la manipulación mediática).

Rusia se ha convertido en un experto en campañas de ciberespionaje entre Estados desde fines del siglo XX. Comenta Baños que los agentes de inteligencia rusos se encargan de hackear determinados objetivos, obtener de ellos información clasificada y comprometedora y luego filtrarlas, a través de maniobras que garanticen que no queden rastros de que ellos fueron los autores materiales, a organizaciones o sitios que revelan filtraciones sin delatar las fuentes, como WikiLeaks.

Dentro del contexto de pugnas y rivalidades, una de las estrategias empleadas es la utilización de operaciones de falsa bandera, responsabilizando a un tercero (país u organización) de una acción encubierta. El objetivo con esta estrategia es culpar a un determinado enemigo (o simplemente a alguien al azar) de dicha acción realizada, o bien culpar a alguien cualquiera para intentar mostrarlo como rival de otro y, así, intentar traer a este último como aliado o para que entre ambos se desgasten mutuamente. Estas acciones mencionadas no hacen referencia solamente al espacio físico, sino que cada vez es más frecuente en los sistemas de comunicaciones y en el ciberespacio (sabotaje de sistemas eléctricos, ciberataques, espionaje, etc.), de las cuales se darán ejemplos más adelante. Habitualmente, por tratarse de operaciones encubiertas, suelen ser llevadas a cabo por personal calificado de servicios de inteligencia.

Para que la operación de falsa bandera tenga éxito es clave que sea ampliamente divulgada, tanto en los países afectados como en el mundo en general, tergiversando tanto como se pueda la realidad. Por lo cual, es habitual que se recurra a la manipulación de las masas a través de los

medios de comunicación, haciendo un montaje teatral, mediante un relato ambiguo con mezcla realidad y ficción, que derribe las defensas mentales y siembre en el pueblo un gran odio hacia el enemigo. Como indica Baños:

> *"No hay que olvidar que la mente humana es manipulable por varias razones: tiende a creerse lo que desea o aquello que concuerda con sus ideas preconcebidas (ya sean inculcadas intencionadamente o bien fruto de la idiosincrasia de la comunidad en la que se vive); en ella calan los mensajes simples pero insistentes; y necesita ver despejadas las dudas que la intranquilizan".*

En definitiva, para intentar "encarrilar" a un país que se muestre rebelde a los intereses de una potencia, esta última emplea sus servicios de inteligencia y efectúa sus campañas de guerra psicológica. Pero, además, dispone de ONGs y fundaciones para desestabilizar y derribar a gobiernos que se han atrevido a hacerle frente. Uno de los principales métodos consiste en aprovechar y magnificar algunos descontentos internos (que ocurren en todos los países) para fomentar la creación de movimientos que den la impresión de ser espontáneos y no manipulados desde el exterior. De conseguirse el cambio de gobierno hacia uno más manipulable por la potencia, el éxito se habrá conseguido.

7.5- Secretismo y filtraciones

En una entrevista con Rafael Correa [104], Edward Snowden sostuvo que cuando en algunos países no es posible meter en prisión a periodistas, la forma de disciplinar a los medios es a través del acceso. Existen gobiernos y empresas muy poderosas, de quienes los ciudadanos tienen derecho a conocer sus actividades por el nivel de influencia que tienen en sus vidas, que niegan el acceso a aquellos periodistas críticos, abusando del secretismo. Y la única alternativa es la filtración de información por parte de informantes que logran acceso a ellas (muchas veces de manera ilegal), la cual es criticada por dichos gobiernos y empresas cuando suceden. Afirmó también que, a veces, la única decisión moral que puede tomar un individuo es violar la ley para dar a conocer la verdad a la población: revelar cuando los gobiernos y empresas cometen delitos.

Sobre Julian Assange y WikiLeaks comentó lo siguiente:

> *"Julian Assange es un editor acusado por violar las leyes de Estados Unidos sin ser ciudadano estadounidense, habiendo publicado información veraz (recibida de una fuente anónima) que la prensa considera de interés público, verdades que merecíamos y que nos hacía falta saber. El New York Times ha publicado material secreto del gobierno de China sobre abusos de derechos humanos, y, según las leyes de China esto es un delito. ¿Acaso Estados Unidos va a entregar a China a los periodistas del New York Times que divulgaron esta información? […] Lo que paso con Julian Assange representa una gran amenaza para el periodismo y la libertad de expresión. Estados Unidos, quien fue uno de los principales promotores de la Declaración Universal de los Derechos Humanos (que, entre otras cosas, garantiza el derecho a solicitar y gozar de asilo político), es uno de los países que más ha atacado el derecho de protección que representa el asilo político"*[30].

Por otra parte, el ex analista de la CIA y la NSA sostuvo que en Estados Unidos, en Rusia y en distintos países del mundo hay un aumento del autoritarismo en gobiernos que cada vez adquieren más poder, expandiendo su influencia en los medios, en todas las herramientas de comunicación y en Internet. Algunas historias incómodas son calificadas con fake news y la revelación de hechos veraces que son imprescindibles conocer se califica como delito.

7.6- Principales agencias de inteligencia del mundo

Estados Unidos ocupa a nivel mundial el primer puesto en servicios de inteligencia, contando con 16 agencias (17 si se incluye el Centro Nacional de Contraterrorismo). Las más conocidas son la CIA, la NSA y el FBI.

[30] El 11 de abril de 2019, el presidente de Ecuador, Lenin Moreno, le quitó a Assange el asilo político que este tenía desde 2012, con el cual residía en la embajada ecuatoriana en Londres por considerar que su vida corría peligro ante una hipotética extradición a Estados Unidos. Inmediatamente, Assange es detenido por las autoridades británicas en dicha embajada, en respuesta a la petición de extradición del gobierno estadounidense.

El GCHQ es uno de los tres servicios de inteligencia con los que cuenta el Reino Unido, los otros dos son el MI5 (para la inteligencia interior) y el MI6 (para la inteligencia exterior).

Rusia es probablemente uno de los países que mayores capacidades humanas tiene para el espionaje, contando con numerosos espías y soplones que tienen acceso a información clasificada en diferentes partes del mundo, además de su principal agencia de inteligencia, la FSB (Servicio Federal de Seguridad), dedicada a la inteligencia interior y contrainteligencia, y la SRV (Servicio de Inteligencia Exterior), ambas surgidas a partir de la división de la antigua agencia rusa KGB. Además de la FSB y de la SRV, Rusia cuenta con otras siete agencias que terminan de componer el organigrama de su comunidad de inteligencia.

En China, tanto la inteligencia exterior como la seguridad interior están a cargo del Ministerio de Seguridad del Estado de China (MSS), el máximo organismo de la inteligencia nacional. Este servicio de inteligencia es muy desconocido.

El país más pequeño del mundo, el Vaticano, dispone de uno de los servicios de inteligencia más respetados del mundo, el cual, actuando conjuntamente con la diplomacia vaticana, le permite ser uno de los países mejor informados del mundo.

7.7- Avances tecnológicos en la inteligencia de Estados Unidos

La CIA, principalmente a través de su Directorio de Ciencia y Tecnología, promueve y lleva a cabo proyectos e investigaciones de altísima relevancia en materia tecnológica. Por ejemplo, en los años sesenta desarrolló la batería de litio (muy utilizada actualmente en dispositivos móviles), especialmente para solucionar el problema de la durabilidad de las baterías de los equipos de vigilancia ubicados en los satélites. A su vez, colaboró en el desarrollo de Internet, que se originó con el proyecto ARPANET a finales de los años sesenta. En los últimos años, la agencia ha puesto foco en el ámbito de los drones, aviones espía y satélites.

Debido a todo esto, tanto la CIA como el Departamento de Defensa de Estados Unidos mantienen acuerdos de colaboración con prestigiosos centros de investigación, como el Instituto Tecnológico de Massachusetts (MIT).

Con una vocación similar a DARPA, IARPA (Actividad de Proyectos de Investigación Avanzados de Inteligencia) es otra entidad norteamericana, creada en 2006 y especializada en realizar investigaciones y desarrollar programas para enfrentar los temas más desafiantes para la comunidad de inteligencia y espionaje estadounidense, como lo son: el procesamiento del lenguaje natural, el machine learning, el reconocimiento por biometría o por acciones humanas, la neurociencia, el mapeo de actividad cerebral humana, el big data, la ciberseguridad e inteligencia de amenazas, el procesamiento de imágenes satelitales, la biotecnología y bioinformática, la nanotecnología, la electrónica con superconductores y los sistemas cuánticos.

7.8- Dominio tecnológico y espacial

Desde hace algunos años, tanto Estados Unidos como el resto de las grandes potencias mundiales están haciendo hincapié en la enseñanza y aplicación de la ciencia, la tecnología, la ingeniería y la innovación, considerándolas fundamentales para el crecimiento económico y la seguridad. Por lo tanto, aquellos países que no inviertan a mediano o largo plazo en es estos sectores y que no busquen nichos en los que destacarse serán dominados tecnológicamente por aquellas potencias más avanzadas.

Además de esta dominación del ciberespacio, hoy también resulta fundamental el dominio del espacio. Desde la década del sesenta, Estados Unidos y la Unión Soviética compitieron por el dominio espacial. Esta carrera espacial entre estas potencias durante la Guerra Fría se desinfló a finales de los años setenta, habiendo conseguido ya la llegada a la luna, por la pérdida de interés del público y por los altos costos que implicaban las misiones espaciales.

La exploración espacial ha continuado avanzando, aunque a un ritmo menor. A Estados Unidos y Rusia se ha sumado la Agencia Espacial Europea (ESA), con ambiciosos proyectos tanto dentro como fuera del Sistema Solar.

Por su parte, China, si bien recién logró enviar astronautas al espacio en 2003, ya en 2016 estableció su segunda base espacial (Tiangong-2) y tiene entre sus planes enviar misiones espaciales a la Luna y a Marte (en el planeta rojo existe abundante cantidad de agua, algo que, en principio, augura la posibilidad de albergar vida humana). A su vez, en 2017, China lanzó el primer satélite de comunicación cuántica (Micius), mediante la distribución de claves cuánticas (QKD, por sus siglas en inglés) a través del uso de bits cuánticos (qubits) [105], lo cual permite una comunicación resistente a hackeos, por las propiedades de dichos bits cuánticos. Un bit tradicional puede tomar el valor 0 o 1, en cambio un qubit, por el principio de la superposición cuántica, puede valer 0 y 1 simultáneamente. Esta superposición permite ejecutar más de un cómputo a la vez, aumentando notoriamente el poder computacional.

Entre las razones de la rivalidad por el dominio espacial se encuentran la colonización espacial (ya sea para la extracción de recursos o para la búsqueda de asentamiento humano), la militarización del espacio (como una demostración de fuerza por parte de las potencias o para desplegar armas en el espacio y usarlas contra objetivos en el espacio o terrestres), el control de los satélites de comunicación (por ejemplo, China posee su sistema de navegación por satélite llamado Beidou con el que pretende destronar al Sistema de Posicionamiento Global –GPS- estadounidense [106]) y el perfeccionamiento de la inteligencia de señales (tomar fotografías de objetivos, realizar ciberataques, guiar unidades navales, terrestres o aéreas).

7.9- Satélites espía

Los sistemas de vigilancia por satélite están en manos de unas pocas empresas que trabajan para distintos gobiernos, registrando lo que pasa con la producción agrícola y ganadera, la extracción de recursos naturales, la actividad industrial, el transporte marítimo (de productos o personas), etc. La información recolectada le sirve a determinados gobiernos o empresas, por ejemplo, para predecir esperanza de ventas, calcular reservas de petróleo de países, determinar cuántas toneladas de granos se van a cosechar en la

temporada, vigilar cumplimiento de medidas por parte de los agricultores o localizar embarcaciones (por más pequeñas que sean). [33]

7.10- Guerra militar

Hoy en día el enfrenamiento militar de antaño ha disminuido a una mínima expresión. Una de las principales razones es el rechazo que genera en los países más desarrollados el hecho de tener que lamentar víctimas propias (sobre todo en intervenciones injustificadas). Otra razón es el riesgo de destrucción mutua que significa que se enfrente dos potencias nucleares. De esta forma, los conflictos armados de la actualidad se limitan a batallas en escenarios ajenos y a través de operaciones de fuerzas de operaciones especiales y drones de combate.

Las armas de destrucción masiva no solo son las nucleares sino también, e igualmente preocupantes, pueden ser radiológicas (irradian material radiactivo), biológicas (basadas en bacterias, virus, hongos o toxinas vivientes) o químicas (algunas sustancias químicas industriales tienen una elevada toxicidad). De aquí que las armas de destrucción masiva (ADM) se conocen como NRBQ, generando todas ellas en los seres vivos efectos amplios, devastadores, indiscriminados y duraderos.

Los avances en robótica militar también representan una gran amenaza, pudiendo generar desastres para la humanidad. Conocidos como Sistemas de Armas Autónomos Letales (LAWS), estos "soldados robots" nunca sentirían compasión por las personas y tampoco son responsables por sus acciones (ni se tiene en claro quién debe ser el culpable de éstas, si el fabricante, el desarrollador o quién los utilice). El Mando de Formación y Doctrina del Ejército de Estados Unidos (TRADOC) considera que para 2035 podrán realizarse acciones de combate de forma autónoma. Los países más avanzados y que más investigaciones tienen en esta temática son Estados Unidos, Rusia, China e Israel. En la Imagen 19 se puede ver el robot armado Maars, creado en 2008, cuyo primer ejemplar fue adquirido por Estados Unidos.

Imagen 19 - Robot Maars
Fuente:
https://www.army.mil/article/11592/robots_can_stand_in_for_soldiers_during_risky_missions

En los últimos años, los presupuestos en Defensa de los países europeos han disminuido, mientras que el de Estados Unidos no ha dejado de crecer. Por esta razón, Estados Unidos presiona a sus aliados de la OTAN para que aumenten sus inversiones en Defensa si pretender continuar bajo su paraguas protector, ya que es la Casa Blanca la que está haciendo los mayores esfuerzos económicos al respecto.

7.11- Guerra económica

Los conflictos armados han pasado a un segundo plano y lo que ha ido tomando mayor relevancia es la "guerra" económica. En este sentido, Baños menciona:

> *"En la actualidad, ante problemas geopolíticos se imponen sanciones económicas, se congelan activos, se grava con aranceles, se deniega la posibilidad de comerciar en dólares, se emplean las divisas como arma, se manipulan las finanzas mundiales, se impide negociar en los mercados internacionales o se embargan cuentas bancarias en el extranjero".*

Esta guerra económica se libra entre Estados, organizaciones o empresas, quienes buscan el control de los mercados, la anulación de la competencia y la supremacía tecnológica.

La rivalidad económico-tecnológica entre Estados Unidos y Europa viene desde hace tiempo. Sin embargo, muchos coinciden que para que Europa pueda hacerle frente a Washington necesita normalizar las relaciones con Rusia (logrando un ejército común, servicios de inteligencia unificados y sólidos instrumentos financieros), algo que la Casa Blanca buscará evitar a toda costa. En 2018, miembros de los gobiernos de Francia y Alemania han manifestado su interés de que Europa tome medidas que le permitan evitar ser víctimas de las sanciones económicas que aplica el gobierno de Donald Trump y lograr la autonomía europea.

Las grandes empresas también ejercen influencia en la política y economía de los países donde se instalan o pretenden instalarse. Esta influencia viene dada por el lugar dónde pague impuestos, por los sentimientos nacionalistas de sus dueños (es probable que favorezcan a su país de origen o a quien les haya prestado ayuda) y por las formas en que estas empresas sean utilizadas por los gobiernos para penetrar en países de interés (vía negocios) e influir en la sociedad. Otras veces, son las propias empresas quienes influyen sobre la política, en la economía o en los medios de comunicación. Enormes empresas monopólicas como Bayer, que compró a la empresa Monsanto en 2018 (logrando así el control de toda la cadena de producción agrícola), pueden fijar precios a su gusto y eliminar a la competencia, además de influir en las políticas nacionales para que se ajusten a sus intereses, y enfrentarse a gobiernos en caso de que le presenten obstáculos. A su vez, se han observado numerables casos donde se pone de manifiesto la conexión entre la política y las grandes empresas, donde estas últimas incorporan ex políticos a sus filas, o bien gobiernos que llevan directores de empresas como ministros (pudiendo tener intereses de los dos lados del mostrador). No deberían ser admisibles traspasos entre gobiernos y empresas cuyas actividades dependan de las regulaciones del Gobierno.

Desde hace varios años, el precio del barril de petróleo es determinante para la economía de algunos países (Venezuela, Rusia, Arabia Saudita, Irak, Irán, entre otros). Estados Unidos tiene la capacidad de influir de modo más o menos directo en el precio del crudo, además de poder manipular el precio del dólar respecto a otras monedas (teniendo en cuenta que aproximadamente el 80% de las transacciones comerciales a nivel mundial

se hacen en esta divisa). Varios países, entre ellos, Libia, Irak, Irán, Venezuela, han intentado utilizar monedas alternativas al dólar para determinadas actividades comerciales (por ejemplo, en transacciones vinculadas al comercio del petróleo) o como moneda común en determinadas regiones geográficas, convirtiéndose en objetivos a combatir por parte de una Casa Blanca, que bajo ningún punto de vista querrá permitir que esto suceda. Y algo similar sucederá con las monedas virtuales que, dado su creciente relevancia, encontrarán trabas para emplearse en actividades comerciales internacionales de gran envergadura.

La prospectiva indica que, a partir del imparable aumento mundial del consumo de gas, la demanda global de gas natural de esquisto para 2035 superará a la de petróleo y carbón juntos. Después de China y Estados Unidos, se estima que Argentina y México disponen de los mayores yacimientos, por lo que estarán en la mira de las potencias. Sin embargo, las cada vez más implementadas energías renovables (como la eólica y la solar) podrían hacer disminuir los intereses geopolíticos sobre los países con fuentes fósiles y concentrarse en incrementar los esfuerzos tecnológicos para explotarlas (ya que, prácticamente, no conocen de límites geográficos).

Un instrumento adicional que tiene Estados Unidos para aumentar su poder son el Banco Mundial (BM) y el Fondo Monetario Internacional (FMI), creadas ambas en Estados Unidos en 1944 (y con sede en Washington), año a partir del cual la moneda norteamericana pasó a ser a moneda de referencia internacional, y sobre los cuales Estados Unidos es el único país con poder de veto. El BM, cuya misión es dar financiación a los países en desarrollo para reducir la pobreza, es fuertemente controlado por Estados Unidos, siempre tuvo un presidente norteamericano (propuesto desde la Casa Blanca) y, más allá de que sus directivos estén o no de acuerdo con las posiciones del gobierno de Estados Unidos, en varias ocasiones han sido influidos por la superpotencia a actuar en favor de sus intereses (incluso hasta pasando por alto sus propios reglamentos).

A su vez, el FMI, cuyo su subdirector es, por norma, estadounidense, es muy criticado por las exigencias de aplicación de políticas neoliberales a las naciones para la concesión de préstamos (basadas en los intereses de la Casa Blanca), las cuales apuntan a liberalizar la economía y a reducir el

déficit y el gasto público. Según muchos expertos, esto fomenta el aumento de la brecha entre países ricos y pobres.

7.12- Guerra híbrida

Actualmente, y debido principalmente al mayor nivel de conciencia social de lo que significa un enfrentamiento armado a grandes escalas, las guerras que se presentan son más bien híbridas. Las principales "armas" son los instrumentos económicos-financieros combinados con guerra de información y propaganda para incidir en decisiones de otros países para que estas resulten favorables (operaciones psicológicas de las que participan servicios de inteligencia, embajadas y medios de comunicación), ciberataques, terrorismo, acciones criminales e incentivos para provocar desórdenes civiles y confrontaciones localizadas.

Uno de los objetivos de la guerra hibrida suele ser la injerencia en procesos electorales, como lo intentó hacer el grupo ruso de hackers CyberBerkut en las elecciones de Ucrania en 2014 (de hecho, este enfrentamiento entre Rusia y Ucrania se convirtió en el paradigma de la guerra híbrida).

Este nuevo tipo de guerra permite que las partes enfrentadas, por más que haya una desproporcionada superioridad de una de ellas, nivelen sus posibilidades.

Cuanto más digitalizado sea un país, probablemente sea más eficiente, pero será más vulnerable a los efectos de las guerras híbridas (y cada vez más, debido a los avances tecnológicos de la SIGINT y el espionaje). Un ejemplo es lo ocurrido en 2007 en Estonia, el país más digital del mundo, donde el 99% de los trámites se realizan de manera online. Ese año, una multitud de servidores del gobierno, bancos y otras entidades del país báltico sufrieron un ataque de Denegación de Servicio Distribuida[31], de forma que ni los cajeros, bancos, historiales clínicos, planes de vuelo, comunicaciones y otros servicios quedaron disponibles para los ciudadanos durante aproximadamente dos semanas, generando una parálisis total del país.

[31] También conocida como DDoS, una Denegación de Servicio Distribuida consiste en saturar de tráfico los servidores mediante accesos desde ordenadores de distintas partes del mundo, mediante botnets, hasta dejar inaccesibles los servicios para los usuarios legítimos.

Aunque no haya una confirmación, se cree que el gobierno ruso fue responsable de estos ataques. Pero, como sucede habitualmente con los ataques cibernéticos o con las acciones de desinformación realizadas a través del ciberespacio, atrás de ellos hay programas destinados a confundir sobre el origen de las acciones (operaciones de falsa bandera). A su vez, es necesario tener en cuenta que, aunque se detecte que un ataque procede del territorio de un país, esto no significa necesariamente que su gobierno sea responsable.

7.13- Operaciones de Inteligencia y Ciberataques

Muchos casos de espionaje han sido revelados a partir de 2007 por las revelaciones de WikiLeaks y a partir de 2013 con los documentos filtrados por Edward Snowden.

El principal argumento que dan las agencias de inteligencia, en especial la NSA, para justificar el espionaje es la lucha contra el terrorismo, el crimen organizado, el narcotráfico y otros delitos. Sin embargo, tal como lo sugiere el informe Moraes, es más bien una excusa para llevar adelante espionajes con fines políticos y económicos. [10]

Como parte del trabajo de las agencias de los Cinco Ojos está el espionaje a presidentes, a sectores estratégicos y a administradores de sistemas. [11]

El espionaje más frecuentemente aplicado es el económico-industrial. No solo las empresas de un mismo país o de distintos países se espían, sino que también este espionaje lo llevan a cabo los Estados. El objetivo es obtener ventajas competitivas, ya que, al conocer las necesidades y prácticas que tienen los procesos productivos y financieros de grandes empresas (haciendo un importante hincapié en empresas que fabrican productos de alta tecnología, como biotecnología, smartphones, autos, aviones de combate, trasbordadores espaciales, etc.), pueden ganar mercados al ofrecer las últimas novedades a los consumidores o bien pueden copiar los métodos y fórmulas confidenciales que estas empresas tienen para crear equipos y productos de similar sofisticación y calidad.

En 2009, según WikiLeaks, la embajada de Estados Unidos en Berlín consideraba a Francia el país que más espiaba la tecnología de sus aliados, sobre todo la alemana.

La película “Snowden” de Oliver Stone [107] sostiene que desde la NSA tenían la orden de espiar a líderes políticos del mundo y jefes de las industrias para rastrear acuerdos, escándalos sexuales o cables diplomáticos para que EEUU tenga ventajas en las negociaciones del G8 y para influir en compañías petroleras en Brasil o para acallar algún líder del tercer mundo (como Venezuela y Bolivia) que enfrente las reglas de Estados Unidos.

Una presentación de la agencia de inteligencia canadiense CSE filtrada por Snowden muestra un esquema detallado de las comunicaciones del Ministerio de Minas y Energía de Brasil, incluyendo llamadas telefónicas, correos electrónicos y navegación en Internet. [10]

La red interna de la mayor compañía petrolera de Sudamérica, Petrobras, estuvo bajo la atenta vigilancia de la NSA durante (al menos) el 2012. Son varios los motivos posibles de este espionaje: información sobre nuevas reservas petrolíferas en el mundo, técnicas y tecnologías de extracción, exploraciones de nuevas zonas, localización de depósitos altamente ricos en petróleo, etc.

En 2011 la NSA recolectó información sobre los directivos de la empresa Petróleo de Venezuela (PDVSA).

En 2010, la NSA logró acceso a los servidores de la compañía de telefonía china Huawei, obteniendo información sobre las operaciones de la empresa y controlando las comunicaciones de sus directivos. Sus objetivos eran encontrar vínculos entre la empresa y el Ejército Nacional Chino y conocer cómo explotar la tecnología de Huawei para poder controlar comunicaciones de sus aparatos exportados a diferentes países.

Según informes filtrados por WikiLeaks en 2015, la NSA logró acceso profundo al gobierno japonés y a varias empresas niponas, obteniendo información sensible, como su relación con el gobierno de Estados Unidos y posturas comerciales y políticas vinculadas al cambio climático, a políticas nucleares, a planes de desarrollo, a importaciones agrícolas, etc.

WikiLeaks ha publicado documentos entre 2010 y 2016 donde se aprecia claramente el control que ejerce la NSA sobre varios líderes de la Organización de las Naciones Unidas para obtener información sobre misiones y planes estratégicos (por ejemplo, sobre el cambio climático).

Dentro de dirigentes internacionales de los cuales es de público conocimiento que han sido espiados se destacan los casos de la canciller alemana Angela Merkel, del ex presidente venezolano Hugo Chávez y de la ex presidenta brasileña Dilma Rousseff. Al igual que en el caso japonés, la NSA puede acceder a información altamente sensible y confidencial, tanto política como económica.

La NSA también pone foco en los administradores de sistemas, ya que, si se logra obtener un acceso a los sistemas de una organización con los privilegios que tienen los administradores, se estaría accediendo a toda la información que en ellos se almacena. Para poder vulnerar al equipo al que tiene acceso un administrador, la NSA dispone, por ejemplo, de malware que intenta enviar vía una red social o un servicio de webmail. [11]

En cuanto a la agencia GCHQ, su departamento JTRIG (Grupo de Tareas Contra Amenazas, "Joint Threat Research Intelligence Group" en inglés) llevó a cabo la operación denominada “QUITO” en Argentina. La misma consistió en infiltrar personas haciéndolas pasar por argentinos generando información falsa en redes sociales, foros, o contactándose con periodistas para inclinar la opinión pública a favor de las pretensiones británicas [108]. Además, documentación revelada por Snowden muestra que el GCHQ también mostraba interés en vigilar comunicaciones de líderes y militares argentinos.

En 2016, en una conferencia informal para la Escuela Superior de Ingeniería Centrale Supélec, el ex jefe de SIGINT de la agencia francesa DGSE entre 2006 y 2013, Bernard Barbier, realizó una serie de declaraciones que avalan las revelaciones de Snowden y WikiLeaks. Según Barbier, la DGSE había espiado y realizado ciberataques a numerosos países, incluidos algunos aliados. A su vez, confirmó que la inteligencia norteamericana, desde su embajada en Francia, había logrado intervenir teléfonos celulares de personal del Palacio del Eliseo (sede de la presidencia de Francia) y que en

2012 la NSA había introducido malware en los ordenadores de dicha sede presidencial.

Un informe publicado en 2018 por el Centro Nacional de Contrainteligencia y Seguridad estadounidense (NCSC), detalla operaciones de espionaje llevadas a cabo en los últimos años contra Estados Unidos por parte de sus principales rivales geopolíticos China, Rusia e Irán, entre ellas se encuentran el hackeo de ordenadores, el robo de documentos secretos y la obtención ilegal de propiedad intelectual.

Sin embargo, Estados Unidos ha sido el país que más agresivamente ha utilizado el espionaje económico, tanto a enemigos como a aliados, principalmente a través de Echelon.

Según archivos develados por WikiLeaks en 2015, Estados Unidos espió al menos desde 2006 hasta mayo de 2012 a quienes fueron presidente de Francia en esos años: Jacques Chirac, Nicolás Sarkozy y François Hollande, y a sus colaboradores más cercanos. Este espionaje se llevó a cabo a través del sistema SCS que la NSA y la CIA tienen en la embajada de Estados Unidos en París (también lo tiene en otras embajadas alrededor del mundo).

En febrero de 2017, otras revelaciones de WikiLeaks demostraron que la CIA había estado espiando a los principales candidatos a presidente de Francia de las elecciones del 2012, para saber cómo interactuaban con sus asesores y con los demás candidatos, el apoyo que recibían de las élites económicas, su visión sobre Estados Unidos, y demás posturas geopolíticas.

A comienzos de 2018, la Cámara de Representantes de Estados Unidos, con pleno apoyo del presidente Trump, aprobó extender por seis años más la facultad de la NSA para el espionaje masivo de extranjeros fuera del territorio norteamericano.

En marzo de 2017, WikiLeaks reveló varios proyectos de la CIA para infectar firmware de dispositivos Apple con malware que persistiera incluso a reinstalaciones del sistema operativo. Pocos días después, WikiLeaks develó un programa secreto de la CIA, denominado Marble, cuyo objetivo consistía en impedir que investigaciones forenses pudieran atribuirle virus, troyanos y ataques cibernéticos a la agencia norteamericana, por ejemplo, empleando el idioma ruso, chino o árabe en parte del código fuente del malware (operación de falsa bandera).

Diversas filtraciones de WikiLeaks han develado otros programas de CIA para espiar dispositivos en tiempo real de forma remota (a través de sus cámaras integradas), manipular micrófonos, infectar ordenadores (inclusos aquellos supuestamente más seguros), geolocalizar equipos, recopilar información desde dispositivos móviles, controlar la actividad en Internet, etc. En noviembre de 2017, WikiLeaks develó que la CIA había suplantado la identidad de Kaspersky, compañía rusa proveedora de soluciones de seguridad informática, al generar certificados digitales falsos que le permitían hacerse pasar por la compañía rusa y así enmascarar la herramienta Hive, utilizada por la CIA para distribuir malware de forma masiva.

Tal como lo muestra la película “Snowden” de Oliver Stone, Edward Snowden comenta que cuando trabajó para la NSA en Japón no solo establecieron bases para vigilar a la población japonesa, sino también fueron incorporando programas a los sistemas de redes eléctricas, represas, hospitales, etc. La idea era que, si un día Japón dejaba de ser aliado, tenían la capacidad de dejar sin luz a todo el país. También afirma que plantaron malware en México, Alemania, Brasil, Bélgica, China, Rusia, Irán y Venezuela.

Según un artículo del New York Times de junio de 2019 [109], funcionarios estadounidenses reconocieron que, al menos desde 2012, Estados Unidos ha puesto sondas de reconocimiento de los sistemas de control de las redes eléctricas de Rusia, y que en el último tiempo la estrategia se ha vuelto más ofensiva, hasta el punto de insertar malware dentro del sistema ruso, por un lado como advertencia ante los intentos de ciberataques rusos a la infraestructura norteamericana y, por otro, como una potente arma capaz de paralizar dicho sistema eléctrico en caso de un mayor conflicto entre Washington y Moscú.

Este mayor nivel de agresividad en cuanto a las ofensivas cibernéticas ha sido motivado por el presidente Donald Trump, quien otorgó un mayor margen de acción a los organismos de ciberseguridad. Un ciberataque de la inteligencia rusa que a fines de 2015 dejó sin suministro eléctrico por unas horas a cientos de miles de ciudadanos del oeste de Ucrania fue suficiente para que la Casa Blanca comience a tomar este tipo de medidas.

En junio de 2019, en represalia por el derribo de un dron militar estadounidense por parte de agentes iraníes, Donald Trump autorizó iniciar, con la colaboración de Israel, una campaña de ciberataques contra los sistemas informáticos militares y la red de SIGINT de Irán. Sin embargo, los dirigentes del país persa sostuvieron que estos intentos de afectar su infraestructura de inteligencia no tuvieron éxito, y que su país se encuentra preparado para defenderse de ciberataques. [110]

En el mes de junio de 2019, el gobierno iraní anunció el desmantelamiento de una nueva red de espías de la Agencia Central de Inteligencia (CIA) de Estados Unidos en el país del golfo, capturando a algunos de sus espías. [111]

La tensión entre estos dos países se desató en 2018 cuando Estados Unidos se retiró unilateralmente del acuerdo nuclear y comenzó a establecer sanciones económicas a Teherán. Este acuerdo tenía como objetivo justamente limitar la capacidad atómica de Irán a cambio de un levantamiento de las sanciones económicas internacionales contra dicha República Islámica.

7.14- China vs Estados Unidos

Actualmente, China, a pesar de ser todavía oficialmente comunista, ha dejado claro su objetivo de ser el líder de la globalización y el libre comercio. Su principal motor es la capacidad de innovación, y posee la capacidad de inundar los mercados de todo el mundo con diversidad de productos (desde manufacturas hasta tecnología de punta) a mucho menor costo que lo podrían hacer el resto de los países desarrollados. Esta competencia del gigante asiático lo llevaría, a su vez, a transformarse en un serio rival en materia militar y espacial, y también en el ciberespacio. [76]

Para hacer frente a las corporaciones estadounidenses GAFAM (Google, Apple, Facebook, Amazon y Microsoft) y NATU (Netflix, Airbnb, Tesla y Uber), China ha creado a BAT: Baidu (similar a Google, ofrece como servicios un motor de búsqueda, un servicio de mapas, correo electrónico y hasta coche autónomo), Alibaba (competencia de Amazon para el comercio electrónico, enfocada al e-Commerce y a aspectos tales como Marketplace -

los supermercados digitales-) y Tencent (ofrece servicios de mensajería instantánea y entretenimiento interactivo, además de ser el segundo grupo de e-Commerce más grande de China) [38]. Las plataformas streaming de vídeo como Netflix, HBO y Amazon Prime Video tendrían su competidor chino iQiyi, propiedad de Baidu, y TBO, de Alibaba. En cuanto a Airbnb, China tiene a Xiaohzu como su principal plataforma de alojamientos. En cuanto a coches eléctricos y autónomos, China está muy por detrás de Tesla, pero tiene el objetivo ambicioso de que el 10% de todos los vehículos nuevos vendidos para 2030 sean totalmente autónomos [112]. Por último, China tiene un fuerte competidor de Uber: Didi, el cual opera en más de mil ciudades, muchas de ellas de países de América Latina, como México, Brasil, Chile y Colombia.

Los líderes en China y Estados Unidos ven la tecnología fabricada en el otro país con recelo. También, las autoridades chinas han pedido repetidamente que la tecnología hecha por compañías estadounidenses sea reemplazada por otras producidas localmente. El gigante asiático también ha bloqueado a las principales compañías estadounidenses de Internet para que no ofrezcan productos en el país. [113]

En 2018, la empresa estadounidense AT&T decidió cancelar un acuerdo con Huawei para comercializar los smartphones de la compañía china en Estados Unidos. Se estima que la principal razón obedece a una investigación de la Inteligencia estadounidense que asegura que, tanto Huawei como su competidor ZTE, podrían utilizar su equipamiento de redes para filtrar información desde Estados Unidos al gobierno de China. Esto es algo que nunca tuvo pruebas concretas, aunque se cree que en sus primeros años de existencia Huawei firmó una alianza con el gobierno chino, en la cual Pekín iba a proteger a Huawei de la competencia extranjera y a cambio la compañía de telecomunicaciones se comprometía a compartirle información recolectada y recursos [114]. A su vez, esta razón esgrimida es algo curiosa teniendo en cuenta que durante años la Inteligencia estadounidense ha vigilado a distintos países del mundo, incluyendo a sus aliados [115].

A pesar de esto, Huawei decidió continuar vendiendo nuevos productos en Estados Unidos, aunque sin la enorme red de puntos de venta que dispone de una compañía como AT&T.

Desde marzo de 2018, empezó una guerra comercial entre Estados Unidos y China, con imposición de aranceles a diferentes tipos de productos, en la que ambos países salieron perjudicados, no solo los gobiernos sino también las empresas de ambos rivales.

Cansado del juego de aranceles, en mayo de 2019 el presidente Donald Trump ordenó al Departamento de Comercio que colocara a Huawei en la lista de empresas con las que las compañías estadounidenses tienen prohibido hacer negocios a menos de que cuenten con una licencia. De esta forma, Huawei quedaba sin acceso al hardware (placas de video, microprocesadores, etc.) y software (Android -desarrollado por Google-, Windows, etc.) norteamericano y a los servicios de Google incluidos en Android (Gmail, YouTube, WhatsApp, etc.). Y, a su vez, quedaba imposibilitado de vender sus productos en el país norteamericano. Al poco tiempo, en junio de 2019, esta decisión del bloqueo a Huawei se ha visto "suavizada", ya que Trump decidió que hay determinados productos que las empresas norteamericanas sí pueden vender a Huawei. Sin embargo, los nuevos dispositivos lanzados por la empresa china posteriores al bloqueo no podrán utilizar los servicios de Google, por lo que Huawei debería decidir si usar la versión libre de Android, Android Open Source Project (AOSP), o utilizar un sistema operativo propio (Harmony OS).

Muchos sostienen que Huawei ha sido solo un peón de la guerra comercial entre Estados Unidos y China. Por ejemplo, Juan Elman sostiene que Huawei es la punta de lanza en la estrategia china en la carrera por 5G disputada con Estados Unidos [115]. El 5G, además de ofrecer mucha más velocidad y confiabilidad que su predecesor 4G, requiere una enorme inversión en infraestructura. Huawei es una de las poquísimas empresas que puede ofrecer el equipamiento necesario, junto con la también china ZTE, las europeas Nokia y Ericsson, la surcoreana Samsung y la estadounidense Cisco. Y es la mejor posicionada para ofrecer un equipamiento con alto desarrollo tecnológico, a escala global y a un menor costo.

Es importante destacar que quien tenga el control del 5G va a tener el control de los datos que van a circular por la nueva infraestructura, que serán exponencialmente superiores a la actual. En tiempos del auge del big data y la vigilancia masiva, esto representa una ventaja de suma importancia.

Por último, China, junto con Huawei, ha propuesto en 2020 ante la Unión Internacional de Telecomunicaciones (ITU) de las Naciones Unidas un nuevo protocolo de Internet, llamado New IP, para reemplazar al actual modelo TCP/IP [116]. Huawei afirma que TCP/IP es "inestable e insuficiente" para las necesidades actuales y futuras del mundo digital, por ejemplo, para los autos autónomos. En este sentido, propone que el nuevo protocolo haga más eficientes las conexiones, por ejemplo, permitiendo que los dispositivos dentro de una misma red se comuniquen directamente entre sí sin tener que enviar información a través de Internet.

Países como Estados Unidos, Reino Unido y Suecia han manifestado su preocupación por este nuevo protocolo, argumentando que permitiría a los Estados un control granular sobre el uso de Internet por parte de los ciudadanos. Algo que no parece descabellado teniendo en cuenta el sistema de vigilancia que existe en China.

7.15- Vigilancia en tiempos de pandemia

Tal como lo recuerda Glenn Greenwald en un artículo de The Intercept [117], a los pocos días del 11S Estados Unidos legalizó la vigilancia masiva (mediante la Patriot Act) y el uso de la violencia y la fuerza militar contra cualquiera que Washington considere, unilateralmente, responsable de los atentados, prácticamente sin oposición del Congreso ni de los ciudadanos, que, abrumados por el miedo, aceptan renunciar al derecho de privacidad y libertad. Por eso sostiene Greenwald que las decisiones no deben tomarse en base al miedo sino en base a un debate razonable, ya que las decisiones que se tomen hoy persistirán durante los años venideros. Al respecto, Greenwald afirma:

> "*Es casi inevitable que los poderes que se confieren a las empresas y los gobiernos en nombre de una emergencia temporal terminen*

siendo todo menos temporales. Terminan siendo permanentes, e incluso se expanden en lugar de contraerse, una vez que la crisis original ha terminad. Pienso que el mejor ejemplo son las medidas adoptadas luego del 11S, comenzando por la Patriot Act".

En este mismo artículo de The Intercept, que incluye una entrevista de Greenwald con Snowden, el ex contratista de la CIA compara la propagación de miedo del 11S con la generada por la pandemia del Coronavirus durante 2020, recordando que el miedo es, junto al odio, una de las principales emociones que movilizan la histeria de la gente, principalmente en redes sociales. En el caso del 11S el miedo era por la seguridad nacional y en el caso de la pandemia el bienestar y la salud pública.

Tal como indican Greenwald y Snowden, la pandemia tuvo diferentes respuestas en los distintos países. En países como China y Singapur, donde a su vez existe una cultura de disciplinamiento y obediencia, se aplicó la fuerza bruta para encerrar en sus casas a las personas, y en países occidentales como España e Italia, donde la población suele ser desafiante a los mensajes gubernamentales, se tomaron medidas de forma más tardía. Un caso particular fue el de Corea del Sur, que, evitando la fuerza bruta, manejando la situación mejor que en Europa y aplicando vigilancia masiva en su población para encontrar y aislar a aquellas personas que hayan tenido contacto con ciudadanos infectados, ha conseguido enfrentar de buena forma la pandemia.

Snowden sostiene que esta vigilancia sobre los ciudadanos surcoreanos no se sabe bien cuánto ayudó y que el caso de Corea del Sur es excepcional por varias razones. Una de ellas es su cultura, a partir de la cual cada vez que alguien se resfría, se ponen un barbijo (máscara facial), incluso cuando no existe una pandemia. Otra, muy importante, fue que el público escuchó las recomendaciones de los expertos de las autoridades sanitarias y las puso en práctica. Estas acciones colectivas resultan ser efectivas.

En la misma línea, Marta Peirano afirma:

"Estamos equivocados en darle más valor a las tecnologías que se dedican a vigilar a las personas y no a los virus. Y muchos se remiten a que las han usado con éxito en Corea del Sur o en Singapur para justificar el tipo de seguimiento que debe hacer nuestro Gobierno en

nuestros móviles, a nuestros movimientos, que se registran en las aplicaciones que usamos. Pero, en realidad, el éxito que han tenido países como Corea del Sur o Singapur no ha sido tanto por sus tecnologías como por sus protocolos de emergencias, enormemente efectivos, que desarrollaron después del SARS. Y por eso, en cuanto surgió la primera noticia del brote de un virus parecido, se pusieron en marcha, distribuyeron la gestión de los recursos necesarios, comenzaron a fabricar mascarillas y test como locos". [118]

Snowden sostiene que es incorrecto pensar que la vigilancia masiva es el único tipo de vigilancia que podría ayudar a controlar la expansión de un virus. Indica que lo que se está pidiendo es que la gente acepte que la actividad registrada por sus teléfonos durante los últimos meses o años sea vigilada de forma involuntaria.

Snowden afirma que un tipo de vigilancia donde un ciudadano infectado acepte voluntariamente compartir los datos registrados por su teléfono, sin requerir sacrificios de privacidad ni ningún tipo de violación involuntaria o intrusiva de derechos, puede ser útil y podría crearse en muy pocos días.

Por otra parte, se ha visto a grandes corporaciones tecnológicas, como Facebook, Google y Twitter, censurar determinados contenidos en sus plataformas. Greenwald advierte que, si bien algunos de ellos fueron a usuarios que contradecían a estudios u organizaciones científicas (por ejemplo, la OMS), como Jair Bolsonaro, es importante prestar atención al hecho de que estas empresas pueden decidir lo que está permitido expresar y lo que no.

En línea con este pensamiento, Snowden no cree que deba existir en estas corporaciones una autoridad central que decida lo que puede y lo que no puede decirse. Y piensa que aquellos líderes, como Trump y Bolsonaro, que niegan los hechos y los mensajes de las instituciones más importantes lo hacen como una lucha política por la influencia, abusando de su autoridad y de la confianza de sus votantes para mejorar su suerte en las próximas elecciones. Y comenta que en muchos países se están generando divisiones en lugar de ofrecer seguridad y enfocarse en mejorar la salud pública, el bienestar económico y los derechos humanos.

A la hora de pensar en otorgar poderes a gobiernos y corporaciones para luchar contra una pandemia es crucial ser realista y reconocer es poco probable que los poderes otorgados sean solo temporales.

Sobre el tema, Snowden concluye:

> *"Se ha iniciado una carrera entre todas las crisis que este sistema ha producido y que ahora están trabajando para persuadir a la gente de que tal vez el sistema necesita ser reemplazado y que la gente que se está beneficiando de esos sistemas lo mantenga en su lugar.*
>
> *Las crisis siempre son explotadas por los actores políticos para obtener autoridades que de otra manera les estarían prohibidas. Las consecuencias de la concesión de estas autoridades son inevitables. Nunca ha habido un momento en la historia en el que hayamos creado lo que hoy se pone en pie, un sistema en el que cualquier gobierno pueda conocer la ubicación de cada persona en todo momento. Esta es la arquitectura de la represión. Y esta capacidad existirá en tres meses, en tres años y en 30 años si permitimos que se implemente hoy.*
>
> *[…] Pregúntese por qué, durante décadas, se le ha pedido que dé más y más. Y cuando llega un momento de crisis y el Congreso empieza a tirar dinero, estamos recibiendo la menor parte de los recursos. Y luego piense en lo único que nos queda, nuestros derechos, nuestros ideales, nuestros valores como personas. Eso es por lo que vienen ahora. Eso es lo que nos piden que dejemos. Eso es lo que nos piden que cambiemos. Y recuerden eso desde la perspectiva de una sociedad libre. Un virus es un problema serio, es dañino. Pero la destrucción de nuestros derechos es fatal. Eso es permanente".*

7.16- El abuso de los algoritmos

Un algoritmo es un conjunto de instrucciones diseñadas para resolver un problema concreto. Pero cuando los algoritmos no son públicos ya no se sabe cuál es el problema que intentan resolver. Esto es lo que genera que

las empresas, argumentando que su algoritmo es neutral, aprovechen la buena fe de las personas y cometan abusos dentro del mismo. [33]

Uno de estos abusos es discriminar a los clientes que le resultan menos rentables, es decir, sus clientes con menor nivel de compras, valor que calcula el propio algoritmo. Y el algoritmo está tan entrenado que es prácticamente imposible de vulnerar.

Otro de sus principales abusos es el de los precios dinámicos, que tiene el propósito de calcular cuál es el máximo precio que puede cobrarle a cada cliente. Una forma de obtener este cálculo es gracias a que se tienen muchos datos del cliente, como su historial de compras y su perfil (obtenido, por ejemplo, con la tarjeta de puntos de un comercio). Y los datos que no disponen los pueden comprar a otras empresas que los recolectan (data brokers). Este algoritmo nunca juega a favor del consumidor y es completamente oportunista. Otra forma de calcular el precio dinámico es aprovechándose de las crisis o desastres de emergencia humanitarias, aumentando los precios de vuelos, medicamentos, alimentos u otros productos o servicios de primera necesidad ante el aumento de la demanda.

Otro mal uso de los algoritmos se pueden observar en los juzgados, donde, por ejemplo, se ha probado que en Estados Unidos las personas de color son más severamente penadas que las personas blancas ante un mismo hecho, en vez de juzgar de forma imparcial. También sucede en los sistemas de contratación de recursos humanos, donde, por ejemplo, en 2015 Amazon descubrió que su algoritmo penalizaba curriculums asociados a las mujeres, sus logros y luchas, en vez de valorar únicamente aspectos vinculados al puesto vacante.

Los algoritmos basados en machine learning permiten a las máquinas aprender por sí mismas. Sus decisiones no están programadas, sino que, a partir de un entrenamiento, van detectando patrones que le indican cuál es la decisión más eficiente. Si se aplican estos mismos algoritmos, alimentándolos con la enorme cantidad de datos extraídas de las personas por los gigantes tecnológicos, los data brokers y los Estados, para determinar qué cosas se merecen las personas, se estará construyendo algo muy similar al sistema de crédito social chino, solo que, en este caso, podrá ocultarse a las personas.

8- Posibles contramedidas

8.1- Navegación anónima

TOR (del inglés "The Onion Router") es una red superpuesta a Internet en la que un cliente construye un circuito por medio del protocolo SSL/TLS, el cual permite enviar información a través de Internet de forma cifrada con claves previamente establecidas con cada nodo de la red TOR, agregando así una capa de cifrado para cada punto de enrutamiento (de aquí el nombre de enrutamiento cebolla). Debido a su diseño, TOR logra que cada nodo solo conozca su predecesor y sucesor en este circuito, consiguiendo enviar tráfico a un destino sin exponer su origen.

Tal como indica Chaparro Zúñiga [119], TOR brinda la posibilidad de una navegación anónima sobre una red insegura como Internet a aquellas personas que desean conservar su privacidad a la hora de compartir contenidos, sobre todo en aquellos países en los cuales se persigue y censura a quienes difunden determinado tipo de material. También afirma que Internet “no debe estar absenta de poder garantizar los mismos derechos en cuanto a privacidad y libre expresión que tiene una persona fuera de esta”.

La idea importante detrás del anonimato es que una persona no sea identificable, alcanzable ni rastreable. El enrutamiento de cebolla evita que se sepa quién se está comunicando con quién: la red solo sabe que se está realizando una comunicación. Además, el contenido de la comunicación está oculto a quienes la intercepten hasta que el tráfico salga de la red. TOR resiste tanto las escuchas ilegales como el análisis de tráfico, al separar la identificación del enrutamiento [120].

La navegación vía la red de anonimato TOR también hace más difícil la tarea de espionaje de agencias como la NSA y el GCHQ. Un documento de la NSA revelado por Snowden [121], llamado “Tor Stinks” (Tor apesta), muestra la preocupación de la agencia por la dificultad para des-anonimizar a los usuarios del navegador Tor.

El enrutamiento de cebolla funciona de la siguiente manera [120]: una aplicación, en lugar de hacer una conexión (socket) directamente a una máquina de destino realiza una conexión de socket a un proxy de

enrutamiento de cebolla (Onion Proxy, OP). Ese OP genera una conexión anónima a través de otros enrutadores de cebolla (Onion Routers, OR) hacia el destino (el circuito por el cual se envía la información está construido por, al menos, 3 OR). Cada OR solo puede identificar los a los OR adyacentes a lo largo de la ruta (es decir, el anterior y el próximo). Antes de enviar datos a través de una conexión anónima, el primer OR agrega una capa de cifrado para cada OR en la ruta. A medida que los datos se mueven a través de la conexión anónima, cada OR elimina una capa de cifrado, por lo que finalmente llega un texto plano. Esta estratificación se produce en el orden inverso para que los datos vuelvan al iniciador. Los datos transmitidos a lo largo de la conexión anónima aparecen diferentes en cada OR, por lo tanto, los datos no se pueden rastrear en ruta y los OR comprometidos no pueden cooperar. Cuando se interrumpe la conexión, toda la información sobre la conexión se borra en cada OR.

Los OP de la red Tor no utilizan llaves públicas, ya que su objetivo es que el usuario no sea identificado, y la comunicación entre OP y OR y entre OR y OR es protegida a través de cifrado simétrico con AES.

El navegador Tor, creado por el Proyecto Tor, es una versión de Mozilla Firefox con mejoras en la privacidad. Y, si bien su instalación es simple, los tiempos de respuesta son más lentos.

Tor también permite publicar servicios ocultos, únicamente accesibles desde la red Tor. Estos servicios además de proporcionar anonimato tienen la ventaja práctica de que no requieren de una dirección IP pública. Esto es muy usado por organismos como WikiLeaks para recibir denuncias anónimas desde Internet. Para conocer cómo se realiza la conexión cifrada y autenticada entre un cliente y un servicio oculto Tor ver el trabajo de Rafael Bonifaz [122].

TOR es mantenida por un gran número de personas encargadas de colaborar en su crecimiento, aportando investigaciones sobre posibles fallos, vulnerabilidades, mejoras en el diseño y algoritmos utilizados. Igualmente, representa un desafío para la comunidad científica crear una tecnología que permita garantizar una navegación anónima en una red pública como Internet y, a su vez, lograr que ésta sea lo suficientemente popular como

para que cada vez más personas tengan conocimiento de ella y de la importancia de la privacidad, y la puedan aprovechar. [119]

Por otra parte, el uso de VPN es muy utilizado para acceder a una red corporativa desde una red insegura como Internet. La VPN establece canales de comunicación cifrados, por lo que ni los ISP ni ningún espía pueden conocer el contenido de sus comunicaciones. Sin embargo, el proveedor de la VPN sí tiene acceso a las comunicaciones que realizan sus clientes, por lo cual podrían ser presionados para entregar esa información, y se perdería la privacidad.

Por último, la red I2P (Proyecto de Internet Invisible) tiene una funcionalidad similar que Tor pero difieren en que la primera está pensada solo para tráfico sobre la dark web[32] y no requiere de servidores centralizados. Al ser una estructura descentralizada, todos los nodos de la red pueden reenviar tráfico a otros nodos. A su vez, el camino de ida es diferente al de vuelta, ya que se generan rutas diferentes para el tráfico de entrada y el de salida. Esta configuración de ruteo dificulta aún más el espionaje de las comunicaciones. Pero, el hecho de que no permita acceder a servicios de la clear web contribuye a que sea menos utilizado por los usuarios.

Tal como sostiene Bonifaz "[…] no es suficiente con ocultar el contenido de las comunicaciones, sino que hay que ocultar el hecho de que las mismas ocurrieron" [122], por lo cual es necesario ocultar los metadatos con redes de anonimato y el contenido de las comunicaciones con cifrado extremo a extremo.

8.2- Seguridad en servicios de mensajería

El protocolo Signal (inicialmente, protocolo TextSecure) permite que las llamadas de voz, las videollamadas y los mensajes enviados a través de servicios de mensajería tengan un cifrado extremo a extremo (end-to-end encryption o E2EE). Esto significa que, al ser cifrados los datos enviados por un remitente antes de salir de su dispositivo, solo el equipo del destinatario

[32] La dark web es una mínima parte de la deep web solo accesible mediante navegadores especiales. La deep web abarca aproximadamente el 90% del contenido de la red y no es habitualmente indexada por los buscadores. El restante 10% se conoce como clear web y está formado por el contenido fácil y públicamente accedido por todos los usuarios, siempre indexado por los buscadores.

puede ver el mensaje original, y toda la infraestructura intermedia (routers, servidores de mensajería, bases de datos, etc.) no puede tener acceso al texto en claro.

A pesar de que en 2016 implementó el protocolo Signal, WhatsApp, además de ser el servicio de mensajería instantánea más ampliamente utilizado, es muy inseguro. Más allá de pertenecer a Facebook, empresa envuelta en numerosas acusaciones por no proteger los datos de sus usuarios, WhatsApp ha tenido muchas vulnerabilidades. Por ejemplo, en octubre de 2019, WhatsApp demandó a NSO Group por instalar un spyware en teléfonos de activistas, abogados, periodistas, religiosos y académicos aprovechando una vulnerabilidad en las llamadas de voz, que luego fue parcheada en una actualización posterior de la aplicación. Fueron hackeados un total de 1400 usuarios en veinte países diferentes durante un período de 14 días desde finales de abril hasta mediados de mayo de ese mismo año [123].

Desde junio de 2019, los altos funcionarios de las Naciones Unidas tienen prohibido usar el servicio de mensajería WhatsApp, ya que la organización no lo considera seguro. [124]

El servicio de mensajería Telegram no implementa un cifrado de extremo a extremo por defecto en sus conversaciones, sino que el usuario debe elegir la opción de “chat secreto” para obtenerlo. Telegram usa su propio cifrado de extremo a extremo, llamado MTProto (Mobile Transport Protocol). Al igual que WhatsApp, Telegram requiere enlazar la cuenta del usuario al número de teléfono, lo cual representa un problema para el anonimato, ya que, en muchos países las operadoras telefónicas exigen el número de documento al cliente que adquiere el servicio. Por otro lado, Telegram tiene la ventaja de permitir, mediante un alias, que las personas se comuniquen sin necesidad de dar a conocer su número de teléfono.

Telegram, aunque en mucho menor medida que WhatsApp, también ha tenido fallas de seguridad. Un ejemplo es la detectada en 2018 en su versión de escritorio (Telegram Desktop), con la cual se podía acceder a las bases de datos de la aplicación de un usuario, ya que los datos que se almacenan en éstas (incluso los provenientes de los “chats secretos”) se guardaban sin cifrar [125].

Los mensajes de Telegram se almacenan en la nube (de forma similar a WhatsApp). Según investigadores del Instituto Tecnológico de Massachusetts (MIT), esto permite que los mensajes (encriptados en el caso de los chats secretos, y sin cifrar en el caso de chats convencionales) y sus metadatos estén accesibles para gobiernos o hackers que obtengan control de sus sistemas, o que estén disponibles para venderlos a otras empresas. [126]

A su vez, el estudio del MIT indica que MTProto, a diferencia del protocolo Signal, carece de acceso para ser auditado y analizado por criptógrafos externos. El protocolo Signal, creado en 2013 por la organización Open Whisper Systems para su servicio de mensajería TextSecure (que después se convirtió en Signal), es el más recomendado por los expertos ya que está abierto para ser auditado y es ampliamente conocido.

Edward Snowden, si bien reconoce que son más seguras que el uso de los SMS, desaconseja el uso de las aplicaciones WhatsApp y Telegram debido a que no sirven a la seguridad pública y ponen en riesgo la privacidad. [127]

El ex contratista de la NSA sí ha recomendado, en más de una oportunidad, el uso de Signal. Esta aplicación añade una capa más de seguridad debido a que es Open Source, por lo cual su código está abierto para que sea auditado por la comunidad en busca de vulnerabilidades. Por otra parte, permite realizar configuraciones para que los mensajes se autodestruyan luego de un cierto período de tiempo. Como desventaja, además de ser un servicio centralizado, tiene el hecho de que, al igual que WhatsApp, también requiere asociar el número de teléfono a la cuenta.

Tanto WhatsApp como Telegram y Signal, y cualquier empresa que provea servicios de mensajería de forma centralizada y tenga acceso a los mensajes de sus usuarios, puede revisar los metadatos de las comunicaciones, aunque el contenido de la conversación esté cifrado. Los metadatos pueden llegar a revelar hasta más información que el propio contenido de las conversaciones.

Si bien todas las aplicaciones de mensajería instantánea pueden tener vulnerabilidades, es fundamental que implementen medidas de seguridad para disminuir los riesgos. El cifrado extremo a extremo por defecto, el código fuente disponible para que sea auditado por la comunidad, el

almacenamiento cifrado de los mensajes fuera de servidores centralizados, la posibilidad de destruir los mensajes, el empleo de técnicas criptográficas seguras, el hecho de no tener que vincular un número de teléfono al servicio y el uso diferentes factores de autenticación son características deseables para que este tipo de servicios conserven la privacidad y el anonimato.

8.3- Seguridad en correo electrónico

Para proteger la información entre servidores y clientes de correo electrónico se utilizan protocolos como TLS. Los principales servidores de webmail, como Gmail, lo implementan. Sin embargo, los administradores de los servidores de webmail tienen acceso a los mails sin cifrar. De hecho, analizan el contenido de los mails, por ejemplo, para detectar spam o phishing, para sugerir respuestas automáticas o venderlo para que el usuario reciba publicidad orientada a sus intereses (Gmail anunció en junio de 2017 que ya no permitiría más anuncios publicitarios personalizados). A su vez, el ISP correspondiente puede ver a sus clientes comunicándose por webmail.

Para lograr anonimato y confidencialidad en la comunicación por correo electrónico es necesario combinar el uso de un navegador como Tor, que garantice el anonimato en la navegación, junto a un cifrado extremo a extremo. De esta forma, el administrador del servidor de webmail no podrá ver el contenido de los mensajes ni conocer quiénes se están comunicando. Y el ISP solo sabrá que sus usuarios están usando Tor, pero no sabrán para qué.

S/MIME (estándar Secure Multipurpose Internet Mail Extensions) y OpenPGP (estándar del protocolo PGP -Pretty Good Privacy-) son dos estándares que permiten realizar un cifrado extremo a extremo sobre correos electrónicos. Ambos se parecen en el hecho de que utilizan criptografía asimétrica para cifrar y descifrar mensajes y para firmar los correos. Sin embargo, S/MIME utiliza una Autoridad Certificante (CA) para autenticar usuarios, con lo que se pierde la posibilidad de anonimato.

OpenPGP se basa en una red de confianza[33] para lograr la autenticación, lo que puede exponer las redes de relaciones de los usuarios ante terceros desconocidos (por exposición de los metadatos). Tal como sostiene Bonifaz [122], se deberían validar las claves públicas solo de forma manual y entre las personas que desean establecer la comunicación.

Por otra parte, en el envío de correos electrónicos es importante, en comunicaciones públicas, la firma digital de los mismos, para garantizar el no repudio. Sin embargo, esto va en contra del objetivo de lograr comunicaciones secretas, ya que la firma identifica unívocamente al emisor. Este es un problema que puede resolverse mediante el uso de seudónimos en vez de nombres reales. Usando seudónimos se logra ocultar los nombres reales, mediante el uso de Tor se oculta la ubicación geográfica y mediante PGP se cifra el contenido del mail (el asunto, por lo general, no es cifrado, por lo que sería conveniente rellenarlo con caracteres sin sentido).

8.3.1- Correo electrónico seguro: el caso de Lavabit

Ladar Levison, creador de Lavabit, un servicio de correo electrónico encriptado que utilizaba Snowden, comentó en el Parlamento Europeo en septiembre de 2013:

> *"Lavabit estaba diseñado para impedirme violar la privacidad de un usuario en caso de verme obligado a espiarlo, eliminándome como proveedor del servicio de la ecuación, al no guardar registros de los usuarios en servidores. Al conocer esto, el FBI me exigió que le otorgara las claves SSL (utilizadas para cifrar los mensajes) para que pudieran recolectar las comunicaciones y así poder descifrarlas […] Por esto, mi única opción ética fue cerrar el servicio"*. [7]

8.4- Seguridad en el almacenamiento y transferencia de datos

OnionShare es una herramienta de código abierto[34] para compartir archivos de forma anónima y sin intermediarios. Para lograrlo, un usuario que desee

---

[33] En una red de confianza los usuarios autentican a otros usuarios (firman con su llave privada la llave publica del usuario) en caso de que confíen en ellos (por haberlos conocido antes), para que un tercero que nos los conoce pueda confiar en que ellos son quienes dicen ser y así poder comunicarse con éstos.

[34] https://github.com/micahflee/onionshare

compartir sus archivos debe levantar un servicio Onion de la red Tor, accesible temporalmente desde una URL ".onion", que debe ser compartida con los destinatarios para que puedan acceder al sitio y descargar los archivos. Por defecto, una vez que los archivos se terminan de compartir, la dirección ".onion" desaparece por completo de Internet, ya que estas direcciones están destinadas a un solo uso. Esta configuración se puede cambiar si se desea compartir los archivos con más de una persona. OnionShare está disponible para Windows, Mac y Linux.

Nextcloud es un servicio de código abierto[35] para almacenamiento en una nube controlada por el propio usuario, sin alojarlo en los servidores de un tercero. Nextcloud provee el software de servidor, que se puede implementar de manera local (doméstica o empresarial) o hostear en un tercero de confianza, y el software cliente con el cual acceder al servidor.

Tanto OnionShare como Nextcloud se tratan solo de dos ejemplos para compartir y almacenar información, que permiten hacerlo de forma anónima y sin exponerse al espionaje de datos y metadatos.

8.5- Redes descentralizadas

Tal como menciona Elías Rodríguez García [128], una oportunidad para hacer frente al fin de la neutralidad de la red es la creación de una gran red descentralizada. Una Internet descentralizada consistiría en quitar a los nodos que centralizan las conexiones, es decir, a los ISP (que reciben y retransmiten todas las conexiones de sus clientes), los cuales, ante una ley que se los permita (como ocurrió en Estados Unidos luego de que Trump derogó las normas de neutralidad de la red a fines de 2017), podrían favorecer o perjudicar determinados servicios o conexiones según sus necesidades.

Quitando a los ISP, lo que proponen quienes promueven un Internet descentralizado es que los routers de los usuarios se conecten directamente entre ellos (una red P2P), en vez de hacerlo a través de un ISP. Para lograr esto, se requeriría de la instalación de un software específico en el router.

[35] https://github.com/nextcloud

La principal desventaja de esta red descentralizada es que requiere que muchos usuarios hagan esto en su router, ya que se debe trazar un camino entre todos los puntos a conectar. Otro riesgo es que, al no haber entidades que administren lo que fluye en la red, los controles sobre el tráfico son mucho más complicados de implementar (por ejemplo, censurar contenido inapropiado).

La red descentralizada (también conocida como web 3.0) ofrece muchas ventajas: sería imposible beneficiar un tipo de tráfico sobre otro, los servicios de conexión tendrían más disponibilidad (no se depende más de los servidores de un ISP), ofrecería una gran resistencia a la vigilancia masiva de gobiernos y privados y garantizaría el acceso gratuito y abierto a todo el contenido disponible.

Estas redes ya existen en algunas partes del mundo. Un ejemplo es la red NYC Mesh en Estados Unidos (ver Imagen 20), una comunidad que tiene nodos activos que conectan desde Manhattan hasta Brooklyn.

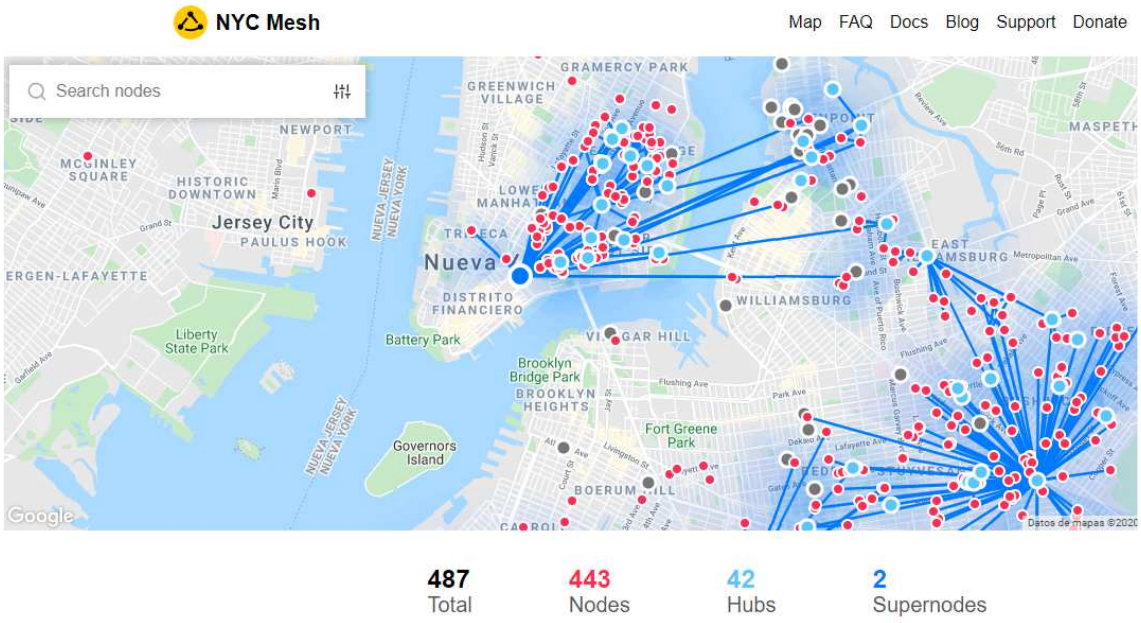

Imagen 20 - NYC Mesh
Fuente: https://www.nycmesh.net/map

Una red descentralizada ayudaría a contrarrestar los algoritmos de las grandes corporaciones de Internet (por ejemplo, Facebook y Google) que favorecen determinados contenidos. [129]

Tal como indica la fundación Substratum, y que aplica sobre su red descentralizada (Substratum Network), las redes descentralizadas deben

incorporar algoritmos criptográficos seguros para garantizar la seguridad y privacidad [130]. A su vez, es recomendable que se tomen medidas para lograr que personas no técnicas puedan incorporarse a la red de manera sencilla, favoreciendo el crecimiento de la red. También es muy importante ofrecer a los desarrolladores las interfaces (API) necesarias para que puedan construir aplicaciones compatibles con la red. Por último, es necesario el uso de una estructura de datos segura como lo es blockchain sobre la red Peer-To-Peer, para permitir una gestión segura de los datos que no dependa de una entidad centralizada.

8.6- Blockchain

Blockchain es una red de software P2P totalmente distribuida que utiliza la criptografía para alojar aplicaciones, almacenar datos y transferir fácilmente instrumentos digitales de valor (que representan dinero del mundo real) de una forma segura. Ethereum y Bitcoin son redes blockchain de código abierto. En ambas se usa criptografía para obtener un entorno seguro de miles de máquinas similares ejecutándose sin una autoridad central ni un propietario [131].

Las redes blockchain funcionan de forma similar a redes de malla o redes de área local (LAN): simplemente están conectados a otras computadoras pares (peers) que ejecutan el mismo software. Cuando se desea que una de estas redes P2P sea accesible a través de un navegador web, se deben usar librerías de software especiales para conectar el front-end de una aplicación (la interfaz gráfica del navegador) a su back-end (el blockchain).

Blockchain permite ejecutar de forma descentralizada transacciones vinculadas a dinero, bienes, e incluso votos, quitando el poder de procesamiento a una entidad centralizada y dándoselo a la comunidad de pares que la integran. [132]

Como su nombre lo indica, una blockchain está formada por una cadena de bloques. Cada bloque contiene datos (en el caso de Bitcoin, por ejemplo, el detalle de las transacciones, el emisor, el receptor y la cantidad de bitcoins), el hash del bloque y el hash del bloque anterior (a excepción del bloque inicial que únicamente contiene su propio hash). Si los datos de un bloque se

modifican, cambia su hash, y esto permite detectar el cambio ocurrido (ya que cada bloque contiene su hash y el hash del bloque anterior).

Para prevenir la manipulación de los bloques, existe el minado de bloques (conocido también como minado de criptomonedas), que consiste en la resolución de problemas matemáticos. Los usuarios de la blockchain que compitan por el minado de un bloque deberán resolver la prueba matemática, la cual consume muchos recursos, pero es sencillo comprobar su validez, y obtendrán una recompensa (una cantidad de criptomonedas, por ejemplo). Una vez calculada la prueba, el bloque se inserta en la blockchain si todos los pares de la red comprueban su validez.

En Ethereum, se pueden escribir fácilmente contratos financieros (contratos inteligentes o smart contracts) con otros usuarios dentro del sistema. Estos contratos inteligentes son programas informáticos no controlados por ninguna de las dos partes que lo firman y cuando ocurre una condición establecida en el contrato el mismo ejecuta automáticamente la cláusula correspondiente, sin ningún tipo de valoración humana. [131]

La principal diferencia entre Ethereum y Bitcoin es que el primero tiene la capacidad de guardar el estado (es statefull), por lo que puede detectar cambios en la información y recordarlos con el tiempo. Esto permite a los programadores considerar las interacciones entre usuarios (y las condiciones) para determinar el flujo en las transacciones de criptomonedas. En cambio, en Bitcoin, las transacciones suceden lo antes posible, sin considerar condiciones.

Toda blockchain debe implementar tres tecnologías: una red P2P (grupo de computadoras que se comunican entre sí sin una autoridad central), criptografía asimétrica (la capacidad de enviar mensajes encriptados de forma tal que cualquiera pueda verificar la autenticidad del remitente y que solo los destinatarios previstos pueden leer el contenido de los mensajes), y hashing (técnica criptográfica para generar una “huella digital” pequeña -digest- sobre un mensaje para poder verificar que no haya sido alterado por alguien no autorizado).

La confianza del blockchain se basa en estas medidas de seguridad, por lo que, tal como sostiene Hernández Serrano: “[…] para poder manipular una blockchain, uno debería ser capaz de modificar gran parte de los bloques de

la cadena, ser capaz de calcular todas las pruebas de trabajo y tomar el control de más del 50% de la red. Una hazaña imposible". [132]

8.7- Criptografía cuántica

La computación cuántica, basada en el uso de bits cuánticos, presenta riesgos y oportunidades para el cifrado de los datos [133]. El principal riesgo es que el cifrado convencional actual (usado para el ingreso de credenciales de forma segura en sitios web, el almacenamiento de contraseñas en bases de datos, la comunicación entre dispositivos, etc.) podría ser fácilmente vulnerado mediante el uso de criptografía cuántica. En el caso de RSA (sistema criptográfico creado por Rivest, Shamir y Adleman), la seguridad de su algoritmo radica en la aplicación del logaritmo discreto a un valor n (que forma parte de la clave pública) y es el producto de dos valores primos p y q. Con p y q suficientemente grandes es prácticamente imposible factorizar n para hallarlos utilizando herramientas convencionales. Pero usando, por ejemplo, el algoritmo cuántico de Shor, encontrar estos factores es una labor que tomaría unos pocos minutos. La mayoría de los cifrados convencionales se basan en problemas matemáticos cuya seguridad radica en el hecho de que estos problemas no pueden resolverse con las supercomputadoras actuales. Tanto la privacidad de las personas como la seguridad de sus transacciones (como la que implementa Blockchain) se ven amenazadas por la computación cuántica cuando se emplea el cifrado convencional. De hecho, ya en 2014, una investigación del Washington Post denuncia que la NSA invierte en computación cuántica para vulnerar la seguridad de los cifrados convencionales [134].

La oportunidad radica en el hecho de que reemplazando los bits por qubits a la hora de encriptar los datos, por el principio de incertidumbre de la mecánica cuántica, si un tercero intenta descifrar los datos de forma no autorizada nunca podrá conseguirlo sin alterar el sistema de cifrado, resultando facilmente detectable. [135]

El uso de criptografía cuántica podría permitir canales seguros para la distribución de las claves[36] (utilizadas en los algoritmos de cifrado), mediante

[36] Cadenas de caracteres numéricos usados para cifrar/descifrar datos.

una distribución de claves cuántica (QKD). Aunque la utilización de QKD aún no se ha generalizado, su uso comercial en Europa y Estados Unidos ha estado vigente por varios años para comunicaciones interbancarias, sistemas electorales, entre otros. En 2004, la primera transferencia bancaria del mundo con QKD se realizó en Viena, Austria.

Se cree que las computadoras cuánticas solo servirán para tareas específicas y que no van a reemplazar a las computadoras convencionales [136]. Sin embargo, su uso podría contribuir para implementar comunicaciones seguras y para proteger a las personas del espionaje masivo e ilegal.

8.8- Seguridad en sistemas operativos

Los sistemas operativos mayormente utilizados en computadoras personales y dispositivos móviles son no libres (Windows, MacOS, iOS, Android), ya sea porque su código es totalmente cerrado o porque tienen determinadas piezas de software cuyo código es cerrado. Además, las empresas que los desarrollan (Microsoft, Apple y Google) han formado parte del programa de vigilancia PRISM [122]. El uso de herramientas de empresas de PRISM es ampliamente utilizado en la educación alrededor del mundo. Por ejemplo, entregar notebooks con sistema operativo Windows. [11]

Cuando el código es cerrado, no queda más remedio que confiar en que quienes lo desarrollan preserven la privacidad de sus usuarios. [122]

El software libre permite que su código fuente sea auditado y mejorado por su comunidad. Esto no garantiza que el sistema sea seguro, pero si garantiza, por su transparencia, que no sea necesario tener que confiar en la buena voluntad del desarrollador de no crear puertas traseras u otros mecanismos que violen la privacidad de los usuarios. Por otra parte, no existe una barrera económica: personas de cualquier nivel social pueden tener acceso a él sin costo.

A la hora de elegir el uso de un software libre es muy importante que el mismo tenga una comunidad grande y de calidad, que pueda vigilar el código fuente y proveer mejoras en la seguridad y el rendimiento del mismo.

Tails OS, Qubes y Whonix son tres de los sistemas operativos más recomendados para proteger la privacidad.

Tails es una distro de Linux basado en Debian diseñada para proveer privacidad y anonimato. Todas las conexiones salientes se enrutan, por defecto, a través de la red Tor y se bloquean todas las conexiones no anónimas. Tails fue el sistema operativo que usó Snowden en 2013 para comunicarse con los periodistas a quienes entregó sus filtraciones.

Qubes es otro sistema operativo recomendado por Snowden, y es considerado por muchos como el más seguro. En Qubes, cada aplicación se ejecuta en una máquina virtual separada. Con esta medida de seguridad, si el usuario descarga un malware el equipo no se ve comprometido.

Whonix también es una distro de Linux basado en Debian, y consiste en dos máquinas virtuales: la primera es una puerta de enlace (Gateway) que envía todo el tráfico a través de Tor, mientras que la segunda (Workstation) accede a la red a través la primera. De esta forma, todas las conexiones de red solo son posibles a través de Tor.

8.9- Protección de datos personales

La normativa europea de protección de datos personales (GDPR), que entró en vigor en mayo de 2018, ayudó a aumentar la concientización de las empresas en este tema. Su reglamento [137] contempla cuatro niveles de sanciones en caso de incumplimiento: la advertencia, la amonestación, la suspensión del tratamiento de datos y la multa económica. En este último caso, existen dos niveles: en el nivel 1, un pago de 10 millones de euros o el 2% de los ingresos anuales (la cifra que sea más alta); en el nivel 2, un pago de 20 millones o el 4% de los ingresos anuales (de nuevo, la cifra más alta).

Si bien durante el mismo 2018 ya se dieron las primeras multas, no fue hasta 2019 cuando llegaron las primeras multas millonarias. Algunas de las empresas multadas fueron British Airways, Marriott International y Google. [138]

Sobre GDPR Snowden piensa que, si bien manifiesta la intención de cambiar las cosas, no será efectivo hasta que no se aplique con rigurosidad a las grandes compañías. [48]

Durante una videoconferencia con la Universidad de Dalhousie, Canadá, Snowden se refirió al tema:

> *"La gente puede entender de que el gobierno la está espiando, y por más que confíe en ese gobierno también debe ser consciente de que hay otros gobiernos y compañías en las que no confía que también la están vigilando […] Incluso Facebook, hoy en día, no se preocupa por proteger los derechos que abarca la ley GDPR, violándola por completo a pesar de la pena del pago del 4% de los ingresos a nivel global, porque saben que pueden sostenerse fuera del ámbito legal por algún tiempo más"*. [139]

Marta Peirano indica que lo único que puede impedir que vigilancia masiva de parte de las grandes tecnológicas devoren a la sociedad es la ley, pero que es complicado hacerlo cuando muchos congresistas son accionistas de esas empresas [118]. Como dijo el novelista francés Honoré de Balzac: "Las leyes son como las telas de araña, a través de las cuales pasan libremente las moscas grandes y quedan enredadas las pequeñas".

8.10- Seguridad en big data

El análisis de grandes volúmenes de datos (big data), incluyendo información personal sensible, puede resultar muy beneficioso para hacer negocios y para beneficiar a la sociedad (mejorar un sistema de salud, detectar efectos del calentamiento global, optimizar el consumo de recursos naturales, etc.). Sin embargo, si se lo hace violando la privacidad de las personas con fines inescrupulosos, como se ha visto con el caso de Cambridge Analytica, puede dañar los derechos de las personas. A su vez, puede significar pérdidas económicas para quienes lo cometan por violar determinadas normas, como el GDPR.

Para evitar estos problemas existen métodos para la extracción de conocimiento de grandes volúmenes de datos que preservan la privacidad, conocidos como técnicas PPDM (técnicas de Minería de Datos que Preservan la Privacidad, por sus siglas en inglés).

La minería de datos consiste en la extracción de conocimiento no trivial a partir de la detección de patrones de comportamiento y relaciones en una

gran cantidad de datos que se toman como entrada. Esto permite, luego, crear modelos descriptivos, sobre los cuales poder clasificar datos, o predictivos, para poder predecir datos futuros [140]. La gran mayoría de las técnicas de PPDM modifican o eliminan algunos de los datos de entrada para preservar la privacidad. Esta degradación de la calidad de los datos en pos de preservar la privacidad se conoce como utilidad. Los métodos PPDM están diseñados para garantizar un cierto nivel de privacidad y, al mismo tiempo, maximizar la utilidad de los datos para permitir una minería de datos efectiva.

Existen muchas técnicas estándar para PPDM, pero son principalmente para datos estructurados. La mayoría de los datos que alimentan al big data son del tipo no estructurado, como audio, video y texto, los cuales son mucho más difíciles de analizar que los datos estructurados, debido a su heterogeneidad. Por lo tanto, antes de proceder a analizarlos es necesario transformarlos en un formato que permita aplicar técnicas de Preservación de Privacidad de los Datos a Publicar (o PPDP, por sus siglas en inglés), que no es más que PPDM aplicada antes de la minería de datos. El objetivo de PPDP es que los datos a los que se le apliquen técnicas de minería de datos lleguen protegidos ante posibles filtraciones de datos sensibles. Para lograrlo es posible aplicar Perturbación (reemplazo de valores originales sensibles por otros sin afectar la estadística) y Anonimización (técnicas como k-anonymity y l-diversity permiten modificar registros de datos de forma que los mismos no puedan posteriormente ser asociadas a los individuos a los cuales hacen referencia), técnicas que forman parte de lo que se conoce como sanitización de datos. [141]

Si bien es cierto que existen técnicas muy prometedoras para la preservación de la privacidad en la recolección y el tratamiento de datos, como la mencionada PPDM, en la práctica no es habitual que se implementen. Existe un amplio consenso con respecto a la baja demanda de tecnologías de minería de datos que protegen la privacidad [142], ya que se considera que va en contra de los objetivos comerciales. Sin embargo, los incidentes vinculados a la privacidad que han trascendido y la aparición de nuevas y más estrictas regulaciones pueden ayudar a cambiar las cosas.

Además de las soluciones tecnológicas, es necesario que los Estados de todo el mundo generen y hagan cumplir leyes de conservación de la privacidad. GDPR ha sido una buena iniciativa en la Unión Europea. A su vez, los Estados deberían crear conciencia en los ciudadanos sobre el acceso a los datos personales que permiten a las aplicaciones y servicios (cuando se aceptan los accesos y términos de uso) que consumen día a día con el uso de smartphones, computadoras personales y equipos de IoT.

8.11- Seguridad en IoT

Hay en todo el mundo más de veinte mil millones de objetos conectados a Internet (cámaras IP, termostatos, puertas de garaje, controladores de equipos industriales, de estaciones de servicio o de semáforos, heladeras, televisores, etc.), y la cifra crece año a año. Al estar el IoT en una etapa relativamente temprana, muchos fabricantes se centran más en las funcionalidades y en el costo de estos dispositivos que en su seguridad. Esto provoca que la mayoría de los equipos de IoT presenten vulnerabilidades criticas como credenciales por defecto (por ejemplo, “admin”:”admin”), comunicaciones no cifradas, páginas de configuración inseguras y ausencia de soporte y actualizaciones [143].

Existen diferentes motores de búsqueda de dispositivos conectados a Internet. Algunos de estos son Shodan[37], que afirma haber sido el primero de todos y que permite encontrar detalles de dispositivos (webcams, routers, controladores, etc.) como localización, estado actual y especificaciones de hardware, y Thingful[38], que permite obtener todo tipo de detalle de equipos de IoT que sus propietarios le permitan.

En las Imágenes 21 y 22 se pueden apreciar ejemplos de cada uno.

[37] https://www.shodan.io/
[38] https://www.thingful.net/

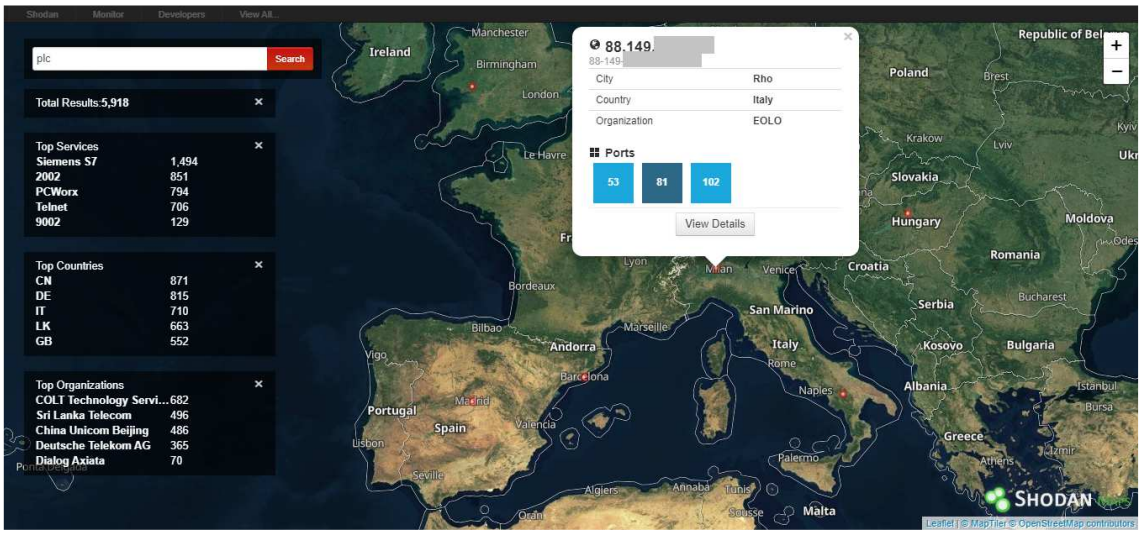

Imagen 21 - Búsqueda en Shodan
Fuente: Producción propia, mediante captura de pantalla

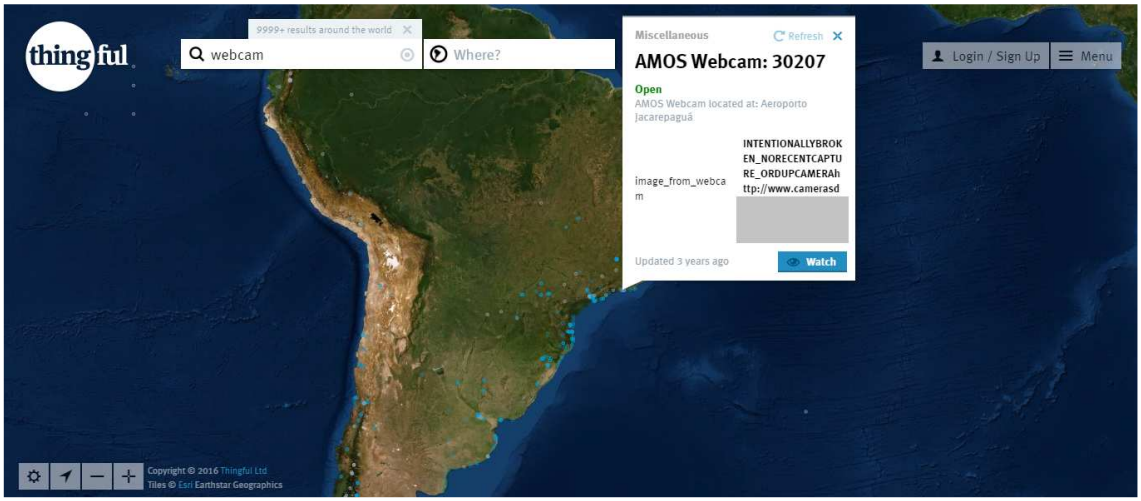

Imagen 22 - Búsqueda en Thingful
Fuente: Producción propia, mediante captura de pantalla

Un tercero malintencionado podría valerse de esta información y de los fallos de seguridad de los dispositivos IoT para realizar ataques sobre estos equipos y usarlos como puerta de entrada a redes corporativas, industriales o domésticas.

Por el lado de los usuarios, para aumentar la seguridad en estos dispositivos, se recomienda adquirir solo dispositivos que emitan actualizaciones de seguridad periódicas, instalar estas actualizaciones, cambiar las credenciales por defecto y habilitar sus conexiones solo cuando sea necesario y en redes seguras.

En cuanto a los fabricantes, sería apropiada una solución integral que establezca un marco de desarrollo seguro para estandarizar el diseño, la

implementación, la administración y la certificación de dispositivos IoT. Esto permitiría pensar en la seguridad de los dispositivos desde su diseño y durante todo su ciclo de vida. [144]

Para comprometer más a los fabricantes a implementar seguridad desde el diseño resulta oportuno que los Estados establezcan leyes a cumplir. Un intento en este sentido ocurre en California, Estados Unidos, donde en 2018 se aprobó una ley que regula el Internet de las Cosas, la cual entró en vigencia desde el 1 de enero de 2020 [145]. Esta ley exige a los fabricantes que cada dispositivo tenga una contraseña única o que soliciten obligatoriamente a los usuarios a modificar la contraseña al usarlo por primera vez. Además, los fabricantes deberán considerar aspectos de seguridad sobre la información que recolectan, contienen, transmiten y eliminan los equipos. Si bien no indica sanciones ante infracciones y algunos la consideran poco exhaustiva, podría llegar a inspirar a otros Estados a seguir un camino similar y más estricto.

8.12- Derecho al olvido

En este mundo de digitalización de cualquier actividad humana, de archivos digitales, de bases de datos en línea, de aplicaciones móviles y de redes sociales, recordar es la regla general, y olvidar es la excepción. Incluso si una persona prescinde del uso de servicios online o lo utiliza mínimamente, otras actividades online van dejando rastro. Como, por ejemplo, la búsqueda en motores de búsqueda como Google o Yahoo!, las cuales son almacenadas en los servidores de éstas empresas conformando un historial personal. También puede ocurrir que ciertos datos sobre una persona (fotografía, video, nombre completo en una base de datos, mención de la persona en un blog, etc.) sean subidas a la red por un tercero. O bien que estos datos online en su momento hayan sido subidos a la red voluntariamente por esa persona y que posteriormente borró, pero que un tercero le hizo una copia y lo mantuvo disponible en otro sitio. [32]

Esta información de las personas, recopilada por los distintos intermediarios de la red, permite identificarlas y a la vez definirlas. Extendiendo esta

actividad a lo largo de varios años se obtiene un nivel de precisión cada vez mayor sobre determinados aspectos de estas personas.

Sin embargo, esta recopilación e indexación de múltiples datos a partir de hechos aislados en torno a una misma persona puede llevar a construir un relato muy alejado de la realidad. A modo de ejemplo, si dos personas tuvieron un intercambio de tweets agresivos (lo cual queda registrado en los servidores de Twitter) y esa misma noche fueron ambos a una discoteca (teniendo cada uno un celular con GPS activado, registrando que ambos estaban allí) en la que se generó una pelea entre dos personas, no implica que se haya tratado de una riña entre las dos personas mencionadas.

Otro caso similar sería que un medio de comunicación importante, habitualmente utilizado como fuente de otros sitios de noticias o blogs, acusara de corrupción a un político utilizando información falsa o expresiones sacadas de contexto. Por más que el propio medio al poco tiempo después se rectifique, la versión digital de la noticia puede continuar estando disponible, e incluso haber sido replicada por otros medios.

En estos casos, cuando se busque información en la red sobre estas personas los motores de búsqueda lo asociarán con hechos alejados de la realidad.

En este contexto, existe un debate sobre la necesidad del derecho al olvido que permita eliminar de la red la información digitalizada sobre un individuo y que solo pueda ser controlada por dicho individuo. Eduardo Bertoni comenta:

> *"[…] el derecho al olvido busca, por ejemplo, que una empresa no tenga más en su poder cierto dato sobre alguien, que mis amigos dejen de ver en las redes sociales la foto de mi excursión de bachillerato de hace diez años, o que un motor de búsqueda excluya de sus resultados los rumores falsos que acabaron con la reputación de alguien".*

Sin embargo, Bertoni menciona algunos casos de ejemplo donde no sería conveniente aplicar el olvido:

> *"[…] un político corrupto que desea que no se hable más de su oscuro pasado, un policía buscando que se elimine un video donde acepta un soborno, un médico tratando de eliminar un registro sobre una mala práctica profesional".*

Una búsqueda alternativa ante la imposibilidad o no conveniencia de borrar un dato es la anonimización del mismo, es forma tal que el dato por sí solo no permita identificar al titular. Sin embargo, esto podría resultar insuficiente si se entrecruza este dato junto a una gran masa de datos, permitiendo identificar al individuo.

Una forma de lograr que ciertos datos digitalizados sean accesibles por el público en general, es la configuración por parte de los desarrolladores del archivo "robots.txt" de las páginas web, el cual indica cuáles archivos pueden ser indexados por los buscadores de Internet y cuáles no.

También existen otras dos propuestas para el manejo de los datos en el entorno digital. Una de ellas es que el usuario al momento de crear o compartir un archivo introduzca una fecha de expiración del mismo (días, meses o años), a partir de la cual los servicios online se encargarán de borrar de la red este archivo, obligando también a que las copias que se realicen sobre este archivo contengan la misma fecha de expiración y respondan así al mismo vencimiento.

La propuesta restante se conoce como contextualización y se refiere a la posibilidad de poner en contexto un dato que circule en la red anexando información adicional sobre ese dato. El objetivo es explicar o refutar dicho dato para evitar que sea sacado de contexto, por ejemplo, a través del uso de etiquetas.

8.13- Combatir la manipulación y la desinformación

A principios de 2019, WhatsApp anunció que limitará la cantidad de mensajes reenviados a un máximo de cinco conversaciones (individual o grupal), con el objetivo de luchar contra la propagación de noticias falsas [146]. Esta medida sirve para complementar la medida tomada anteriormente con la cual se añadía el texto “Reenviado” sobre el mensaje, lo cual era insuficiente para frenar las fake news [147]. Otra medida tomada por el servicio de mensajería es la posibilidad de buscar en Google una imagen recibida, y así poder conocer si la misma es o no auténtica.

Sin embargo, un estudio del Instituto de Tecnología de Massachusetts (MIT) y la Universidad Federal de Minas Gerais (Brasil) [147] concluye que “[…] los

esfuerzos actuales desplegados por WhatsApp reducen la velocidad de la difusión de información, pero son poco efectivos bloqueando la propagación de campañas de desinformación cuando el contenido presenta una gran viralidad […] Dependiendo de la viralidad del contenido, esos límites no son efectivos para evitar que un mensaje llegue a toda la plataforma con rapidez".

A fines de 2019, Twitter anunció la prohibición de anuncios políticos en su plataforma [149]. Jack Dorsey, ejecutivo de la empresa, indico al respecto:

> *"Un mensaje político gana influencia cuando la gente decide seguir una cuenta o retuitearlo. Pagar por tener más alcance elimina esa decisión y obliga a que los mensajes políticos sean optimizados y dirigidos. Creemos que esta decisión no debería ser limitada por el dinero".*

A su vez, Dorsey se refiere a los mecanismos de manipulación y desinformación en los anuncios:

> *"Los anuncios políticos en Internet presentan desafíos completamente nuevos para el discurso cívico: la optimización de mensajes a través del aprendizaje de las máquinas, el microtargeting, la desinformación sin control y los deep-fakes. Todo cada vez con más velocidad, sofisticación, y a una escala apabullante".*

Esta medida de Twitter es radicalmente opuesta a la que ha exhibido hasta el momento Facebook, que ha manifestado no hacerse responsable de que se lleven a cabo campañas de desinformación.

La sofisticación de las noticias falsas a partir del deepfake pareciera ser una evolución de las técnicas de phishing y de ingeniería social, ya que puede hacer pensar a cualquier individuo de que realmente sea la persona en cuestión quién lanza un mensaje. [150]

Cada vez resulta más complicado distinguir un vídeo modificado de uno que es real. Se debe recurrir a un análisis minuciosos, como, por ejemplo, la detección del parpadeo, que es una señal fisiológica que no suele estar bien presentada en los videos falsos.

Cualquier persona puede crear un perfil en redes sociales con el cual generar noticias falsas, difundidas, a su vez, por cuentas falsas (bots o trolls). Con este uso fraudulento de las redes sociales se pueden generar

fácilmente campañas de desinformación o de difamación de forma sencilla y barata. Incluso son baratas las herramientas de machine learning para crear videos falsos, habiendo disponible para tal fin servicios en la nube por lo que no es necesario comprar equipamiento.

Teniendo en cuenta que el volumen de las noticias falsas crece exponencialmente, los fact-checkers no pueden abordarlas todas. Esta situación exige procesos automatizados para contribuir en la tarea de reconocer las noticias falsas. Combinando el big data, para almacenar y vincular grandes volúmenes de datos, con el machine learning y el deep learning, para aplicar modelos inteligentes de análisis y predicciones, se pueden realizar evaluaciones de las noticias y detectar aquellas falsas. [151]

Uno de los proyectos para implementar este tipo de soluciones es el que lleva adelante la empresa Fabula AI, comprada por Twitter en 2019, dedicada a la detección de información falsa a través de herramientas de inteligencia artificial [152]. Fabula AI cuenta con varios algoritmos de detección de fake news basados en el campo del "aprendizaje profundo geométrico", que permite procesar conjuntos de datos tan grandes y complejos a los cuales no se les puede aplicar con éxito las técnicas de aprendizaje automático tradicionales.

De la misma forma que se lo ha utilizado para analizar el texto de un e-mail y determinar si se trata o no de un mensaje no deseado (SPAM), el machine learning se puede utilizar para analizar un posteo online para determinar si es falso o no [153]. Por ejemplo, comparando el titular de la noticia con el contenido del artículo para analizar si dicho título es engañoso (muchas personas solo leen los títulos de las noticias), o bien comparando la noticia con artículos similares de otros medios para determinar si sostienen hechos diferentes o no. Así, se podrían identificar cuentas y sitios web que difunden noticias falsas.

Sin embargo, la cura también es parte de la enfermedad, ya que la IA también es la que permite crear deepfakes muy sofisticados y difíciles de detectar como no reales.

Joaquín Quiñonero, doctor en machine learning que trabaja en Facebook desde 2012, afirma [154] que el contenido inapropiado (venta de drogas, pornografía infantil, propaganda terrorista, spam, incitación al suicidio, etc.) y

las cuentas falsas son más sencillos de detectar y contener. Sin embargo, otro tipo de contenido es más difícil de abordar por la inteligencia artificial. Un caso es el de los deepfakes. Otro es el del contenido vinculado al odio (como el bullying o el acoso), ya que “hay palabras que se utilizan de forma cariñosa que en un contexto distinto podrían considerarse insultos y que sacadas de contexto pueden ser calificadas como contenido de odio”. Quiñonero también sostiene que la desinformación y las noticias falsas son difíciles de detectar con éxito para la IA, debido a su limitación en la comprensión del contexto, del sentido común y de ciertas sutilezas y, a su vez, porque el margen de error en la detección debe ser extremadamente bajo.

La mejor forma de combatir las noticias falsas seguirá siendo la inteligencia de las personas, quienes deberían ser más cautelosas. En lugar de creer y compartir una noticia inmediatamente después de leerla (o de leer su título), la persona debería investigar si la información es correcta. El compartirla le da credibilidad a una publicación: cuando otras personas la ven y detectan que fue compartida por alguien que conocen y en quién confían, es menos probable que sospechen que se trata de una fuente poco rigurosa.

En este sentido, Trend Micro realiza recomendaciones a los usuarios para combatir las fake news [83], algunas de las cuales se detallan a continuación.

Una noticia podría sospecharse como falsa si tiene errores ortográficos en el contenido, si el sitio web está mal diseñado, si contiene fotos e imágenes alteradas o no actuales (por ejemplo, buscando en Internet la imagen para conocer la fecha de su origen), o si no hay referencia al autor y a fuentes.

Leer más allá del titular.

Verificar la historia con otros medios de comunicación.

Examinar los enlaces y fuentes que utiliza el artículo para respaldar su historia, analizando que ellos mismos no estén difundiendo información errónea.

Investigar al autor y dónde y cuándo se publica el contenido.

Revisar los perfiles de los usuarios para saber si son reales o bots, por ejemplo, viendo si un párrafo se puede escribir y publicar en un minuto o menos, o si los comentarios anteriores se publicaron textualmente, etc.

Consultar fact-checkers acreditados.

Comprender que las historias que no se alinean con las propias creencias personales no necesariamente significan que sean falsas.

Conclusiones

"[…] La invención del ferrocarril conllevó simultáneamente la invención de los accidentes de tren. Con la Web pasa algo parecido. La catástrofe industrial de Internet es la vigilancia masiva". Esto es lo que afirma Ignacio Ramonet [2]. Snowden también ha trazado otro paralelismo. En este caso, entre la capacidad nuclear, la cual fue corrompida y los conocimientos, la ciencia y las herramientas se transformaron en armas militares terribles, y el avance de la ciencia de la computación, que ha llegado a monitorizar las actividades privadas de las personas y a construir plataformas y algoritmos que pueden predecir decisiones y moldear comportamientos hacia ciertos resultados [139].

Resulta innegable la ventaja que ofrecen las nuevas tecnologías y sus beneficios para la sociedad, como la posibilidad de realizar videollamadas, conocer al instante noticias en cualquier parte del mundo, expresar libremente opiniones y estados en redes sociales y foros, acceder a todo tipo de información y realizar controles de acceso mediante información biométrica, todo de manera rápida, sencilla y “sin costo”. Sin embargo, el precio que se paga es que toda actividad realizada en estos medios queda almacenada en alguna parte de la red, y puede ser recolectada, analizada, explotada o vendida por empresas, Proveedores de Internet, organizaciones o agencias de inteligencia, de las diversas formas que se han detallado en este trabajo. Como reza una famosa frase del mundo informático “Si no pagas por el servicio, entonces formas parte del producto”.

En la novela “1984”, de George Orwell, una de las cosas más graves era que la televisión espiaba a los ciudadanos. Hoy en día, las personas pagan para que los dispositivos (smart TV, smartphones, computadoras personales) los espíen y monitoreen todos sus movimientos.

También es importante señalar que, tal como indica Rafael Bonifaz, muchas compañías de telefonía móvil ofertan promociones de WhatsApp ilimitado sin consumo en planes de datos, a pesar de que WhatsApp fue comprada por Facebook en el año 2014 y esta última es miembro del programa PRISM. [11]

A partir de las revelaciones de Snowden se supo de la conexión entre las agencias de inteligencia y las grandes compañías de telecomunicaciones, los Proveedores de Internet y las redes sociales. Con lo cual, y tal como afirma Ewen Macaskill [9], a estas agencias les encanta que los usuarios de redes sociales suban muchos contenidos. Y si bien los usuarios los suben voluntariamente, los gobiernos y sus agencias de inteligencia no tienen el consentimiento de los usuarios para espiarlos y almacenar sus publicaciones e interacciones.

Snowden asegura que cada vez hay más gobiernos que deciden incluso cortar el acceso a Internet para que la gente no pueda comunicarse y organizar reclamos y protestas. Y más aún aquellos gobiernos que tienen el poder de asociarse con alguno de los gigantes tecnológicos, que concentran casi todas las comunicaciones y datos de los usuarios de la red, permitiéndoles, por ejemplo, rastrear a algún sospechoso. Estos gigantes tecnológicos llevan el registro permanente (de ahí el nombre de su libro lanzado en 2019, “Permanent record”) de todo lo que hacen las personas, transformándolas ya no en usuarios sino en su materia prima. [48]

Por otra parte, es fácil suponer que la capacidad de almacenamiento de los programas revelados por Snowden, que datan de ya algunos años atrás, ha incrementado y lo continuará haciendo, ya que es cada vez más sencillo recolectar, almacenar y procesar información.

Agencias de inteligencia y gobiernos han intentado justificar la vigilancia masiva con el argumento de que las personas que no tienen nada que ocultar no tienen nada de qué temer. Con este enfoque, cualquier persona que exija que se respete su derecho a la privacidad estaría cometiendo actos inadecuados. Muchas personas no se oponen a la vigilancia de los Estados, resignando su derecho al anonimato y la privacidad, porque piensan que no tienen nada que esconder y, además, las autoridades le prometen a cambio beneficios de seguridad. Sin embargo, tal como sostiene Snowden [104], es un error pensar en que hay que resignar privacidad para poder conseguir seguridad, porque sin privacidad no hay libertad, y si no hay libertad los ciudadanos son totalmente vulnerables y no tiene sentido la seguridad.

A su vez, como se indicó en este trabajo, la existencia de una vigilancia masiva genera que las personas se autocensuren, no puedan manifestarse de manera libre y se autolimiten a cumplir los mandatos de la ortodoxia (afectando la identidad de la persona, ya que ésta se construye también en base a un libre proceso de prueba y error), debido a que una simple búsqueda en Google o un posteo en redes sociales podría señalarlas como sospechosas. Esta situación no tiene sentido en países democráticos que se jacten de defender la libertad de expresión y el acceso a la información.

Menciona Eduardo Bertoni que el monitoreo de la red por parte de los gobiernos en pos de la seguridad nacional y el orden público está reconocido por instrumentos de derecho nacionales e internacionales, ya que no necesariamente son sinónimos de represión. La necesidad de combatir el crimen y de recabar pruebas judiciales son objetivos de primer orden. Algunos ejemplos son prohibir el uso de redes sociales cuando haya indicios de que sean utilizadas para organizar actividades criminales, encarcelar personas que visiten constantemente sitios web que promuevan el terrorismo y denunciar ciber acoso, violencia o apología del crimen en blogs y otros sitios web. [32]

A su vez, y tal como lo remarca Ewen Macaskill [9], es peligroso para un político confrontar contra las agencias de inteligencia o limitarlas, porque si ocurre un incidente grave en un país las agencias pueden culpar a los políticos de que no les permitieron espiar todas las comunicaciones que necesitaban. Y esta acusación pública no es del agrado de los políticos por el peso que conlleva.

Por lo tanto, si se establecen claramente límites y controles, no es incorrecto que un Estado democrático vigile las comunicaciones de individuos sospechados de haber cometido algún delito y almacenen su contenido. Aquí es donde hay que señalar la diferencia entre la vigilancia específica y la vigilancia masiva. La primera es efectiva, legal y sirve para identificar delincuentes y juzgarlos, siempre y cuando esté acompañada de una orden judicial mediante basada en una sospecha individualizada de actos ilícitos.

En cambio, la segunda monitorea de forma indiscriminada a todas las personas al mismo tiempo, y es fácil y barato hacerlo debido a que así lo permite el sistema de comunicaciones actual. Esta vigilancia no solo es

ilegal y viola los derechos individuales, sino que también es ineficaz en el objetivo que dice perseguir. Los programas de vigilancia masiva de Estados Unidos no han logrado identificar a ningún terrorista, sin embargo, han violado el derecho a la privacidad ciudadanos de todo el mundo. Esto es porque cuando se vigila y se recopilan datos de todo el mundo, se obtienen demasiados datos como para poder analizarlos, a diferencia de lo que ocurre con la vigilancia específica.

Snowden piensa que si los programas de vigilancia masiva hubieran conseguido detener algunos ataques terroristas tampoco serían correctos, porque violan el derecho a la privacidad y tienen un altísimo costo (miles de millones de dólares). También sostiene que los ataques terroristas son algo prácticamente imposible de impedir, porque ni las leyes, ni la policía, ni los servicios de inteligencia pueden cubrirlo todo, y los grupos criminales siempre van a encontrar alguna forma alternativa de cometer los delitos, por ejemplo, tomar un coche y conducirlo contra personas en un parque. A su vez, piensa que el principal error de Estados Unidos tras el 11S fue tomar a los terroristas, que son asesinos comunes, y elevarlos a la categoría de Estado (por ejemplo, decir que Al Qaeda es lo mismo que Afganistán o Irak). Y en lugar de trabajar con otros países para investigar lo que había sucedido, decidieron invadir Afganistán e Irak. [104]

Robert Tibbo, abogado de Snowden, ha manifestado que su cliente fue en 2013 la persona más buscada por distintos gobiernos por haber permitido el conocimiento público de conductas criminales y abuso de poder de gobiernos. Afirma que en los últimos años se llegó a un nivel de persecución de whistleblowers[39] (como Snowden) o activistas políticos, y de aquellas personas que los ayudan, protegen o trabajan con ellos, nunca antes visto, incluso atacando leyes internacionales de asilo y refugio, como ocurrió con Julian Assange cuando el presidente ecuatoriano Lenin Moreno arbitrariamente le quitó el asilo político en 2019 sin ninguna causa evidente.

El artículo 12 de la Declaración Universal de los Derechos Humanos [155] dice:

[39] Término inglés que hace referencia a denunciantes/delatores/soplones que filtran información sobre presuntos hechos delictivos de organizaciones y gobiernos.

> *“Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”*.

En este sentido, y tal como lo destaca Rafael Bonifaz, los gobiernos están obligados a defender los derechos humanos de sus ciudadanos, y la privacidad es uno de ellos, por lo que se debe hacer todo lo posible para protegerla, sobre todo cuando la privacidad de la vida digital de sus ciudadanos es vulnerada por empresas y gobiernos extranjeros. [11]

Tal como piensa García Fernández, el derecho a la privacidad “es despreciado en la sociedad actual”, mientras que la posverdad mediante la propagación de noticias falsas “es un recurso cada vez más utilizado en las campañas políticas". Y sobre la posverdad sostiene que "[…] el vacío legal la convierte en un terreno fértil para las estrategias de campaña sucia y difamación". [95]

Todos los días se observan nuevas noticias falsas que persiguen determinados objetivos, mayoritariamente políticos, que son generadas principalmente por los grandes medios de comunicación (como lo ha demostrado el estudio del profesor Albright) y que se basan en generar miedo u odio para que se viralicen más rápidamente. Los trolls de las redes sociales son un importante vehículo para esta viralización, además de su diaria tarea de realizar publicaciones y comentarios para estigmatizar y demonizar a determinadas personalidades. Incluso ante una verdad irrefutable y comprobada los trolls son capaces de ir en contra de quienes la divulguen, generando que aquellos usuarios comunes que sean seguidores de estas cuentas falsas y consuman sus publicaciones desconfíen de esta verdad. Como dijo George Orwell: "Cuanto más se aleja una sociedad de la verdad, más odia a quienes hablan de ella".

Edward Louis Bernays, considerado el padre de la propaganda y las relaciones públicas, sostiene que en la sociedad democrática la manipulación de las costumbres y opiniones es un elemento importante, y que este moldeo de las mentes es llevado a cabo principalmente por personas de las que nunca se oye hablar. A partir de esto, Pedro Baños afirma:

> *"Pensamos que somos libres, que podemos elegir de forma autónoma nuestro destino, nuestros gustos, la manera de vestir o de comportarnos, lo que comemos o a qué dedicamos el tiempo libre, pero estamos permanentemente inducidos a adoptar acciones, decisiones y actitudes. Con creciente sutileza, los que deciden por nosotros nos imponen formas de vida, modelos sociales e ideologías, de modo que quedamos sometidos a sus designios. Esto es más cierto que nunca hoy en día, cuando se ha puesto de moda la palabra «posverdad» para definir el contexto global de desinformación, aunque en realidad sería más acertado denominarlo «prementira», «multimentira» o «plurimentira», pues lo que principalmente llega al público no es más que una gran falsedad disfrazada de verdad"*. [76]

Los avances tecnológicos deberían estar relacionados con el bienestar y la seguridad humana, acompañados de una ética y moral adecuadas, sino se corre el riesgo de que los ciudadanos sean cada vez más controlados por quienes impongan su liderato tecnológico.

Las contramedidas descritas en el capítulo ocho representan algunos recursos a considerar para combatir en el escenario actual de vulneración de derechos y manipulaciones. Ya en 2014, Enrique Amestoy detallaba cómo hacer frente a esta situación:

> *"Quizá el uso inteligente, responsable, sin exposición de datos personales, pueda ser la primera estrategia para cambiar nuestro hábito de consumo de redes sociales. Luego entiendo que deberemos ir hacia modelos de redes descentralizadas o redes distribuidas donde no hay un único propietario ni los datos se almacenan en forma central. Modelos como el P2P, el utilizado, entre otros, para la descarga de archivos en Internet y modelos de encriptación de información que permitan que nuestros datos no son rastreados. El modelo de la red TOR es un buen ejemplo de navegación anónima y otro buen ejemplo para ir tomando en cuenta es en que se basa la criptomoneda Bitcoin: el Blockchain. Quizá todo esto parezca aún una utopía, pero ya hay cientos pensando y experimentando con estos modelos alternativos en el mundo entero"*. [60]

Tal como sostiene Alessandro Acquisti en una charla TED, la privacidad no tiene que ver con tener algo negativo que ocultar, sino que se orienta a la protección del abuso de la información personal, mediante herramientas de big data y vigilancia masiva que realizan las organizaciones (por ejemplo, las campañas publicitarias direccionadas), con lo cual se busca influir en las personas y manipularlas. [156]

Acquisti también afirma que existen mecanismos para que las organizaciones exploten los datos disponibles en la red sin violar la privacidad de las personas, por ejemplo, con modelos de minería de datos que protegen la privacidad y con la precaución de los usuarios de la red de usar navegación anónima y servicios de e-mail encriptados, todos ellos elementos considerados en el capitulo ocho. Sin embargo, alega que cambiar la comodidad actual (plataformas en las cuales consumir series y películas, redes sociales para compartir estados y fotos, equipos de IoT que facilitan las tareas diarias, uso de tarjetas con chips de identificación, etc.) por autonomía, privacidad y libertad tiene el alto precio de, justamente, abandonar dicha comodidad.

Snowden comenta que la manera de corregir el modelo de las plataformas tecnológicas es “cambiando la legislación, cambiando la tecnología, cambiando nuestras decisiones como consumidores y como ciudadanos”. Además, sostiene que hace falta una descentralización de las infraestructuras, ya que, por ejemplo, la gran mayoría de las aplicaciones utilizan servicios de Google o Facebook para su funcionamiento, brindando acceso a estos gigantes a los datos de los usuarios de dichas aplicaciones, generando una autoridad centralizada que se manifiesta cada vez más corrupta y poderosa. Sobre este tema concluye que “la única manera de evitar estos registros es crear estructuras alternativas, sistemas alternativos, protocolos alternativos que no requieran una autoridad central” y que “no basta con cambiar a Jeff Bezos por otro, a Mark Zuckerberg por otro” sino que hace falta “un cambio holístico, un cambio estructural”. [48]

Snowden también manifiesta que muchos gobiernos, en afán de perseguir el culto de la eficiencia (si algo puede hacerse más rápido, por menos dinero y con menos esfuerzo, entonces es mejor), contratan determinados servicios, por ejemplo, el servicio de la nube de Amazon para mover allí sus datos o

contratar algún sistema informático para usarlo durante un proceso electoral, sin darse cuenta que el exceso de eficiencia atenta contra la seguridad y libertad de los ciudadanos, ya que facilita, por ejemplo, el hackeo de dichos sistemas y el acceso a esa información por parte de terceros no autorizados.

Resulta fundamental el compromiso de parte de los Estados y de la ciudadanía en su conjunto, para poder generar un cambio efectivo y consistente del actual sistema. En este sentido, Snowden manifiesta:

> *"No basta con cambiar gobiernos. Nada cambiará mientras vivamos en un mundo donde los chips solo pueden ser americanos o chinos, donde los métodos para fabricar radios que operan en cierta frecuencia tienen que estar licenciados y cumplir la legislación estadounidense o china, aunque vivas y trabajes en España, Colombia o Chile. Donde la gente que ha creado el sistema en el que nos movemos siga colonizando los medios de producción, los medios de expresión. Han convertido la propiedad intelectual en una herramienta de control político y social a escala global".* [48]

Tal como señaló Marta Peirano en una charla TED en 2019 [157], ya no basta con acciones individuales, como utilizar Tor o utilizar criptografía (las cuales siguen siendo muy recomendables), porque se trata de un problema colectivo (como lo es la lucha contra el cambio climático o contra una pandemia), y nadie se salva solo. Ejemplos de estas acciones colectivas podrían ser juntar firmas para evitar que en escuelas se utilicen productos de empresas que hayan participado del programa PRISM, luchar contra sistemas de reconocimiento facial en la vía pública (como ocurrió en Hong Kong) e implementar redes comunitarias independientes y descentralizadas, como la NYC Mesh de Nueva York.

Sobre la actitud que debería adoptar la ciudadanía, Snowden sostiene:

> *"Las cosas están así solamente porque nosotros lo permitimos. No existen héroes, sino elecciones heroicas. Es solo una decisión la que nos separa de poder cambiar las cosas. No es necesario tomar una decisión que salve al mundo, sino poner un ladrillo que anime a otros a contribuir y aportar sus ladrillos para ir construyendo los cimientos de un sistema mejor que el que tenemos hoy en día"*. [104]

El rol de los ciudadanos pasa a ser fundamental, ya que por más que exista voluntad de un gobierno para que el Estado tome las decisiones necesarias para cambiar las cosas poco es lo que este puede hacer ante los intereses del poder real, es decir, de aquellos gigantes medios de comunicación, corporaciones (por ejemplo las GAFAM), sectores financieros e instituciones. Por lo tanto, esta actitud colectiva de los ciudadanos que destacan Snowden y Peirano es la única capaz de torcer los intereses de los sectores mencionados. En definitiva, solo un pueblo bien informado es capaz de reconocer los ataques a los derechos humanos, de tomar acciones colectivas para contrarrestar la vigilancia masiva y la manipulación y de reclamar que los Estados los defiendan y que, con el sostén de un gran apoyo popular, tomen las medidas necesarias para que la tecnología deje de ser un arma de manipulación de los poderosos y se transforme en un aliado de las personas. Un aliado que contribuya a mejorar su vida sin poner en riesgo su seguridad.

Anexos

Schrems y la revocación del Safe Harbor

El principal responsable de la revocación del acuerdo de Safe Harbor fue el activista austríaco Max Schrems, conocedor de la legislación europea vinculada a la protección de datos personales, que llevó adelante una investigación contra Facebook. En la misma, descubrió que este gigante tecnológico no respetaba el tratado de Safe Harbor y, a su vez, acumulaba por cada usuario y de manera automática un dossier con detalles de cada vez que el usuario se inició sesión, desde dónde, por cuánto tiempo, con qué dispositivo, las personas que ha agregado y eliminado como amigo, las direcciones de mail de sus amigos, los mensajes y chats que escribió, las fotos que ha visto, los posteos que ha leído, etc. Cuando The Guardian publicó los documentos revelados por Snowden sobre el programa PRISM, llevó el caso al Tribunal de Justicia de la Unión Europea. El joven austríaco fue felicitado por el propio Edward Snowden vía Twitter.

Técnica GAN

La técnica GAN consiste en dos redes neuronales enfrentadas, una llamada Generador y otra Discriminador. Ambas reciben un entrenamiento en el que reciben como entrada imágenes o sonidos, los de la red Discriminador son los datos reales (por ejemplo, la voz o cara real de la persona objetivo) y los de la red Generador son datos del mismo tipo que la red Discriminador pero no los reales (por ejemplo, la voz o cara de una persona cualquiera).

La tarea del Generador es producir variaciones de los datos recibidos en el entrenamiento (imágenes o sonidos), las cuales toma como entrada el Discriminador, que los compara con los datos reales y determina si es lo suficientemente aproximado a la realidad, devolviendo verdadero o falso, y dándole un feedback al Generador de en qué medida se acercó a los datos reales para que este vaya mejorando. Este paso se repite hasta que el resultado sea verdadero.

Causas económicas en las dos guerras mundiales

Pedro Baños explica que tanto la Primera como la Segunda Guerra Mundial tuvieron causas principalmente económicas. La Primera se origina por el objetivo de Gran Bretaña (en ese momento el dominador económico) y Francia, aliado con preponderancia naval, de destruir a su incipiente competidor Alemania, que había logrado un alto crecimiento de su industria y su comercio exterior y estaba lanzado a conquistar nuevas colonias para extraer recursos. Para el origen de la Segunda tuvo una gran influencia la pretensión de Alemania de basar su moneda en la producción y no en la reserva de oro (lo cual, si tenía éxito, pudiera expandirse a otros países), lo cual hizo que los teutones se transformaran en un objetivo de guerra para Estados Unidos y Gran Bretaña, que tenían en ese momento la mayor parte de las reservas mundiales de oro y dominaban el sistema financiero de otorgar créditos con interés.

Citas bibliográficas

[1] Gabriel Paz, José, "La alianza Ukusa en inteligencia de señales: de los éxitos en la inteligencia artesanal al fracaso de la masividad", Marina de Guerra del Perú - Escuela Superior de Guerra Naval, 2014, http://virtual.esup.edu.pe/handle/ESUP/80 [Consultado el 04-01-2019]

[2] Ignacio Ramonet, libro "El imperio de la vigilancia", Editorial José Martí, 2016

[3] Artículo de Indymedia Barcelona, “UKUSA, el pacto definitivo”, 28-02-2005, http://barcelona.indymedia.org/newswire/display/162436, [Consultado el 08-01-2019]

[4] Artículo del sitio web Crypto Museum, “Datotek DV-505”, 04-11-2017, https://www.cryptomuseum.com/crypto/datotek/dv505/index.htm, [Consultado el 14-01-2019]

[5] Greg Miller, artículo de The Washington Post, “The intelligence coup of the century”, 11-02-2020, https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/, [Consultado el 04-03-2020]

[6] Marina Meseguer, artículo de La Vanguardia, 11-09-2016, "ThinThread, el programa secreto que podría haber evitado los atentados del 11S", https://www.lavanguardia.com/internacional/20160911/41223154746/thinthread-programa-secreto-evitado-atentados-11s.html, [Consultado el 12-03-2019]

[7] Documental Citizenfour, directora Laura Poitras, 2014

[8] Informe Moraes de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior, 21-02-2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2014-0139+0+DOC+XML+V0//ES#title2

[9] Entrevista de Pedro Brieger y José Natanson a Ewen MacAskill y David Blishen, Noticiero Visión 7 de la TV Pública Argentina, 07-12-2015, https://www.youtube.com/watch?v=__TY2GoQdeg

[10] Eva Mejías Alonso, Trabajo de investigación del Máster de Archivística y Gestión de Documentos de l’Escola Superior d'Arxivística i Gestió de Documents: "La vigilancia y el control de la población a través de la gestión, la conservación y la explotación de datos masivos", 2016, https://ddd.uab.cat/pub/trerecpro/2017/hdl_2072_271333/Treball_de_recerca_3_.pdf

[11] Rafael Bonifaz, “La NSA Según las Revelaciones de Snowden”, UBA, 2017, http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0938_BonifazR.pdf

[12] Barack Obama, “Statement by the President”, 07-06-2013, https://obamawhitehouse.archives.gov/the-press-office/2013/06/07/statement-president

[13] "In most cases, content isn't as valuable as metadata because you can either re-fetch content based on the metadata or, if not, simply task all future communications of interest for permanent collection since the metadata tells you what out of their data stream you actually want", Portal web SPIEGEL ONLINE, 08-07-2013, https://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006-2.html, [Consultado el 02-02-2019]

[14] Ewen MacAskill, artículo del diario The Guardian, "GCHQ taps fibre-optic cables for secret access to world's communications", 21-06-2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, [Consultado el 17-04-2019]

[15] Artículo de Der Spielgel, "NSA-Dokumente: So knackt der Geheimdienst Internetkonten", 30-12-2013, http://www.spiegel.de/fotostrecke/nsa-dokumente-so-knackt-der-geheimdienst-internetkonten-fotostrecke-105326.html, [Consultado el 21-04-2019]

[16] Documento revelado por Edward Snowden, https://edwardsnowden.com/wp-content/uploads/2015/01/media-35669.pdf, [Consultado el 04-12-2018]

[17] Matthew Humphries, artículo del sitio web PCMag de la compañía Ziff Davis, "Dropbox Bug Restores Files Deleted 7 Years Ago", 24-01-2017, https://www.pcmag.com/news/351256/dropbox-bug-restores-deleted-files-7-years-later, [Consultado el 29-11-2018]

[18] Entrevista de Jorge Gestoso a Julian Assange desde la embajada de Ecuador en Londres, agosto 2012, https://www.youtube.com/playlist?list=PL5059AE71F969F0D8

[19] Reporte de investigación del laboratorio The Citizen Lab, "Hide and seek", 18-09-2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/, [Consultado el 22-11-2019]

[20] Reporte de investigación del laboratorio The Citizen Lab, "The million dollar dissident", 24-08-2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/, [Consultado el 22-11-2019]
[21] Artículo del blog de Kaspersky "Pegasus: The ultimate spyware for iOS and Android", 11-04-2017, https://www.kaspersky.com/blog/pegasus-spyware/14604/, [Consultado el 22-11-2019]
[22] Reporte de investigación del laboratorio The Citizen Lab, "Reckless VI", 27-11-2018, https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/, [Consultado el 22-11-2019]
[23] Azam Ahmed & Nicole Perlroth, artículo de The New York Times: "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families", 19-06-2017, https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html?ref=nyt-es&mcid=nyt-es&subid=article, [Consultado el 24-11-2019]
[24] Mails filtrados a Wikileaks sobre intento de negociación de Argentina para adquirir software espía, 2015, https://wikileaks.org/hackingteam/emails/emailid/1088127, [Consultado el 22-11-2019]
[25] Artículo del portal web Info 135, "Una buena: no salió el proyecto que le iba a permitir a Macri legalizar el espionaje a ciudadanos", 26-04-2018, https://info135.com.ar/2018/04/26/una-buena-no-salio-el-proyecto-que-le-iba-a-permitir-a-macri-legalizar-el-espionaje-a-ciudadanos/, [Consultado el 14-12-2019]
[26] Horacio Verbitsky, video de la página de YouTube de El Destape, acerca del uso de Pegasus en Argentina, 31-10-2018, https://www.youtube.com/watch?v=TYKWKNb7h8Q
[27] Mehul Srivastava & Tim Bradshaw, artículo del Financial Times: “Israeli group’s spyware ‘offers keys to Big Tech’s cloud’”, 19-07-2019, https://www.ft.com/content/95b91412-a946-11e9-b6ee-3cdf3174eb89, [Consultado el 29-11-2019]
[28] Tova Cohen & Ari Rabinovitch, artículo del sitio web de Reuters, “Israel eases rules on cyber weapons exports despite criticism”, 22-08-2019, https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ, [Consultado el 29-11-2019]
[29] Artículo del sitio web CNBC: "Amazon’s cloud business acquires Sqrrl, a security start-up with NSA roots", 23-01-2018, https://www.cnbc.com/2018/01/23/amazons-cloud-business-acquires-sqrrl-a-security-start-up-with-nsa-roots.html, [Consultado el 09-01-2020]
[30] Artículo del portal web de la BBC, "La poderosa herramienta de EE.UU. para vigilarlo todo en internet", 01-08-2013, https://www.bbc.com/mundo/noticias/2013/08/130801_tecnologia_snowden_nsa_xkeyscore_dp, [Consultado el 19-11-2018]
[31] Martín Gendler, artículo de la revista Hipertextos "¿Qué es la Neutralidad de la Red?", 2015, http://revistahipertextos.org/wp-content/uploads/2015/12/Qu%C3%A9-es-la-Neutralidad-de-la-Red-Mart%C3%ADn-Gendler.pdf
[32] Eduardo Bertoni, Centro de Estudios en Libertad de Expresión y Acceso a la Información, Facultad de Derecho, Universidad de Palermo, libro "Internet y derechos humanos - Aportes para la discusión en América Latina", 2014, https://www.palermo.edu/cele/pdf/InternetyDDHH.pdf
[33] Marta Peirano, libro "El enemigo conoce el sistema", Editorial Debate, 2019
[34] Lucas Malaspina, articulo del portal web Nueva Sociedad, "¿La democracia de Google, Facebook y YouTube?", Febrero 2018, http://nuso.org/articulo/la-democracia-de-google-facebook-y-youtube/, [Consultado el 07-01-2019]
[35] Elena Santos, artículo del sitio web Genbeta, "¿Por qué nadie parece querer el Internet gratis de Facebook?", 9-02-2016, https://www.genbeta.com/web/por-que-nadie-parece-querer-el-internet-gratis-de-facebook, [Consultado el 07-03-2019]
[36] Ilya Lopes, articulo del sitio web We Live Security, "Marco Civil: la nueva constitución de Internet en Brasil", 26-06-2014, https://www.welivesecurity.com/la-es/2014/06/26/marco-civil-nueva-constitucion-internet-brasil/, [Consultado el 17-05-2019]
[37] Álex Barredo, artículo del portal web de La Vanguardia, "La fórmula de la censura china en Internet", 01-03-2018, https://www.lavanguardia.com/tecnologia/20180301/441152076692/censura-china-internet.html, [Consultado el 29-06-2019]
[38] Pedro Baños, libro "El dominio mundial", Editorial Ariel, 2018

[39] Olivia Canny, artículo de F Newsmagazine, “Apple, China, and the Great Firewall”, 06-11-2019, https://fnewsmagazine.com/2019/11/apple-china-and-the-great-firewall/, [Consultado el 29-11-2019]
[40] Antonio Sabán, artículo del sitio web de Genbeta, "Google ha cancelado Dragonfly, su buscador con censura para China, según The Intercept", 17-12-2018, https://www.genbeta.com/actualidad/google-ha-cancelado-dragonfly-su-buscador-censura-para-china-the-intercept, [Consultado el 30-11-2019]
[41] Ryan Gallagher, artículo de The Intercept, “GOOGLE PLANS TO LAUNCH CENSORED SEARCH ENGINE IN CHINA, LEAKED DOCUMENTS REVEAL”, 01-08-2018, https://theintercept.com/2018/08/01/google-china-search-engine-censorship/, [Consultado el 29-11-2019]
[42] Ryan Gallagher, artículo de The Intercept, “GOOGLE SHUT OUT PRIVACY AND SECURITY TEAMS FROM SECRET CHINA PROJECT”, 29-11-2018, https://theintercept.com/2018/11/29/google-china-censored-search/, [Consultado el 29-11-2019]
[43] Benjamin Haas, articulo del portal web El Diario, "China bloqueará completamente el acceso al internet sin censura en 2018", 13-07-2017, https://www.eldiario.es/theguardian/China-bloqueara-completamente-internet-censura_0_664233769.html, [Consultado el 27-11-2019]
[44] Steven Lee Myers & Amy Cheng, artículo de The New York Times, "68 Things You Cannot Say on China’s Internet", 24-09-2017, https://www.nytimes.com/2017/09/24/world/asia/china-internet-censorship.html?ref=nyt-es&mcid=nyt-es&subid=article, [Consultado el 31-11-2019]
[45] Jack Turner, “Internet Censorship Rankings – The Worst Countries for a Free Web”, 18-02-2019, https://tech.co/vpn/internet-censorship-rankings, [Consultado el 31-11-2019]
[46] Daniela Blandón Ramírez, artículo de France 24, “Rusia: el Gobierno ya podrá desconectar de internet al país en caso de amenaza”, 02-11-2019, https://www.france24.com/es/20191102-gobierno-rusia-desconectar-internet-amenaza, [Consultado el 01-12-2019]
[47] Resolución 2016/2225, "Resolución del Parlamento Europeo, de 14 de marzo de 2017, sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI))", 14-03-2017, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0076+0+DOC+XML+V0//ES
[48] Marta Peirano, Entrevista a Edward Snowden, Periódico digital eldiario.es, 16-09-2019, https://www.eldiario.es/internacional/gobiernos-empezando-autoridad-plataformas-tecnologicas_0_942806555.html, [Consultado el 23-09-2019]
[49] Artículo del portal web Actualidad RT, "Snowden: 'Reino Unido ha legalizado la vigilancia más extrema de la democracia occidental'", 18-11-2016, https://actualidad.rt.com/actualidad/223939-snowden-reino-unido-legalizar-vigilancia-extrema, [Consultado el 04-07-2019]
[50] Edison Lanza, artículo del diario La Nación, "¿El fin de una Internet libre, abierta e inclusiva?", 29-01-2018, https://www.lanacion.com.ar/2104577-el-fin-de-una-internet-libre-abierta-e-inclusiva, [Consultado el 11-05-2019]
[51] Artículo del diario La Nación, "Entra en funcionamiento la neutralidad de la red en Europa", 31-08-2016, https://www.lanacion.com.ar/tecnologia/entra-en-vigor-la-neutralidad-de-la-red-en-europa-nid1933087, [Consultado el 21-05-2019]
[52] Claudio Valero, artículo del sitio web ADSL Zone, "¿De verdad está protegida la neutralidad de la red en Europa? Un estudio siembra dudas", 13-02-2019, https://www.adslzone.net/2019/02/13/dudas-neutralidad-red-europa-estudio/, [Consultado el 21-05-2019]
[53] Artículo del diario Clarín, "Qué es y cómo impacta el fin de la neutralidad en Internet", 11-06-2018, https://www.clarin.com/tecnologia/impacta-fin-neutralidad-internet_0_Hyq6BNheX.html, [Consultado el 21-05-2019]
[54] Gabriel J.X. Dance, Michael LaForgia and Nicholas Confessore, artículo del periódico The New York Times, "As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants", 18-12-2018, https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html?ref=nyt-es&mcid=nyt-es&subid=article, [Consultado el 02-09-2019]

[55] Artículo del portal web Infobae, "Juguetes, televisores y aires acondicionados conectados: ¿la revolución de internet o una red de espionaje?", 3-10-2018, https://www.infobae.com/america/tecno/2018/10/03/juguetes-televisores-y-aires-acondicionados-conectados-la-revolucion-de-internet-o-una-red-de-espionaje/, [Consultado el 05-02-2019]
[56] Marta Peirano, charla TED en Madrid "¿Por qué me vigilan, si no soy nadie?", 2015, https://www.youtube.com/watch?v=NPE7i8wuupk
[57] Artículo del blog del Instituto Internacional de Seguridad Cibernética, "How to influence the electoral processes and hack government elections?", Julio 2018, http://www.iicybersecurity.com/hack-government-elections-democracy.html, [Consultado el 03-12-2018]
[58] Pierluigi Paganini, Articulo del Instituto Infosec, "Cellphone Surveillance: The Secret Arsenal", 8-02-2016, https://resources.infosecinstitute.com/cellphone-surveillance-the-secret-arsenal/#gref, [Consultado el 16-02-2019]
[59] Jon Penney, "Chilling Effects: Online Surveillance and Wikipedia Use", Oxford Internet Institute, Universidad de Oxford, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645
[60] Enrique Amestoy, "Redes y Redes Sociales - Usuarios o Usados", 17-12-2014, http://www.rebelion.org/docs/243229.pdf, [Consultado el 24-10-2019]
[61] Glenn Greenwald: Charla TED "Why privacy matters?", 2014, https://www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript?language=es#t-4905
[62] Lucas Malaspina, revista Crisis, "La era de los gobernautas", 06-04-2018, https://revistacrisis.com.ar/notas/la-era-de-los-gobernautas, [Consultado el 19-03-2019]
[63] Elle Hunt, artículo del diario The Guardian, "Peeple, the 'Yelp for people' review app, launches in North America on Monday", 07-03-2016, https://www.theguardian.com/media/2016/mar/07/peeple-the-yelp-for-people-review-app-launches-in-north-america-on-monday, [Consultado el 01-12-2019]
[64] Irene Larraz, artículo del portal web El Tiempo, "La era de la tiranía digital por 'reviews' y evaluaciones de 'apps'", 17-03-2018, https://www.eltiempo.com/tecnosfera/novedades-tecnologia/la-tirania-digital-por-las-evaluaciones-que-las-personas-dan-en-una-aplicacion-195226, [Consultado el 01-12-2019]
[65] Artículo del portal web Xataka, "'Estimados pasajeros: cumplan las normas para evitar puntos negativos', así está implementando China su crédito social", 17-12-2018, https://www.xataka.com/legislacion-y-derechos/estimados-pasajeros-cumplan-normas-para-evitar-puntos-negativos-asi-esta-implementando-china-su-credito-social, [Consultado el 26-09-2019]
[66] Raúl Álvarez, artículo de Xataka, “La policía china estrena gafas con reconocimiento facial para identificar y capturar sospechosos”, 07-02-2018, https://www.xataka.com/privacidad/la-policia-china-estrena-gafas-con-reconocimiento-facial-para-identificar-y-capturar-sospechosos, [Consultado el 27-09-2019]
[67] Rocío A. Gómez Sustacha, articulo del portal web Marketing4eCommerce, "Sesame Credit: Big Data al estilo Gran Hermano para valorar la 'confiabilidad' de los ciudadanos chinos", 30-10-2017, https://marketing4ecommerce.net/sesame-credit-big-data-control-ciudadano/, [Consultado el 26-09-2019]
[68] Ignacio Rey, artículo del diario La Diaria, "Una red social avanza entre los chinos con consecuencias tangibles para los ciudadanos", 06-01-2018, https://findesemana.ladiaria.com.uy/articulo/2018/1/una-red-social-avanza-entre-los-chinos-con-consecuencias-tangibles-para-los-ciudadanos/, [Consultado el 29-09-2019]
[69] Kate Conger, David E. Sanger & Scott Shane, artículo de The New York Times, “Microsoft Wins Pentagon’s $10 Billion JEDI Contract, Thwarting Amazon”, 25-10-2019, https://www.nytimes.com/2019/10/25/technology/dod-jedi-contract.html, [Consultado el 30-11-2019]
[70] Artículo del portal web Noticias de Seguridad Informática, "usuarios deben elegir entre usar smart speaker o su privacidad", 12-01-2019, https://noticiasseguridad.com/tecnologia/usuarios-deben-elegir-entre-usar-smart-speaker-o-su-privacidad/, [Consultado el 04-02-2019]
[71] Jorge Majfud, artículo del portal web Rebelión, "¿Son neutrales las redes sociales?", 23-10-2017, http://www.rebelion.org/noticia.php?id=233128&titular=%BFson-neutrales-las-redes-sociales?-, [Consultado el 22-01-2019]

[72] David Garcia, artículo de la revista Science Advances, "Leaking privacy and shadow profiles in online social networks", 04-08-2017, http://advances.sciencemag.org/content/3/8/e1701172, [Consultado el 04-08-2019]
[73] Germán Padinger, articulo del portal web Infobae, 03-03-2018, https://www.infobae.com/america/tecno/2018/03/03/las-redes-sociales-en-el-banquillo-de-la-fascinacion-al-temor/, [Consultado el 18-05-2019]
[74] Marcelo Colussi, articulo del portal web Rebelión, "Redes sociales e ideología", 08-03-2018, http://www.rebelion.org/noticia.php?id=238790&titular=redes-sociales-e-ideolog%EDa-, [Consultado el 03-02-2019]
[75] Andrea Missinato, artículo del portal web Spindox, "Fake news | Artificial Intelligence and Automated fake news", 13-11-2018, https://www.spindox.it/en/blog/fake-news-artificial-intelligence-and-automated-fake-news/, [Consultado el 26-04-2019]
[76] Pedro Baños, libro "Así se domina el mundo", Editorial Ariel, 2017
[77] Tom Secker & Matthew Alford, artículo de Insurge Intelligence, “EXCLUSIVE: Documents expose how Hollywood promotes war on behalf of the Pentagon, CIA and NSA”, 04-07-2017, https://medium.com/insurge-intelligence/exclusive-documents-expose-direct-us-military-intelligence-influence-on-1-800-movies-and-tv-shows-36433107c307, [Consultado el 05-04-2019]
[78] Publicación del portal web Blackbot, "Tendencias 2019", 12-12-2018, https://blackbot.rocks/2018/12/tendencias-2019/, [Consultado el 14-03-2019]
[79] José Ángel Plaza López, artículo del diario El País, "Inteligencia artificial - Los ‘deepfakes’ complican la lucha contra las noticias falsas", 18-09-2018, https://retina.elpais.com/retina/2018/09/17/innovacion/1537177382_367863.html, [Consultado el 14-03-2019]
[80] Artículo del portal web Nobbot, "Lo que nos faltaba: llegan los vídeos ‘deepfake’, más peligrosos que las ‘fake news’", 03-01-2019, https://www.nobbot.com/pantallas/deepfake-fake-news/, [Consultado el 14-03-2019]
[81] Kevin Roose, artículo del periódico The New York Times, "Here Come the Fake Videos, Too", 04-03-2018, https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html?ref=nyt-es&mcid=nyt-es&subid=article, [Consultado el 15-03-2019]
[82] Esther Miguel Trula, “¿Para qué sirve un fact-checking? Por qué la democracia puede sobrevivir sin desmentir un dato falso”, 12-04-2019, https://magnet.xataka.com/en-diez-minutos/sirve-fact-checking-que-democracia-puede-sobrevivir-desmentir-dato-falso, [Consultado el 27-08-2019]
[83] Lion Gu, Vladimir Kropotov, & Fyodor Yarochkin, TrendLabs (The Global Technical Support and R&D Center of TREND MICRO), "The Fake News Machine", 2017, https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
[84] Lee Fang, artículo de The Intercept, “SAUDI ARABIA CONTINUES HIRING SPREE OF AMERICAN LOBBYISTS, PUBLIC RELATIONS EXPERTS”, 05-10-2015, https://theintercept.com/2015/10/05/saudi-arabia-continues-hire-politically-connected-american-lobbyists-public-relation-firms/, [Consultado el 06-04-2019]
[85] Enrique Santiago Romero, artículo del portal web El Diario, “El 'lawfare': guerra jurídica contra la democracia”, 21-08-2018, https://www.eldiario.es/tribunaabierta/lawfare-guerra-juridica-democracia_6_806029406.html, [Consultado el 01-09-2019]
[86] Artículo de CELAG, “Lawfare. La judicialización de la política en América Latina”, 2017, https://www.celag.org/wp-content/uploads/2017/03/LawfareT.pdf
[87] Video del Papa Francisco hablando sobre el Lawfare, 2019, https://www.youtube.com/watch?v=0HL1HMSuT0s
[88] Artículo del sitio resumenlatinoamericano.org, “Argentina. Juez federal Ramos Padilla expone red ilegal de espionaje”, 13-03-2019, http://www.resumenlatinoamericano.org/2019/03/13/argentina-juez-federal-ramos-padilla-expone-red-ilegal-de-espionaje/, [Consultado el 02-09-2019]
[89] Artículo del diario Perfil, “Movistar confirmó que el teléfono que tenía agendado D'Alessio era el de Patricia Bullrich”, 21-05-2019, https://www.perfil.com/noticias/politica/caso-dalessio-patricia-bullrich-quiere-saber-quien-filtro-sus-datos-personales-nieto-amenazas.phtml, [Consultado el 02-09-2019]
[90] The Intercept, “Secret Brazil Archive”, https://theintercept.com/series/secret-brazil-archive/, [Consultado el 16-11-2019]

[91] Ernesto Londoño y Leticia Casado, artículo del New York Times, “Mensajes filtrados despiertan dudas sobre la justicia anticorrupción en Brasil”, 10-06-2019, https://www.nytimes.com/es/2019/06/10/sergio-moro-lava-jato/, [Consultado el 18-11-2019]
[92] Artículo de La tinta, “Brasil: ‘La cadena Globo y el grupo de tareas del Lava Jato son socios’”, 18-06-2019, https://latinta.com.ar/2019/06/brasil-la-cadena-globo-y-el-grupo-de-tareas-del-lava-jato-son-socios/, [Consultado el 17-11-2019]
[93] Brian Mier, artículo de Brasil Wire, “US Congress members demand answers on DOJ/Lava Jato partnership”, 21-08-2019, https://www.brasilwire.com/congress-members-demand-answers-on-doj-lava-jato-partnership/, [Consultado el 20-11-2019]
[94] Berit Anderson & Brett Horvath, "The Rise of the Weaponized AI Propaganda Machine", 12-02-2017, https://medium.com/join-scout/the-rise-of-the-weaponized-ai-propaganda-machine-86dac61668b
[95] Aníbal García Fernández, "Cambridge Analytica, el big data y su influencia en las elecciones", 27-03-2018, http://www.celag.org/cambridge-analytica-el-big-data-y-su-influencia-en-las-elecciones/?preview_id=15676, [Consultado el 26-12-2018]
[96] Sara Suarez, artículo "Tus likes ¿tu voto? Explotación masiva de datos personales y manipulación informativa en la campaña electoral de Donald Trump a la presidencia de EEUU 2016", 2018, https://www.cac.cat/sites/default/files/2019-01/Q44_Suarez_ES.pdf
[97] Lucas Malaspina, artículo "Facebook en crisis" del diario La diaria, 24-03-2018, https://findesemana.ladiaria.com.uy/articulo/2018/3/facebook-en-crisis/, [Consultado el 10-01-2019]
[98] Entrevista de Santiago O´Donnell a Julian Assange, 12-07-2017, http://medioextremo.com/2017/07/12/el-dia-que-dejemos-de-ser-los-chicos-malos-sera-porque-no-estamos-haciendo-nuestro-trabajo/, [Consultado el 30-01-2019]
[99] Artículo de Infobae, “El informe de Robert Mueller revela que no hubo colusión entre el equipo de campaña de Trump y Rusia”, 24-02-2019, https://www.infobae.com/america/eeuu/2019/03/24/el-congreso-de-eeuu-recibio-un-breve-resumen-del-informe-de-robert-mueller-sobre-la-injerencia-rusa/, [Consultado el 10-09-2019]
[100] Begoña Arce, articulo del Portal web El Periódico, "Prostitutas, sobornos y elecciones en Cambridge Analytica", 20-03-2018, https://www.elperiodico.com/es/internacional/20180320/ejecutivos-cambridge-analyticafilmados-alardeando-prostitutas-sobornos-influencia-elecciones-channel-4-6702488, [Consultado el 20-03-2019]
[101] Video de Alexander Nix, el CEO de Cambridge Analytica, "CEO de Cambridge Analytica: 'trabajamos en Argentina'", 2018, https://www.youtube.com/watch?v=K609-CQtO6s
[102] Edición del programa "El destape" de Argentina sobre El trabajo de manipulación en redes sociales del gobierno de Mauricio Macri y sobre Cómo funcionaba la estrategia de Cambridge Analytica, 26-04-2018, https://www.youtube.com/watch?v=zWmsSsusYyE
[103] Juan Torrez López, articulo de su página web, "No se fíen de Google", 04-11-2017, http://www.juantorreslopez.com/no-se-fien-de-google/, [Consultado el 04-05-2019]
[104] Entrevista de Rafael Correa a Edward Snowden, 2020, https://www.youtube.com/watch?v=hluk3rXZQqE
[105] Artículo de MIT Technology Review, “¿Qué es la comunicación cuántica? Definición y conceptos clave”, 27-02-2019, https://www.technologyreview.es/s/10953/que-es-la-comunicacion-cuantica-definicion-y-conceptos-clave, [Consultado el 09-12-2019]
[106] Pratik Jakhar, artículo de la BBC, “Beidou vs GPS: cómo China quiere hacer global su alternativa al sistema de navegación de Estados Unidos”, 01-10-2018, https://www.bbc.com/mundo/noticias-45639488, [Consultado el 13-12-2019]
[107] Película “Snowden”, director Oliver Stone, 2016
[108] Artículo del portal web de Todo Noticias, "Documentos de Snowden: el manual interno que explica cómo manipular a las personas mediante operaciones en Internet", 2-04-2015, https://tn.com.ar/politica/la-operacion-quito-desacreditando-al-adversario_578060, [Consultado el 01-05-2019]
[109] David E. Sanger and Nicole Perlroth, artículo de The New York Times, "U.S. Escalates Online Attacks on Russia’s Power Grid", 15-06-2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html, [Consultado el 27-06-2019]
[110] Artículo del portal web Noticias de Seguridad Informática, "Ha comenzado la guerra cibernética entre Irán y Estados Unidos", 24-06-2019, https://noticiasseguridad.com/hacking-

incidentes/ha-comenzado-la-guerra-cibernetica-entre-iran-y-estados-unidos/, [Consultado el 27-06-2019]
[111] Artículo del portal web de Pagina 12, "Irán dice que cayó una red de espías de la CIA", 19-06-2019, https://www.pagina12.com.ar/201149-iran-dice-que-cayo-una-red-de-espias-de-la-cia, [Consultado el 02-07-2019]
[112] Artículo de Los Ángeles Times, “China está muy por detrás de EE. UU en vehículos autónomos, pero está decidido a mejorar”, 01-06-2019, https://www.latimes.com/espanol/vidayestilo/la-es-china-esta-muy-por-detras-de-ee-uu-en-vehiculos-autonomos-pero-esta-decidido-a-mejorar-20190517-story.html, [Consultado el 14-11-2019]
[113] Paul Mozur, artículo del periódico The New York Times, "AT&T Drops Huawei’s New Smartphone Amid Security Worries", 09-01-2018, https://www.nytimes.com/2018/01/09/business/att-huawei-mate-smartphone.html, [Consultado el 15-11-2019]
[114] Artículo del portal web Infobae, "El gigante tecnológico Huawei, sospechado de espionaje chino en EEUU", 09-01-2018, https://www.infobae.com/america/eeuu/2018/01/09/el-gigante-tecnologico-huawei-sospechado-de-espionaje-chino-en-eeuu/, [Consultado el 31-10-2019]
[115] Juan Elman, artículo del portal web de Cenital, “5G y el regreso de la política bipolar”, 07-06-2019, https://www.cenital.com/5g-y-el-regreso-de-la-politica-bipolar/, [Consultado el 15-11-2019]
[116] Anna Gross & Madhumita Murgia, artículo del Financial Times, “China and Huawei propose reinvention of the internet”, 27-03-2020, https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2, [Consultado el 15-04-2020]
[117] Glenn Greenwald, artículo de The Intercept, “Watch: Are We Vesting Too Much Power in Governments and Corporations in the Name of Covid-19? With Edward Snowden”, 08-04-2020, https://theintercept.com/2020/04/08/watch-are-we-vesting-too-much-power-in-governments-and-corporations-in-the-name-of-covid-19-with-edward-snowden/, [Consultado el 26-04-2020]
[118] Entrevista a Marta Peirano, Revista Ethic, 20-04-2020, https://ethic.es/entrevistas/marta-peirano/, [Consultado el 27-04-2020]
[119] Harold David Chaparro Zuñiga, "TOR, anonimato en internet", UBA, 2015, http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0885_ChaparroZunigaHD.pdf
[120] Saraswat, K. (2015). TOR: The Onion Router. Informe de seminario. National Institute of Technology Karnataka, Surathkal
[121] Documento revelado por Snowden, 2013, https://edwardsnowden.com/wp-content/uploads/2013/10/tor-stinks-presentation.pdf, [Consultado el 11-01-2019]
[122] Rafael Bonifaz, “Comunicaciones Secretas en Internet”, UBA, 2019, http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-1272_BonifazR
[123] Artículo de International Business Times, “WhatsApp files lawsuit against Israeli firm for hacking into activists' phones”, 30-10-2019, https://www.ibtimes.sg/whatsapp-files-lawsuit-against-israeli-firm-hacking-into-activists-phones-33707, [Consultado el 11-02-2020]
[124] Artículo de Reuters, “U.N. says officials barred from using WhatsApp since June 2019 over security”, 23-01-2020, https://ca.reuters.com/article/idCAKBN1ZM32P?rpc=401&, [Consultado el 11-02-2020]
[125] Ionut Ilascu, artículo de Bleeping Computer, “Telegram Desktop Saves Conversations Locally in Plain Text”, 30-10-2018, https://bleepingcomputer.com/news/security/telegram-desktop-saves-conversations-locally-in-plain-text/, [Consultado el 12-02-2020]
[126] Artículo de Outlook India Magazine, “Telegram, Signal won't shield your chats from hackers”, 10-11-2019, https://www.outlookindia.com/newsscroll/telegram-signal-wont-shield-your-chats-from-hackers/1659383, [Consultado el 15-02-2020]
[127] Artículo de RT, “Snowden advierte sobre el peligro del uso de WhatsApp y Telegram”, 16-09-2019, https://actualidad.rt.com/actualidad/327288-snowden-peligro-whatsapp-telegram, [Consultado el 02-02-2020]
[128] Elías Rodríguez García, artículo del portal web Omicrono, "El Internet descentralizado, la solución al fin de la neutralidad de la red", 27-01-2018, https://omicrono.elespanol.com/2018/01/que-es-el-internet-descentralizado/, [Consultado el 27-02-2020]

[129] Angela Karl, artículo del sitio web de TechGenix, "Fight the power: why it is time for the decentralized web", 01-03-2018, http://techgenix.com/decentralized-web/, [Consultado el 27-02-2020]
[130] Whitepaper oficial de la fundación Substratum sobre la web descentralizada, https://whitepaper.io/document/51/substratum-whitepaper
[131] Chris Dannen, "Introducing Ethereum and Solidity", 2017, http://kek.ksu.ru/EOS/Blockchain/Introducing%20Ethereum%20and%20Solidity_%20Foundatiin%20Programming%20for%20Beginners%20-%20Chris%20Dannen.pdf
[132] Juan Bautista Hernández Serrano, "Explorando la Blockchain de Ethereum y el desarrollo de smart contracts", Universidad Politécnica de Cataluña, 2018, https://upcommons.upc.edu/bitstream/handle/2117/127784/memoria.pdf?sequence=1&isAllowed=y
[133] Artículo del portal web Noticias de Seguridad Informática, "Criptografía cuántica, nueva forma de cifrar comunicaciones privadas", 14-06-2019, https://noticiasseguridad.com/tecnologia/criptografia-cuantica-nueva-forma-de-cifrar-comunicaciones-privadas/, [Consultado el 28-01-2020]
[134] Steven Rich & Barton Gellman, artículo de The Washington Post, "NSA seeks to build quantum computer that could crack most types of encryption", 02-01-2014, https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html, [Consultado el 27-01-2020]
[135] Raphael Labaca Castro , artículo de Welivesecurity, "La revolución cuántica y los desafíos de la seguridad", 01-07-2014, https://www.welivesecurity.com/la-es/2014/07/01/revolucion-cuantica-desafios-seguridad/, [Consultado el 26-01-2020]
[136] Héctor Cancino, artículo de AE Tecno, "PROFESOR MATEO VALERO Y LOS DESARROLLOS EN COMPUTACIÓN CUÁNTICA: 'HASTA AHORA, ESTÁN EN EL INVIERNO POLAR'", 16-01-2020, https://tecno.americaeconomia.com/articulos/profesor-mateo-valero-y-los-desarrollos-en-computacion-cuantica-hasta-ahora-estan-en-el, [Consultado el 27-01-2020]
[137] Reglamento (UE) 2016/679, 2016, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=ES
[138] Artículo de Panda Security, "El GDPR en 2019: el año de la multa millonaria", 18-12-2019, https://www.pandasecurity.com/spain/mediacenter/seguridad/gdpr-multas-resumen/, [Consultado el 07-11-2019]
[139] Edward Snowden, videoconferencia desde Moscú ante una audiencia en la Universidad de Dalhousie (Halifax, Canadá), 31-05-2019, https://actualidad.rt.com/actualidad/316813-snowden-advierte-mayor-control-social, [Consultado el 15-06-2019]
[140] Ricardo Mendes, Joao P. Vilela, Universidad de Coimbra, Portugal, "Privacy-Preserving Data Mining: Methods, Metrics, and Applications", 2017, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7950921
[141] Ramya Shree Kiran A N P., "Privacy Preserving Unstructured Data Publishing (PPUDP) Approach for Big Data", International Journal of Computer Applications, 2019, https://www.ijcaonline.org/archives/volume178/number28/kiran-2019-ijca-919091.pdf
[142] D. Bachlechner, K. La Fors, A. M. Sears, "The Role of Privacy-Preserving Technologies in the Age of Big Data", 2018, https://www.albany.edu/wisp/papers/WISP2018_paper_11.pdf
[143] Ana Gómez Blanco, BBVA, "Internet de las cosas: precauciones de seguridad a tener en cuenta", 13-05-2019, https://www.bbva.com/es/internet-de-las-cosas-precauciones-de-seguridad-a-tener-en-cuenta/, [Consultado el 04-01-2020]
[144] Artículo del sitio web de Smart Lighting, "Tomémonos en serio la seguridad en IoT: ¿Qué se puede hacer?", 30-12-2019, https://smart-lighting.es/tomemonos-serio-la-seguridad-iot-se-puede/, [Consultado el 04-01-2020]
[145] Fernando Biurrun Abad, "La seguridad del Internet de las cosas (IoT) va a tener su primera regulación en California", 03-01-2020, http://www.legaltoday.com/gestion-del-despacho/nuevas-tecnologias/articulos/la-seguridad-del-internet-de-las-cosas-iot-va-a-tener-su-primera-regulacion-en-california, [Consultado el 08-01-2020]
[146] Artículo del diario El País de Uruguay, "WhatsApp combate las fake news", 22-01-2019, https://www.elpais.com.uy/vida-actual/whatsapp-combate-fake-news.html, [Consultado el 23-09-2019]

[147] Adrian Diaz, Artículo de El Espectador, “WhatsApp contra las fake news: estas son las nuevas medidas que adoptará la app”, 26-03-2019, https://www.elespectador.com/tecnologia/whatsapp-contra-las-fake-news-estas-son-las-nuevas-medidas-que-adoptara-la-app-articulo-846998, [Consultado el 23-09-2019]
[148] Philipe de Freitas Melo, Carolina Coimbra Vieira, Kiran Garimella, Pedro O. S. Vaz de Melo & Fabrício Benevenuto, UFMG-MIT, “Can WhatsApp Counter Misinformation by Limiting Message Forwarding?”, 2019, https://arxiv.org/pdf/1909.08740.pdf
[149] Pablo Ximénez de Sandoval, diario El País, “Twitter prohíbe los anuncios políticos en su plataforma en todo el mundo”, 31-10-2019, https://elpais.com/internacional/2019/10/30/actualidad/1572467801_480841.html, [Consultado el 04-11-2019]
[150] Whitepaper de ElevenPaths, Telefónica, “La Inteligencia Artificial: Aplicabilidad de GANs y Autoencoders en la Ciberseguridad”, 2019, https://www.elevenpaths.com/wp-content/uploads/2019/06/whitepaper-la-inteligencia-artificial-aplicabilidad-de-gans-autoencoders-ciberseguridad.pdf
[151] Iván Arribas, artículo del sitio web Vandalytic, “Cómo Machine Learning y la IA pueden combatir las FAKE NEWS”, 20-08-2019, https://vandalytic.com/como-machine-learning-y-la-ia-pueden-combatir-las-fake-news/, [Consultado el 29-09-2019]
[152] Marcos Merino, artículo de Xataka, “Twitter adquiere una startup de deep learning para mejorar su propia tecnología de detección de 'fake news'”, 04-06-2019, https://www.xataka.com/inteligencia-artificial/twitter-adquiere-startup-deep-learning-para-mejorar-su-propia-tecnologia-deteccion-fake-news, [Consultado el 02-10-2019]
[153] Anjana Susarla, Michigan State University, “HOW ARTIFICIAL INTELLIGENCE CAN DETECT - AND CREATE - FAKE NEWS”, 02-08-2018, https://msutoday.msu.edu/news/2018/how-artificial-intelligence-can-detect-and-create-fake-news/, [Consultado el 22-09-2019]
[154] Artículo de El Independiente, Entrevista a Joaquín Quiñonero, 17-11-2019, https://www.elindependiente.com/futuro/2019/11/17/la-inteligencia-artificial-nos-ha-ayudado-a-detectar-los-contenidos-que-incitaban-al-odio/, [Consultado el 28-11-2019]
[155] “La Declaración Universal de Derechos Humanos”, https://www.un.org/es/universal-declaration-human-rights/
[156] Alessandro Acquisti: charla TED "Why privacy matters?", 2013, https://www.ted.com/talks/alessandro_acquisti_why_privacy_matters/transcript?awesm=on.ted.com_g0KWd&language=es&share=13767d4893&utm_source=direct-on.ted.com&utm_content=roadrunner-rrshorturl&utm_medium=on.ted.com-none&utm_campaign=#t-126475
[157] Marta Peirano, charla TED en Madrid “La vigilancia es un problema colectivo, como el cambio climático”, https://www.ted.com/talks/la_vigilancia_es_un_problema_colectivo_como_el_cambio_climatico?language=es

Índice de imágenes

Imagen 1 - Metadatos recopilados por la NSA....17
Imagen 2 - Estación de Menwith Hill....19
Imagen 3 - Medidas de seguridad que las agencias de inteligencia intentan vulnerar....21
Imagen 4 - Justificación de la NSA a la vigilancia de los SMS....22
Imagen 5 - Interceptación de equipos e insersión de implantes....25
Imagen 6 - Mapa mundial de ruteo de fibra óptica....26
Imagen 7 - Programa PRISM....26
Imagen 8 - Características técnicas de PRISM....28
Imagen 9 - Funcionamiento de PRISM....29
Imagen 10 - Definición de los programas UPSTREAM y PRISM....30
Imagen 11 - Mapa del programa FinFisher....32
Imagen 12 - Mapa de la presencia de Hacking Team....33
Imagen 13 - Mapa del programa Pegasus....34
Imagen 14 - Países con los que los Cinco Ojos comparten datos....37
Imagen 15 - Flujo de datos del programa PRISM....39
Imagen 16 - Posibles consultas sobre XKEYSCORE....41
Imagen 17 - Dispositivo Gossamer....75
Imagen 18 - Fuentes vinculadas a noticias falsas encontradas por el profesor Albright....122
Imagen 19 - Robot Maars....138
Imagen 20 - NYC Mesh....163
Imagen 21 - Búsqueda en Shodan....172
Imagen 22 - Búsqueda en Thingful....172